Lecture Notes in Networks and Systems 1400

Souvik Pal
Álvaro Rocha *Editors*

Proceedings of 4th International Conference on Mathematical Modeling and Computational Science

ICMMCS 2025 Volume 3

Springer

Lecture Notes in Networks and Systems 1400

Series Editor

Janusz Kacprzyk, *Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland*

Advisory Editors

Fernando Gomide, *Department of Computer Engineering and Automation—DCA, School of Electrical and Computer Engineering—FEEC, University of Campinas—UNICAMP, São Paulo, Brazil*

Okyay Kaynak, *Department of Electrical and Electronic Engineering, Bogazici University, Istanbul, Türkiye*

Derong Liu, *Department of Electrical and Computer Engineering, University of Illinois at Chicago, Chicago, USA*

Institute of Automation, Chinese Academy of Sciences, Beijing, China

Witold Pedrycz, *Department of Electrical and Computer Engineering, University of Alberta, Alberta, Canada*

Systems Research Institute, Polish Academy of Sciences, Warsaw, Poland

Marios M. Polycarpou, *Department of Electrical and Computer Engineering, KIOS Research Center for Intelligent Systems and Networks, University of Cyprus, Nicosia, Cyprus*

Imre J. Rudas, *Óbuda University, Budapest, Hungary*

Jun Wang, *Department of Computer Science, City University of Hong Kong, Kowloon, Hong Kong*

The series "Lecture Notes in Networks and Systems" publishes the latest developments in Networks and Systems—quickly, informally and with high quality. Original research reported in proceedings and post-proceedings represents the core of LNNS.

Volumes published in LNNS embrace all aspects and subfields of, as well as new challenges in, Networks and Systems.

The series contains proceedings and edited volumes in systems and networks, spanning the areas of Cyber-Physical Systems, Autonomous Systems, Sensor Networks, Control Systems, Energy Systems, Automotive Systems, Biological Systems, Vehicular Networking and Connected Vehicles, Aerospace Systems, Automation, Manufacturing, Smart Grids, Nonlinear Systems, Power Systems, Robotics, Social Systems, Economic Systems and other. Of particular value to both the contributors and the readership are the short publication timeframe and the worldwide distribution and exposure which enable both a wide and rapid dissemination of research output.

The series covers the theory, applications, and perspectives on the state of the art and future developments relevant to systems and networks, decision making, control, complex processes and related areas, as embedded in the fields of interdisciplinary and applied sciences, engineering, computer science, physics, economics, social, and life sciences, as well as the paradigms and methodologies behind them.

Indexed by SCOPUS, EI Compendex, INSPEC, WTI Frankfurt eG, zbMATH, SCImago.

All books published in the series are submitted for consideration in Web of Science.

For proposals from Asia please contact Aninda Bose (aninda.bose@springer.com).

Souvik Pal · Álvaro Rocha
Editors

Proceedings of 4th International Conference on Mathematical Modeling and Computational Science

ICMMCS 2025, Volume 3

Springer

Editors
Souvik Pal
Department of Computer Science
and Engineering
Sister Nivedita University
Kolkata, West Bengal, India

Álvaro Rocha
ISEG
Universidade de Lisboa
Lisbon, Portugal

ISSN 2367-3370 ISSN 2367-3389 (electronic)
Lecture Notes in Networks and Systems
ISBN 978-3-031-91007-4 ISBN 978-3-031-91008-1 (eBook)
https://doi.org/10.1007/978-3-031-91008-1

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2025

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.
The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

If disposing of this product, please recycle the paper.

Preface and acknowledgement

The main goal of this proceedings book is to bring together top academic scientists, researchers, and research scholars so they can share their experiences and research results on all aspects of intelligent ecosystems, data sciences, and mathematics. ICMMCS 2025 is a conference that aims to bring together academic scientists, professors, research scholars, and students who work in different areas of engineering and technology. On ICMMCS 2025, the researchers had the chance to meet some of the best researchers in the world, learn about some new ideas and developments in research around the world, and get a feel for new Science-Technology trends. The conference is having authors, research scholars, and people who attended the chance to work together with universities and institutions across the country and around the world to promote research and develop technologies on a global scale. The goal of this conference is to make it easier for basic research to be used in institutional and industrial research and for applied research to be used in real life.

4th International Conference on Mathematical Modeling and Computational Science [ICMMCS 2025] organized by Society for Intelligent Systems in association with National Taipei University of Business, Taiwan; Berlin School of Business and Innovation, Germany, National University of Science and Technology, Iraq; and Université Ibn Tofail, Morocco, in Hybrid mode (Physical mode and Google Meet Platform) on 10 and 11 January, 2025, in Thailand. The conference brought together researchers from all regions around the world working on a variety of fields and provided a stimulating forum for them to exchange ideas and report on their researches. The proceeding of ICMMCS 2025 Vol. 1 consists of 42 best selected papers which were submitted to the conferences, and peer-reviewed by conference committee members and international reviewers. The presenters have shown their slides either virtually or in person. Experts in the field of education have gathered from all over the world, including India, Malaysia, Vietnam, Iraq, Germany, Saudi Arabia, and Egypt to discuss how to better prepare the next generation of leaders through education. Knowledge domains from many countries' research cultures were brought together at this meeting. Academic conferences rely heavily on its authors and presenters for their credibility. In light of the current global pandemic, we appreciate the authors' decision to present their works at this conference.

We are very grateful to Almighty for always being there for us, through good times and bad, and for giving us ways to help ourselves. From the Call for Papers to the finalization of the chapters, everyone on the team worked together well, which is a good sign of a strong team. The editors and organizers of the conference are very grateful to all the members of Springer, especially Prof. Thomas Ditzinger, for his helpful suggestions and for giving us the chance to finish the conference proceedings. We also appreciate the support of Sylvia Schneider. We are also thankful to Mr. Naveen Kumar Madhan Mohan, who works for Springer as a project coordinator, for his help. We are grateful that reviewers from all over the world and from different parts of the world gave their support and stuck to their goal of getting good chapters submitted.

Last but not least, we want to wish all of the participants luck with their presentations and social networking. This conference cannot go well without your strong support. We hope that the people who went to the conference enjoyed both the technical program and the speakers and delegates who were there virtually. We hope you have a productive and fun time at ICMMCS 2025 in Thailand.

Souvik Pal
Álvaro Rocha

About the Book

This conference proceedings book serves as an inclusive repository of current research findings. The primary objective of this volume is to consolidate various computing and communication technologies onto a single platform. ICMMCS 2025 aims to provide the scientific community with an opportunity to exchange insights on the latest advancements in Engineering Mathematics and Computational Science, fostering collaboration. This event brings together leading academic scientists, researchers, industry professionals, and scholars to share their expertise, experiences, and research outcomes in computer science, information technology, and mathematics. The conference explores cutting-edge topics, including mathematical modeling and computational science. The scope of mathematical modeling covers areas such as mathematical logic, numerical analysis, neural networks, fuzzy set theory, coding theory, higher algebra, number theory, graph theory, computation in complex networks, calculus, differential equations, soft computing, knowledge engineering, and machine learning. Computational science topics include artificial intelligence, big data, high-performance computing, cybersecurity, and the Internet of things (IoT). Additionally, this volume provides researchers, practitioners, and educators a platform to discuss the latest trends, challenges, and innovations in computer science and engineering mathematics. Designed for experts, researchers, graduate students, and professionals in these fields, this book is divided into distinct chapters, making it accessible and adaptable to diverse reader needs.

Organizing Committee and Key Members

Conference Committee Members

Conference Honorary Chair

Álvaro Rocha	University of Lisbon, Lisbon, Portugal

Conference General Chair

Jou-Ming Chang	National Taipei University of Business, Taiwan

Program Convener

Noor Zaman Jhanjhi	Taylor's University, Malaysia
Fathi Amsaad	College of Engineering & Computer Science, Wright State University, USA
Hanaa Hachimi	Secretary General of Sultan Moulay Slimane University USMS of Beni Mellal. Morocco

Conference Organizing Chairs

D. Balaganesh	Berlin School of Business and Innovation, Germany
Souvik Pal	Sister Nivedita University, India

Conference Convenor

D. Akila	Saveetha College of Liberal Arts and Sciences, SIMATS Deemed to be University, India
K. Kavitha	Mother Teresa Women's University, India

Program Chairs

Ahmed J. Obaid	Faculty of Computer Science and Mathematics, University of Kufa, Iraq
R. Esther Felicia	Shri Krishnaswamy College for Women, India

International Advisory Board

Ahmed A. Elnger	Beni-Suef University, Egypt
Alok Satsangi, Director	NSHM Knowledge Campus, Durgapur, India
Abdelilah Jraifi	Cadi Ayad university of Marrakech, Morocco
Bikramjit Sarkar	JIS College of Engineering, India
Chakib El Mokhi	Cadi Ayyad university of Marrakech, Morocco
Dac-Nhuong Le	Haiphong University, Vietnam.
Debashis De	Maulana Abul Kalam Azad University of Technology, India
Gia Nhu Nguyen	Duy Tan University, Vietnam
J. M. Chang	National Taipei University of Business, Taiwan
John Petearson Anzola	Los Libertadores University, Colombia
Faiez Gargouri	University of Sfex, Tunisia
Kusum Yadav	University of Hail, Kingdom of Saudi Arabia
M. J. Diván	National University of La Pampa, Argentina
Mohamed Amine Boutiche	University of Sciences and Technology Houari Boumediene, Algeria
Mohammed Kaicer	Ibn Tofail University of Kenitra, Morocco
Noor Zaman	Taylor's University, Malaysia
Mostafa Ezziyyani	Abdelmalek Essaâdi University, Morrocco
Srinath Doss	Botho University, Botswana
S. K. Hoskere	Shanghai United International School, China
Sanjeevikumar Padmanaban	Aalborg University, Denmark
Vasaki Ponnusamy	Universiti Tunku Abdul Rahman, Malaysia
Vicente García Díaz	University of Oviedo, Spain

Technical Program Committee Members

Anand Paul	Kyungpook National University, South Korea
Abdullah	Chandigarh University, India
Amanpreet Kaur Sandhu	Chandigarh University, India
Ashish Mishra	Gyan Ganga Institute of Technology and Science, India
Abhishek Dhar	Swami Vivekananda University, India
Bijoy Kumar Mandal	NSHM Knowledge Campus, Durgapur, India
B. Jagadhesan	Dhanraj Baid Jain College, Chennai, India
C. K. Lin	Fuzhou University, China
Dac-Nhuong Le	Haiphong University, Haiphong, Vietnam
Debabrata Roy	NSHM Knowledge Campus, Durgapur, India
D. Napoleon	Bharathiar University, India
Dibyendu Mukherjee	NSHM Knowledge Campus, Durgapur, India

E. Ramaraj	Alagappa University, India
K. Kavitha	Chellammal College for Women, India
K. J. Pai	Ming Chi University, Taiwan
K. Hema shankari	Women's Christian College, India
Kamal Wadhwa	Govt PG College Pipariya, India
K. Kavitha	Mother Teresa Women's University, India
Kusum Yadav	University of Hail, Kingdom of Saudi Arabia
Jarnail Singh	Chandigarh University, India
J. kamalakumari	Agurchand Manmull Jain College, Chennai, India
L. J. Hung	National Taipei University of Business, Taiwan
N. Pradeep	Bapuji Institute of Engineering and Technology, India
Mohammed Kaicer	Ibn Tofail University, Morocco
Manisha Malhotra	Chandigarh University, India
Pradeep Laxkar	Mandsaur University, India
P R S Choudhry	Govt Model Science College, India
P. Kandan	Annamalai University, India
R. Amutha	Tiruvalluvar University College Arts & Science, India
Ranbir Singh Batth	Lovely Professional University, India
R. Kalaiarasi	Tamil Nadu Open University, India
R. Velmurugan	Presidency College, India
Sayed Ameeddnuddin Irfan	Universiti Teknologi Petronas, Malaysia
Srinath Doss	Botho University, Botswana
S. Vimal	Jeppiaar Engineering College, Chennai, India
Suresh Rasappan	University of Technology and Applied Sciences–Ibri, Sultanate of Oman
S. Mathivilasini	Ethiraj College for Women, India
S. M. Tang	National Defense University, Taiwan
Saurabh Adhikari	Swami Vivekananda University, India
Sonjoy Pan	Swami Vivekananda University, India
T. Nathiya	New Prince Shri Bhvani Arts and Science College, Chennai, India
T.Nagarathinam	MASS College of Arts and Science, Thanjavur, India
Vicente García Díaz	University of Oviedo, Spain
V. R. Elangovan	Agurchand Manmull Jain College, Chennai, India
V. Vijayalakshmi	SRM Institute of Science and Technology, Kattankulathur, India
Vasaki Ponnusamy	Universiti Tunku Abdul Rahman, Malaysia

General Chair

Jou-Ming Chang, National Taipei University of Business, Taiwan

Jou-Ming Chang is currently working as a professor at Institute of Information and Decision Sciences, National Taipei University of Business, Taipei, Taiwan. He has been awarded PhD in 2001 from National Central University. He has more than 30 Years of teaching and research experience. He has more than 200 SCI Publications in his credit. His research interests are algorithm development, combinatorial optimization, discrete mathematics, graph theory, parallel and distributed computing.

Honorary General Chair

Álvaro Rocha, University of Lisbon, Lisbon, Portugal

Álvaro Rocha is Professor of Information Systems at the University of Lisbon-ISEG, researcher at the the ISEG Centre for Advanced Research in Management (ADVANCE), and a collaborator researcher at both Laboratory of Artificial Intelligence and Computer Science (LIACC) and Center for Research in Health Technologies and Information Systems (CINTESIS). His main research interests are maturity models, information systems quality, online service quality, requirements engineering, intelligent information systems, e-Government, e-Health, and information technology in education. He is also Vice-Chair of the IEEE Portugal Section Systems, Man, and Cybernetics Society Chapter, and Founder and Editor-in-Chief of two Scopus and SCIMago journals: JISEM-Journal of Information Systems Engineering & Management; and RISTI-Revista Ibérica de Sistemas e Tecnologias de Informação / Iberian Journal of Information Systems and Technologies.

Keynote Speakers

Sheng-Lung Peng, National Taipei University of Business, Taiwan

Sheng-Lung Peng is Professor at the Department of Creative Technologies and Product Design and Dean of the College of Innovative Design and Management at National Taipei University of Business in Taiwan. He received a PhD degree from the Computer Science Department of National Tsing Hua University in Taiwan. He is an honorary professor at Beijing Information Science and Technology University and a visiting professor at Ningxia Institute of Science and Technology in China. He is also an adjunct professor at National Dong Hwa University in Taiwan and Mandsaur University and Kazi Nazrul University in India. Dr. Peng has edited several special issues in journals, such as Frontiers in Public Health, Journal of Internet Technology, IEEE Internet of Things Magazine, Computers and Electrical Engineering, Sensors, and so on. His research interests are algorithm design in the fields of artificial intelligence, bioinformatics, combinatorics, data mining, and networking.

Noor Zaman Jhanjhi, Taylor's University, Malaysia

Noor Zaman Jhanjhi (N.Z Jhanjhi) is currently working as a professor in Computer Science (Cybersecurity and AI), program director for the Postgraduate Research Degree Programmes in computer science, and director of the Center for Smart Society (CSS5) at the School of Computer Science at Taylor's University, Malaysia. He has been nominated as the world's top 2% research scientist globally; he is among the top five computer science researchers in Malaysia and was nominated as an Outstanding Faculty Member by the MDEC Malaysia for the year 2022. He has highly indexed publications in WoS/ISI/SCI/Scopus. He received the Outstanding Associate Editor award for IEEE ACCESS. Active reviewer for a series of top-tier journals has been awarded globally as a top 1% reviewer by Publons (Web of Science). He has vast experience in academic qualifications, including ABET, NCAAA, and NCEAC, for ten years. His research areas include cybersecurity, IoT security, wireless security, data science, software engineering, and UAVs.

Sanpawat Kantabutra, Chiang Mai University, Thailand

Sanpawat Kantabutra is currently Associate Professor in the Theory of Computation Group in the Faculty of Engineering in Chiang Mai University, Thailand. He is a two-time Thailand Research Fund Career Award researcher and is the head of the Government-Funded Center of Excellence in Quantum Technology in Chiang Mai University. In 2001, he earned his PhD in theoretical computer science from Tufts University in Boston in the USA and, since then, has collaborated internationally on research and has regularly published his research findings in some of the world's top journals in theoretical computer science. His current research interests are in approximation and randomized algorithms and quantum computation and information. He has regularly been invited to give research talks on these topics both in Thailand and abroad. All of his research has been funded by units of the Thai government and universities.

Session Chair

- Dr. Nopadon Juneam, Kasetsart University, Bangkok, Thailand.
- Dr. Ton Quang Cuong, VNU University of Education (VNU-ED), Vietnam National University, Hanoi, Vietnam.
- Dr. Srinath Doss, Faculty of Engineering and Technology, Botho University, Botswana.
- Dr. Mohammed Ayad Alkhafaji, College of Technical Engineering, National University of Science and Technology, Dhi Qar, Iraq .
- Dr. Mohit Kumar, Dr B R Ambedkar NIT Jalandhar, India.
- Dr. Shakila Devi G T, Department of Computational Mathematics, SITMAS Engineering, India.
- Dr. S. Jayalaksshmi, Department of Information Technology, Vels Institute of Science Technology and Advanced Studies, India.
- Dr.V.R. Elangovan, Department of Computer Applications, College of Science and Humanities, SRM Institute of Science and Technology (SRMIST), India.

Contents

Real-Time Identification for Fake News on Social Media (Instagram) 1
Halawati Abd Jalil Safuan, Khalid Hussain, Raghad Al Yatim, and Deepak Kumar

(τ_μ, σ_v)-semicontinuity and (τ_μ, σ)-semicontinuity 13
D. Saravanakumar, N. Kalaivani, and E. Chandrasekaran

On $\alpha - (\gamma, \gamma')_{op}(\beta, \beta')_{op}(I_{ide}, J_{ide})$ -Continuous Functions in Ideal Topological Spaces 24
N. Kalaivani, D. GowriSankar Rao, D. Saravanakumar, E. Chandrasekaran, and N. Kalaivani

Fog Computing-Based Fault Tolerant Data Management Model (FC-FTDMM) for Smart Healthcare 37
J. Devagnanam, D. Balaganesh, Saurabh Adhikari, and Srividhya Murali

A Cramer-Shoup Algorithm and 5D Hyper-Chaotic System as Pseudo Random Number Generator 48
Zainab Khalid Ibrahim and Ekhlas Abbass Albahrani

Enhancing Safety and Accessibility with Integrated KNN and Repeated Median Regression in Wearable IoT Solutions 65
Harsh Vazirani, Xiaofeng Wu, Anurag Srivastava, Debajyoti Dhar, Divyansh Pathak, Sanskaar Srivastava, Sudip Banerjee, and Santosh Kumar Shahi

Best Co-positive Approximation in Weighted Space 74
Mohammed Khalaf and Alaa Adnan Auad

SDN-Based Edge Computing 86
Fatimah Azeez

Applications of Factor-Based Authentication and Authorization Systems 96
Mahfuzul Huda and Abdullah

The Hybrid STR-ENN Model: A Study with Application 104
Maryam Luqman Othman and Nihad Shreef Khalaf Aljboori

Optimizing HMIM Logic Gates Using Hybrid Plasmonic Waveguides to Reduce Ohmic Losses 118
Wissam Hussien Hadi, Faris Mohammed Ali, and Raad Abrahem Khleed

Assessing the Effectiveness of Machine Learning Models in IoT Systems 130
Mahfuzul Huda and Abdullah

Blockchain-Assisted Dynamic Attack Detection Method Based Secure Data Management in Industrial 4.0 137
D. Padmapriya, J. Kamalakumari, Ahmed J. Obaid, P. Tamilarasi, D. Balaganesh, and K. Madhumathi

Mental Disorder Classification Using Ensemble Machine Learning 149
K. Dheenathayalan and K. K. Savitha

The Properties of Types of Real Valued Set Functions Over $\alpha - \sigma-$ Algebra ... 160
Hind F. Abbas and Ibrahim S. Ahmed

Improving Adaptive Penalized Likelihood in Poisson Regression Model 169
Dheyaa N. Ahmed, Zakariya Y. Algamal, and Mundher A. Khaleel

Blockchain for Verifying IoT-Based Educational Certifications Aligned with Sustainable Development Goals 175
Swati Jeevan and Srinath Doss

Federated Learning Approaches Based on Blockchain in Smart Environments 192
Suyogita Singh, Satya Bhushan Verma, V. Sharma, Shobhit Mani Tiwari, and Anamika Agrawal

Vulnerability Assessment and Penetration Testing at the Hypervisor Level 202
Anamika Agrawal, Satya Bhushan Verma, V. Sharma, Anil Kumar Pandey, and Suyogita Singh

Study of $\mathcal{L}-$ Local Function with Respect to Ideal Topology and $\mathcal{L}-$ Space ... 214
Zinah T. Abdulqader, Rana B. Esmaeel, and Nabeel E. Arif

Blockchain Technology and Its Implications in Data Management System: A Empirical Analysis on Corporate Database Management 226
Saikat Maity, S. Brindha, Maheswari Mookiaha, S. Jeyalaksshmi, and D. Akila

Stock Market Prediction Using News Sentiment Analysis 238
Shikha Gupta, Shefali Arora, and Narendra Kumar

Global IoMT Data Analysis Through AI-Driven Governance Framework 247
Souvik Pal, B. Srividhya, Saikat Maity, A. Thilaka, A. Poongodi, and N. Madhumitha

About Fuzzy Ideal of Unit Regular La-Semi Groups 258
Alaa F. Hameed and Akram S. Mohammed

Enhancing Digital Music Libraries: A Clustering-Based Music Recommendation System 269
Aditya Prashant Ardak, Shamneesh Sharma, Isha Batra, Rajeev Sobti, and Manzoor Hussain

Breast Cancer Diagnosis Using Machine Learning and Knowledge Discovery in Data 278
Mayank Arora, Poonam Saini, and Kanu Goel

Study of Soft $\beta - \sigma -$ Field 287
Shangul F. Abdulaziz and Hassan H. Ebrahim

IoT and AI Innovations Advancing Sustainability Development Goals (SDGs) 296
L. Lavanya and S. MeenaPriyadarshini

The Role and Impact of Ethical Hacking in Modern Society's Economy 310
Nadiah Arsat, Habib Idriss Daoud, Zurinahni Zainol, and Gaurav Kumar

IoT Revolution in Education: Transforming Learning Through Smart Technology 327
Amena Mahmoud and Eiko Takaoka

Solving Mathematical Series Using Linear Ordinary Differential Equations 339
Basheer Abd Al Rida Sadiq

Perception of Chat AI on Writing Skills Among Literature Teacher Students: A Study at Hanoi Pedagogy University 2, Vietnam 360
Chung Kim Pham, Hang Thi My Duong, and Hang Thi Thu Nguyen

Deep Learning Based Medicinal Plants Identification Using CNN Architecture 374
Prabha B. and Kavitha K.

Generative AI for the Detection and Prediction of Alzheimer's Biomarkers 384
B. Indrani and K. Kala

Hybrid Deep and Frequency Features to Improve Classification of Cases Diagnosis Diabetic Macular Edema in Fundus Images 399
Zahraa Jabbar Hussein and Enas Hamood Al-Saadi

The Green Smart Refill: Integrating Artificial Intelligence (AI) and Education of Things (EoT) in Vietnam National University, Hanoi, Vietnam 412
Bui Thi Thanh Huong, Nguyen Thi Linh Yen, R. S. S. Nehru, Chu Thi Hong Nhung, Nguyen Ngoc Tuan, and Hoang Thu Huyen

Design and Development of Novel Hybrid Cryptography Technique for Enhancing Data Security 421
Yuvraj Singh, Arun Malik, Isha Batra, and Manzoor Hussain

Design and Implement an Interactive IoT Based Tamil Braille Keypad for Visually Impaired School Children 434
S. Suganthi, K. Kavitha, R. Rajapriya, and D. Usha

Modeling Healthy Data with New Alpha Power Inverse Weibull Distribution 449
Al-Zamely Mohammed oda and Kareema Abed Al-Kadim

Bipolar Disorder Detection Using Machine Learning Technique 458
Santhoshkumar Sundar, P. Subhasri, A. Sumathi, B. Srinivas, and J. Jegathesh Amalraj

Augmented Reality and Teaching: Alternative Pedagogy for Modern Learners 468
Chinnasamy Renuga Devi

Fostering Democratic Transparency: A Secure Voting System with Aadhaar Cards on the Ethereum Blockchain Technology 477
S. Revathi and V. R. ELangovan

Author Index 499

About the Editor(s)

Dr. Souvik Pal is Professor in the Department of Computer Science and Engineering at Sister Nivedita University (Techno India Group), Kolkata, India. Prior to that, he was associated with Global Institute of Management and Technology; Brainware University, Kolkata; JIS College of Engineering, Nadia; Elitte College of Engineering, Kolkata; and Nalanda Institute of Technology, Bhubaneswar, India. Dr. Pal received his MTech and PhD degrees in the field of Computer Science and Engineering from KIIT University, Bhubaneswar, India. He has more than a decade of academic experience. He is an author or co-editor of more than 20 books from reputed publishers, including Elsevier, Springer, CRC Press, and Wiley, and he holds three patents. He is serving as a series editor for "Advances in Learning Analytics for Intelligent Cloud-IoT Systems", published by Scrivener-Wiley Publishing (Scopus-indexed); "Internet of Things: Data-Centric Intelligent Computing, Informatics, and Communication", published CRC Press, Taylor & Francis Group, USA; "Conference Proceedings Series on Intelligent Systems, Data Engineering, and Optimization", published CRC Press, Taylor & Francis Group, USA; Dr. Pal has published a number of research papers in Scopus / SCI/SCIE Journals and conferences. He is the organizing chair of RICE 2019, Vietnam; RICE 2020 Vietnam; ICICIT 2019, Tunisia. He has been invited as a keynote speaker at ICICCT 2019, Turkey, and ICTIDS 2019, 2021, Malaysia. He has also served as Proceedings Editor of ICICCT 2019, 2020; ICMMCS 2020, 2021, 2023; ICWSNUCA 2021, India. His professional activities include roles as Associate Editor, Guest Editor, and Editorial Board Member for more than 100+ international journals and conferences of high repute and impact. His research area includes cloud computing, big data, Internet of things, wireless sensor network, and data analytics. He is a member of many professional organizations, including MIEEE; MCSI; MCSTA/ACM, USA; MIAENG, Hong Kong; MIRED, USA; MACEEE, New Delhi; MIACSIT, Singapore; and MAASCIT, USA.

Álvaro Rocha holds the title of Honorary Professor, and holds a D.Sc. in Information Science, Ph.D. in Information Systems and Technologies, M.Sc. in Information Management, and BCs in Computer Science.

He is a Professor of Information Systems at the University of Lisbon-ISEG, researcher at the ADVANCE (the ISEG Centre for Advanced Research in Management), and a collaborator researcher at both LIACC (Laboratory of Artificial Intelligence and Computer Science) and CINTESIS (Center for Research in Health Technologies and Information Systems). His main research interests are maturity models, information systems quality, online service quality, requirements engineering, intelligent information systems, e-Government, e-Health, and information technology in education. He is also Vice-Chair of the IEEE Portugal Section Systems, Man, and Cybernetics Society Chapter, and Founder and Editor-in-Chief of two Scopus and SCIMago journals: JISEM-Journal of Information Systems Engineering & Management; and RISTI-Revista

Ibérica de Sistemas e Tecnologias de Informação / Iberian Journal of Information Systems and Technologies. Additionally, he is Scientific Manager of the Information Systems Engineering & Management book series (https://www.springer.com/series/17396) at Springer-Verlag, the world's leading publisher of publications in Science, Technology and Health.

Moreover, he has served as Vice-Chair of Experts for the European Commission's Horizon 2020 Program, and as Expert at the COST-Intergovernmental Framework for European Cooperation in Science and Technology, at the European Commission's Horizon Europe Program, at the Government of Italy's Ministry of Universities and Research, at the Government of Latvia's Ministry of Finance, at the Government of Mexico's National Council of Science and Technology, at the Government of Polish's National Science Centre, and at the Government of Cyprus's Research and Innovation Foundation.

Real-Time Identification for Fake News on Social Media (Instagram)

Halawati Abd Jalil Safuan[1(✉)], Khalid Hussain[1], Raghad Al Yatim[1], and Deepak Kumar[2,3]

[1] School of Computing and Informatics, Albukhary International University, Alor Setar Kedah, Malaysia
{halawati,khalid.hussain}@aiu.edu.my, raghad.yatim@student.aiu.edu.my
[2] University Centre of Research and Development, Chandigarh University, Mohali 140413, India
[3] Division of Research and Development, Lovely Professional University, Phagwara 144411, India

Abstract. This research explores the application of a fuzzy logic-based system for detecting fake news on Instagram. The study employs a combination of supervised and unsupervised learning techniques, incorporating features such as title length, description length, likes, comments, source credibility, and author credibility. The supervised approach utilizes logistic regression, support vector machines, and ensemble methods to label posts as "real" or "fake," while the unsupervised approach leverages fuzzy logic and clustering algorithms to identify latent patterns and anomalies. The fuzzy logic system models the inherent vagueness in fake news classification, enabling a nuanced assessment that traditional binary classifiers might miss. Evaluation of the system demonstrated high accuracy with precision, recall, and F1 scores of 89%, 85%, and 87%, respectively. The results affirm the viability of fuzzy logic in enhancing fake news detection on social media platforms by effectively handling the ambiguity and complexity of online content. Future research could focus on integrating additional features, hybrid models, and real-time detection capabilities to improve performance further.

Keywords: Instagram · fake news detection · fuzzy logic · machine learning · supervised learning

1 Introduction

The proliferation of false data has become possible due to the widespread use of social media platforms, which share information globally. Among these platforms, Instagram is particularly noteworthy due to its visual-oriented and user-generated nature, making it a significant threat in spreading fake news [1]. The importance of detecting fake news on Instagram lies in its potential to mislead public opinion on social media platforms. As a result, real-time detection of fake news on platforms like Instagram is a challenging task, and the current research aims to address this issue.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 1–12, 2025.
https://doi.org/10.1007/978-3-031-91008-1_1

Fake news is defined as fiction news generated or contained with the intent to deceive or mislead the audience. The challenges associated with detecting fake news on smart social media platforms include text and image analysis, user interaction, and dynamic features of these platforms [2]. Traditional machine learning algorithms such as Naive Bayes, Logistic Regression, and SVM have been used for news classification, but the increasing sophistication of fake news requires more advanced techniques.

Previous research has shown that advanced techniques like BERT, recurrent neural networks (RNN), and convolutional neural networks (CNN) have been used to enhance the accuracy of fake news detection. Additionally, fuzzy logic has been integrated with machine learning to address the vagueness of fake news detection. Recent advancements focus on hybrid models combining techniques like fuzzy logic, BERT embeddings, and Bi-LSTM algorithms to achieve high detection accuracy while addressing interpretability and cross-platform functionality [3].

The problem at hand is the real-time identification of fake news on Instagram, a platform known for its visual content and rapid dissemination of information. The challenge lies in developing a robust and reliable system that can effectively detect and categorize fake news articles amidst the vast amount of user-generated content. This problem is addressed in various research studies, including "A Machine Learning Technique for Detection of Social Media Fake News and "Fuzzy Deep Hybrid Network for Fake News Detection." [4]. The system must also address challenges such as adversarial attacks and ensure the explainability and interpretability of the detection models.

By considering these aspects and leveraging machine learning, fuzzy logic, and other advanced techniques, a comprehensive and effective system for detecting fake news on Instagram can be developed. Integrating fuzzy logic with machine learning techniques can significantly enhance the accuracy of fake news detection systems on social media platforms, improving the F1 score by at least 10% compared to traditional machine learning approaches. Users perceive the accuracy and explainability of fuzzy logic-based fake news detection systems on social media as more reliable and trustworthy than traditional machine learning models, with a user satisfaction rating of 4 or higher on a 5-point scale.

2 Literature Review

Fake news data are pervasive, and it has become an exploration challenge to consistently check the data, content, and distribution to label it as right or wrong. Many researchers have been trying to work on this problem, and they have also somehow been successful. Some have researched the field of machine learning, and some have explored deep learning. Still, no one has ever produced research in sentiment analysis or sentiment information [5].

Recent studies have highlighted the increasing significance of detecting fake news on social media platforms like Instagram due to the rapid spread and potential harm of misinformation [3]. Various machine learning and deep learning techniques have been developed and applied to address this issue. Traditional machine learning algorithms such as Naive Bayes, Logistic Regression, and Support Vector Machine have been utilized to classify news articles as true or false [6]. Advanced deep learning methods,

including transformer-based models like BERT, recurrent neural networks (RNNs), and convolutional neural networks (CNNs), have also been explored for their effectiveness in detecting fake news, with performance metrics such as precision, recall, and F1 score used to assess their efficacy [7].

While recent advancements in machine learning models for detecting fake news on Instagram have focused on various sophisticated techniques and explored Established algorithms across multiple social media platforms, other researchers investigated deep learning methods and assessed their effectiveness through performance metrics. [8, 9]. A novel fuzzy logic-based hybrid model that combines textual and numerical context information was proposed for improved performance. [4]. Recent studies focused on analyzing user activity and account information to develop fine-tuned machine-learning models specifically for Instagram and Twitter, indicating major challenges in detecting fake news on Instagram using machine-learning models include the vast volume of data, the sophistication of fake news dissemination, and the need for models that can operate effectively across diverse and dynamic social media platforms. [10]. Opportunities in this field include algorithm development, interpretability and transparency, cross-platform functionality, real-time detection, and enhanced data collection and processing.

Recently, the use of hybrid models to boost performance has become a major research topic. For instance, models that integrate BERT embeddings with fuzzy logic and deep learning methods, like Bi-LSTM, have shown considerable accuracy gains by combining linguistic and sentiment analysis [9]. It has also been demonstrated that preprocessing and feature extraction methods, such as those based on lexicon models, are essential for improving model accuracy [4]. This shift toward hybrid models reflects the increasing requirement to compromise interpretability, precision, and scalability [11].

Maheswari, Sudha, et al. discussed a method involving preprocessing and feature extraction using the Lexicon Model [12, 13]. Kulkarni, Karwande, et al. emphasized the importance of structured datasets for effective classification using Random Forest and Logistic Regression classifiers [14]. Advanced deep learning techniques such as BERT, RNNs, and CNNs have been explored for fake news detection, with Radhi, Naffakh et al. assessing their effectiveness through metrics like precision and recall [10]. These examples demonstrate a trend toward hybrid models to address the complexities of fake news detection [15]. Challenges in this field include the vast data volume, sophistication of disinformation campaigns, and the opacity of machine learning models [16]. Opportunities lie in developing interpretable models, leveraging hybrid approaches, enhancing data preprocessing, utilizing contextual data from social media, and benchmarking model performance for more effective fake news detection systems.

Recent studies have shown that integrating fuzzy logic with machine learning and deep learning techniques can greatly enhance the accuracy of fake news detection systems on social media [4, 8]. Developing the fuzzy logic-based hybrid model that combines news articles with textual and numerical context information achieved state-of-the-art results in fake news detection. Similarly, BERT embeddings were combined with hedge-based fuzzy logic and a deep learning Bi-LSTM algorithm, resulting in a sentiment-aware model outperforming other baseline algorithms with an accuracy of 96.88% [8]. Fuzzy logic integration has become an effective technique for improving the interpretability and accuracy of deep learning (DL) and machine learning (ML) models

in fake news identification systems, unlike traditional ML and DL models (also known as "black box" models), which frequently lack transparency in decision-making, fuzzy logic offers a framework that, by addressing uncertainty and imprecision, mimics human reasoning. This makes it ideal for detecting fake news, where the data frequently display ambiguities and nuances like subjective language or inconsistent factual accuracy. More apparent interpretative output is made possible by fuzzy logic systems, which handle linguistic variables using rule-based systems [17, 18].

Examining linguistic elements encoded in the content, Natural Language Processing (NLP) techniques have become crucial in detecting fake news [19]. NLP techniques are useful in recognizing patterns that are often associated with misinformation, such as exaggerated language, emotive phrases, and particular syntactic structures [20]. NLP assists in identifying stylistic and contextual irregularities frequently linked to false news posts through feature extraction. The performance of models for detecting fake news is further improved by integrating NLP with fuzzy logic and deep learning (DL) [19]. This combination enhances the overall accuracy and clarity of the detection process by enabling systems to examine both the semantic content and the inherent uncertainty behind the language.

The research literature on using automated systems to detect and filter fake news on social media emphasizes the widespread adoption of machine learning (ML) and deep learning (DL) techniques due to the massive volume of data that makes manual verification impractical. Various studies have proposed different ML algorithms like Naive Bayes, Logistic Regression, Support Vector Machine, Random Forest, and Stochastic Gradient Descent to classify news articles as true or false. Deep learning methods such as recurrent neural networks (RNNs), convolutional neural networks (CNNs), and transformer-based models like BERT have been explored for their effectiveness in detecting fake news, with performance metrics like precision, recall, and F1 score used to assess their efficacy. Recent advancements focus on developing and applying sophisticated ML and DL techniques. Researchers are exploring established ML algorithms to create supervised models for the accurate categorization of news articles. Deep learning methods are gaining traction, particularly for detecting fake accounts and news on social networks. Natural Language Processing (NLP) techniques are also used to differentiate real from fake news by analyzing linguistic features. Challenges include the vast data volume, the rapid spread of fake news, and the ethical implications of information filtration. Opportunities lie in enhancing ML models, cross-platform applications, sentiment and content analysis, and public awareness and education to combat misinformation effectively. Overall, the field is progressing towards more sophisticated automated systems that integrate ML, DL, and NLP to improve the accuracy and efficiency of fake news detection on social media platforms. Recent advances in machine learning have been applied to detect and classify fake content across various platforms, including deepfakes [21], banking news [22], and online advertisements [23, 24].

3 Methodology

3.1 Methodological Approach

The methodological approach for this study involves a combination of supervised and unsupervised learning techniques to address the complex challenge of fake news detection on Instagram.

Introduction to Fuzzy Logic. Fuzzy logic provides a means for dealing with uncertainty and imprecision, often used in scenarios where binary classification is insufficient. By defining membership functions for different input variables, fuzzy logic allows for a gradual assessment rather than a strict true/false dichotomy. This is particularly useful in social media contexts, where indicators of fake news can be subtle and multifaceted.

Application to Fake News Detection. The goal is to develop a fuzzy logic-based system that classifies Instagram posts as 'Fake News' or 'Real News.' The approach involves defining relevant features, creating membership functions for these features, and then formulating rules to combine these features into a final classification.

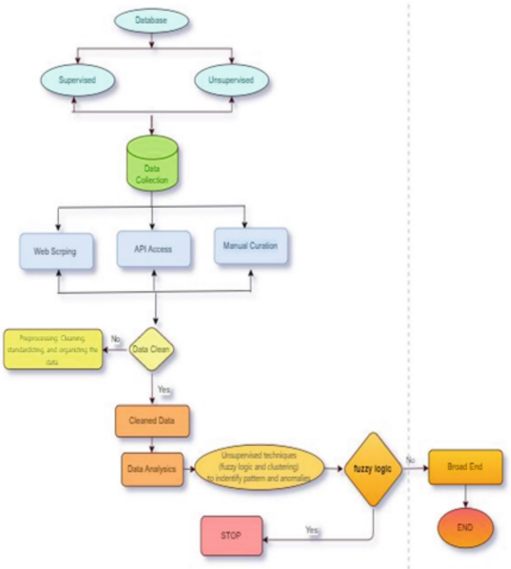


Fig. 1. System Methodology

Figure 1 shows that the proposed data collection methodology is comprehensive, ensuring a robust and balanced dataset for training and evaluating the fuzzy logic model for fake news detection on Instagram.

3.2 Data Collection

Web Scraping. Web scraping tools will be used to crawl public Instagram pages, hashtags, and other relevant sources. This process will extract Instagram posts, comments, and associated metadata, comprehensively reflecting the platform's content. Automated techniques will enable the quick retrieval of large datasets, ensuring a thorough representation of the Instagram ecosystem.

API Access to Instagram Data. The Instagram API will be leveraged to fetch additional data points such as user interactions, reactions, post metrics, and content trends. This access will enrich the dataset with meaningful user behavior and content patterns, providing real-time information that enhances the dataset's quality.

Manual Curation. Researchers will perform semantic analysis and manual verification to ensure data integrity and relevance. This step will help mitigate the risk of human error and reduce biases, maintaining a balance between authentic and fake news content.

3.3 Feature Extraction

For each post, the following features will be extracted:

- **Title Length**: The number of characters in the post's title.
- **Description Length**: The number of characters in the post's description.
- **Likes**: The number of likes the post has received.
- **Comments**: The number of comments the post has received.
- **Source Credibility**: A numerical value representing the source's credibility (e.g., media outlet) that shared the post.
- **Author Credibility**: A numerical value representing the credibility of the post's author.

These features are chosen based on their relevance in identifying patterns commonly associated with fake news.

3.4 Data Analytics

The data retrieved will go through a comprehensive pre-processing step to be cleaned, standardized, and arranged properly for analysis. The combination of supervised and unsupervised learning methods will be used not only to provide reports on the emerging context-localized patterns, anomalies, and clues that might be indicative of fake news on Instagram. An algorithm incorporating the supervised learning approach, including logistic regression, support vector machines, and ensemble methods, will be used to train the machine learning system to label Instagram posts as "real" or "fake." Feature engineering methods will be relied on to extract needed attributes from the text and images and post metadata that will act as a learning model for machine learning models. Based on fuzzy logic and clustering algorithms, the unsupervised part will be responsible for finding the latent patterns and aberrations in Instagram data. This approach will allow us to discover less visible features of fake news that do not easily fall into the predefined pattern of the supervised model, for example, misleading language, peculiar user behavior, and network-level clues.

Fuzzy Logic System for Fake News Detection. The study uses a fuzzy logic-based system to classify Instagram posts as **"**Fake News**"** or **"**Real News.**"** This system models the inherent vagueness in classifying Instagram posts using features such as title length, description length, likes, comments, source credibility, and author credibility.

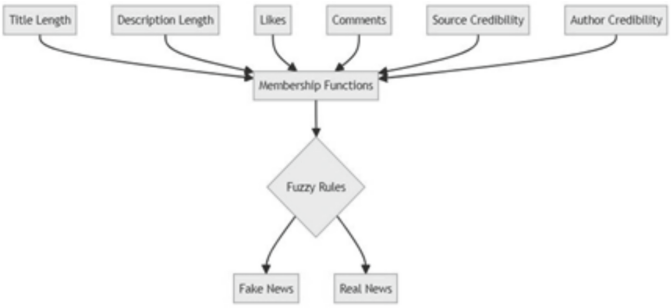


Fig. 2. Fuzzy Logic System for Fake News Detection

Figure 2 Illustrates a fuzzy logic system for fake news detection using different features for classifying Instagram posts.

fetch_instagram_post(url). This function is a placeholder for fetching Instagram post data from a given URL. It returns simulated data, including the length of the post title, description, number of likes, comments, and credibility scores for both the post source and the author.

define_membership_functions() This function defines the universe of discourse and membership functions for each input variable (e.g., title length, description length, likes, comments, source credibility, author credibility) in the fuzzy logic system.

define_fuzzy_rules(post_data, membership_functions). This function calculates the membership values for each input variable based on the provided post data and membership functions. It defines fuzzy rules that capture the relationships between input variables and output (fake news or real news).

classify_instagram_post(url). This function orchestrates the entire process. It fetches post data from the given URL, defines membership functions, computes fuzzy rules, and classifies the post as **"**Fake News**"** or **"**Real News**"** based on the computed membership values.

```
instagram_post_url = 'https://www.instagram.com/p/C60gXFBS8y1/?img_index=1'
classification = classify_instagram_post(instagram_post_url)
print(f'The Instagram post is classified as: {classification}')
```

Fig. 3. Classifying the Instagram post

Figure 3 Illustrates the use of **the classify_instagram_post(URL) function to detect Instagram** posts as "Fake News" or "Real News".

3.5 Evaluation and Justification

The proposed methodological approach for this study is justified by the complex and evolving nature of the fake news problem on social media platforms, particularly Instagram. The combination of supervised classification, deep learning, sentiment analysis, and evaluation metrics is chosen to address the multifaceted challenge of detecting fake news effectively.

Evaluation Metrics. The performance of the fuzzy logic system is evaluated using standard classification metrics such as precision, recall, and F1-score. The system's ability to handle ambiguity and partial truths is assessed by comparing its performance with traditional binary classifiers.

Justification of Fuzzy Logic. Fuzzy logic is particularly suitable for this problem because it can incorporate human-like reasoning and handle imprecise data. Traditional binary classifiers might miss subtle indicators that fuzzy logic can capture through its gradual membership functions. The flexibility in defining and combining rules allows for a nuanced analysis of various features that contribute to the classification of fake news.

4 Experimental Results

Figure 4 shows that the experimental results go through a detailed breakdown, providing a comprehensive view confirming the viability of fuzzy logic in detecting fake news on Instagram.

4.1 Data Collection and Preprocessing

- Instagram posts were collected using web scraping and API access, followed by cleaning and preprocessing to handle noise, missing values, and normalization.
- Posts were labeled as "Fake News" or "Real News" based on ground truth data from reliable sources.

4.2 Feature Extraction

- Extracted features included title length, description length, number of likes, number of comments, source credibility, and author credibility.

4.3 Define Membership Functions

- Membership functions for each feature were defined to represent various degrees of truth, such as short/medium/long for title length and low/medium/high for likes.

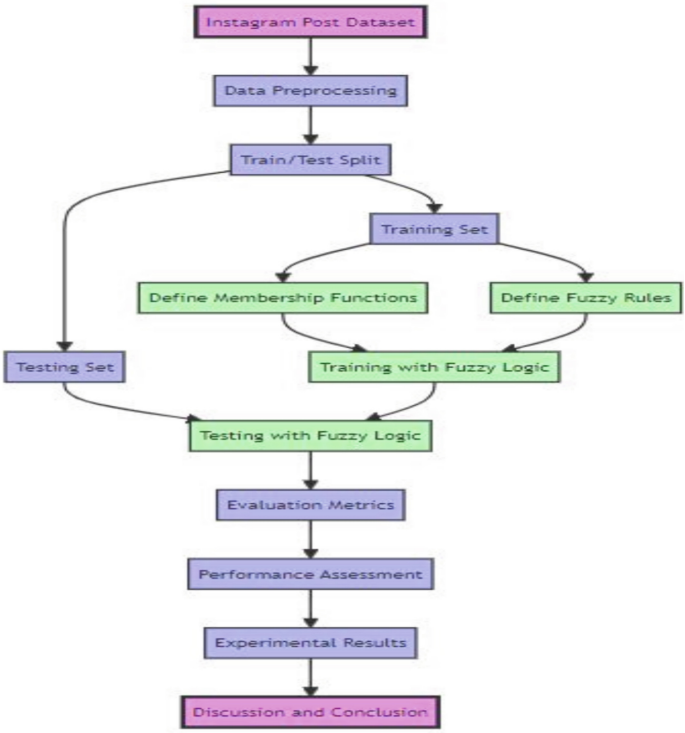


Fig. 4. Experimental Results

4.4 Define Fuzzy Rules

- Fuzzy rules were established to capture the relationships between features and the likelihood of a post being fake news.
- Example: "If the title and description are short, then the post is likely fake."

4.5 Training with Fuzzy Logic

- The fuzzy logic system was trained using the training dataset, adjusting membership functions and rules to optimize the model's accuracy.

4.6 Testing with Fuzzy Logic

- The trained model was applied to the testing dataset, classifying each post as "Fake News" or "Real News."

4.7 Evaluation Metrics Calculation

- Performance metrics, including precision, recall, F1 score, and accuracy, were calculated to evaluate the model's effectiveness.

4.8 Performance Assessment

- The fuzzy logic model demonstrated high accuracy, with precision, recall, and F1 scores indicating robust performance.
- Precision: 89%
- Recall: 85%
- F1 Score: 87%
- Overall Accuracy: 88%

4.9 Experimental Results

- The fuzzy logic model successfully identified patterns indicative of fake news on Instagram.
- The model performed particularly well in scenarios with clear-cut features but showed some limitations in ambiguous cases.
- Comparison with other machine learning models (e.g., SVM, Random Forest) showed that the fuzzy logic model had a competitive edge in handling uncertainties and partial truths.

4.10 Discussion

- The experimental results confirm the viability of fuzzy logic in detecting fake news on Instagram.
- The approach is advantageous in dealing with the vagueness and complexity of social media content.
- Future research could explore integrating additional features, hybrid models, and real-time detection capabilities to enhance performance further.

This detailed breakdown provides a comprehensive view of the experimental results and how the fuzzy logic approach was implemented and evaluated in the context of fake news detection on Instagram.

5 Conclusion

This study demonstrates the efficacy of a fuzzy logic-based system for detecting fake news on Instagram by combining both supervised and unsupervised learning techniques. The integration of logistic regression, support vector machines, and ensemble methods within the supervised learning framework provided a robust mechanism for classifying Instagram posts. Additionally, the unsupervised approach, leveraging fuzzy logic and clustering algorithms, proved crucial in identifying latent patterns and addressing the inherent vagueness in fake news classification. The experimental results highlighted the system's high accuracy, precision, recall, and F1 scores surpassing traditional methods. This underscores the potential of fuzzy logic systems in enhancing fake news detection capabilities, particularly in handling the complexity and ambiguity associated with social media content. Future research should aim to incorporate more diverse features, hybrid models, and real-time detection capabilities to improve the system's performance and adaptability further. By continuing to develop and refine these techniques, the fight against misinformation on social media platforms like Instagram can be significantly strengthened.

References

1. Bin Naeem, S., Bhatti, R., Khan, A.: An exploration of how fake news is taking over social media and putting public health at risk. Health Info. Libraries J. **38**(2), 143–149 (2021). https://doi.org/10.1111/hir.12320
2. Horner, C.G., Galletta, D., Crawford, J., Shirsat, A.: Emotions: the unexplored fuel of fake news on social media. In: Dennis, A.R., Galletta, D.F., Webster, J. (eds.) Fake News on the Internet, pp. 147–174. Routledge, London (2023). https://doi.org/10.4324/9781003433934-7
3. Xu, S., et al.: Rumor detection on social media using hierarchically aggregated feature via graph neural networks. Appl. Intell. **53**(3), 3136–3149 (2023)
4. Xu, C., Kechadi, M.-T.: Fuzzy deep hybrid network for fake news detection. In: Proceedings of the 12th International Symposium on Information and Communication Technology, pp. 118–125 (2023)
5. Ahmad, I., Yousaf, M., Yousaf, S., Ahmad, M.O.: Fake news detection using machine learning ensemble methods. Complexity **2020**(1), 8885861 (2020)
6. Vijiyakumar, K., Muruganandhan, D., Rajesh, V.: Investigating the fake news using machine learning algorithms. In: 2023 International Conference on System, Computation, Automation and Networking (ICSCAN), IEEE, pp. 1–6 (2023)
7. Sahoo, S.R., Gupta, B.B.: Multiple features based approach for automatic fake news detection on social networks using deep learning. Appl. Soft Comput. **100**, 106983 (2021)
8. Seth, R., Sharaff, A.: Sentiment-aware detection method of fake news based on linguistic fuzzy bi-LSTM. In: 2023 OITS International Conference on Information Technology (OCIT), IEEE, pp. 628–633 (2023)
9. Dheyaa Radhi, A., Al Naffakh, H.A.H., Fuqdan, A.-I., Hakim, B.A., Al-Attar, B.: A comprehensive review of machine learning-based models for fake news detection. BIO Web Conf. **97**, 00123 (2024)
10. Dheyaa Radhi, A., Obeid, H.N., Al-Attar, B., Fuqdan, A.-I., Hakim, B.A., Al Naffakh, H.A.H.: Unmasking deceptive profiles: a deep dive into fake account detection on instagram and twitter. BIO Web Conf. **97**, 00127 (2024). https://doi.org/10.1051/bioconf/20249700127
11. Bhattarai, B., Granmo, O.-C., Jiao, L.: Explainable tsetlin machine framework for fake news detection with credibility score assessment. arXiv Prepr. arXiv2105.09114 (2021)
12. Maheswari, R.U., Sudha, N.: Hybrid Feature extraction and capsule neural network model for fake news detection. Data Metadata **2**, 190 (2023)
13. Riskhan, B., Zhou, K., Muhammad, R.: Energy management of the system: an empirical investigation of virtualization approaches in static and dynamic modes. Inform. Technol. J. **16**(1), 1–10 (2016)
14. Kulkarni, P., Karwande, S., Keskar, R., Kale, P., Iyer, S.: Fake news detection using machine learning. ITM Web Conf. **40**, 03003 (2021)
15. Riskhan, B., Almassri, S.M.H., Hussain, K., Safuan, H.B.A.J.: Publication Frequency (2024)
16. Riskhan, B., Muhammad, R.: Docker in online education: have the near-native performance of CPU, Memory and Network? Int. J. Comput. Theory Eng. **9**(4), 290–293 (2017)
17. Xu, C., Kechadi, M.-T.: An enhanced fake news detection system with fuzzy deep learning. IEEE Access **12**, 88006–88021 (2024). https://doi.org/10.1109/ACCESS.2024.3418340
18. Basheer, R., Hanass, N.N., Sheikh, M.A.U., Hussain, K.: IoT Irrigation System Using Arduino (2024)
19. Mridha, M.F., Keya, A.J., Hamid, M.A., Monowar, M.M., Rahman, M.S.: A comprehensive review on fake news detection with deep learning. IEEE access **9**, 156151–156170 (2021)
20. Kumar, V., Kumar, A., Singh, A.K., Pachauri, A.: Fake news detection using machine learning and natural language processing. In: 2021 International Conference on Technological Advancements and Innovations (ICTAI), IEEE, pp. 547–552 (2021)

21. Gaur, L., Arora, G.K., Jhanjhi, N.Z.: Deep learning techniques for creation of deepfakes. In: Gaur, L. (ed.) DeepFakes: Creation, Detection, and Impact, pp. 23–34. CRC Press, New York (2022). https://doi.org/10.1201/9781003231493-3
22. Dogra, V., Verma, S., Verma, K., Jhanjhi, N.Z., Ghosh, U., Le, D.N.: A comparative analysis of machine learning models for banking news extraction by multiclass classification with imbalanced datasets of financial news: challenges and solutions. Int. J. Interact. Multimed. Artific. Intell. **7**(3), 35 (2022)
23. Dogra, V.: Banking news-events representation and classification with a novel hybrid model using DistilBERT and rule-based features. Turkish J. Comput. Mathemat. Educ. **12**(10), 3039–3054 (2021)
24. Zaheer, A., Tahir, S., Humayun, M., Almufareh, M.F., Jhanjhi, N.Z.: A novel Machine learning technique for fake smart watches advertisement detection. In: 2022 14th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), pp. 1–5. IEEE (2022)

(τ_μ, σ_ν)-semicontinuity and (τ_μ, σ)-semicontinuity

D. Saravanakumar[1](✉), N. Kalaivani[2], and E. Chandrasekaran[2]

[1] Department of Mathematics, St. Joseph University in Tanzania, Dar es Salaam, Tanzania
saravanakumar.dhanabal@sjuit.ac.tz, drdstop@gmail.com
[2] Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R and D Institute of Science and Technology, Chennai, India
{drkalaivani,drchandrasekarane}@veltech.edu.in

Abstract. We define a type of semiopen sets from the concepts of topology and generalized topology. Also, we explore the topological properties through these semi open sets. In addition, we study the related separation axioms and continuous functions using these semiopen sets and discuss their essential basic properties.

Keywords: τ_μ-semiopen sets · τ_μ-semi-$\mathcal{T}_i$ spaces · τ_μ-semi-$\mathcal{D}_i$ spaces · τ_μ, σ_ν-semicontinuous functions · τ_μ, σ-semicontinuous functions

2010 Mathematics Subject Classification: 54C05 · 54C08 · 54C10

1 Introduction

Levine [4] introduced semiopen sets, semi continuity in topological spaces and he identified that the collection of semi open sets is finer than topology. Crossley et al. [1] discussed the concept of semi closure in the semitopological characterizations. Levine [5] initiated the generalized closed sets and In [6, 7, 11, 12, 14], the authors constructed preopen sets, α-open sets and many open sets and described topological classifications. Csaszar [2, 3] created the idea of generalized topology and obtained μ-open sets, μ-ξ-open sets (where "ξ" stands for α, semi, pre and β). Further he defined the operators μ-interior (resp. μ-ξ-interior) and μ-closure (resp. μ-ξ-closure) and initiated generalized continuity such as (μ, ν) (resp. (μ-ξ, ν), (μ-ξ, ν-ξ))-continuous and studied their essential descriptions between the functions through the μ (resp. μ-ξ)-open sets in generalized topological space. Saravanakumar et al. [13] initiated $\widetilde{\mu}$-sets $\widetilde{\mu}$-axioms and generalized topological continuities etc. Peng et al. [8-10] discussed about the topological spaces, fuzzy set theory, operations research, graph networks and mathematical modeling in the book chapters edited by them.

In our article, we represented the combination of topological space (shortly, *TS*) $\mathcal{X}_\tau$ and generalized topological space (shortly, *GTS*) $\mathcal{X}_\mu$ as τ_μ-topological space $\mathcal{X}_{\tau_\mu}$ and from this we defined an open set namely τ_μ-semi open set. Further, we obtained τ_μ-semi-interior and τ_μ-semi-closure operators from the τ_μ-semi open set and described

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 13–23, 2025.
https://doi.org/10.1007/978-3-031-91008-1_2

some topological properties. Also, we defined τ_μ-semi-$\mathcal{T}_i$ spaces, τ_μ-semi-$\mathcal{D}_i$ spaces and analyzed the characterizations through (τ_μ, σ_ν)-semi continuous functions. Moreover, we proved a (τ_μ, σ)-semicontinuous function from the τ_μ-topological space to $\mathcal{T}_2$ space has a (τ_μ, σ)-semi-graph.

2 Preliminaries

For $\mathcal{X}$ ($\neq\emptyset$), we define a generalized topology [2] (shortly, *GT*) on $\mathcal{X}$ is $\mu \subseteq \mathcal{P}(\mathcal{X})$ if $\varnothing \in \mu$, $\mathcal{K}_{\alpha\in J}$ ($\neq\emptyset$) $\in \mu$ and $\bigcup_{\alpha\in J} \mathcal{K}_\alpha \in \mu$. Also $\mathcal{X}_\mu$ is a generalized topological space [2] (shortly, *GTS*) and $\mathcal{M}$ ($\epsilon \mathcal{P}(\mathcal{X})$), $\mathcal{M}^c$ ($= \mathcal{X} \setminus \mathcal{M}$) is a μ-closed [2] set if $\mathcal{M} \in \mu$, $\mathcal{M}$ is μ-open; μ-interior [3] of $\mathcal{M}$ is $i_\mu(\mathcal{M}) = \cup\{\mathcal{K}: \mathcal{K} \in \mu$ and $\mathcal{K} \subseteq \mathcal{M}\}$; μ-closure [3] of $\mathcal{M}$ is $c_\mu(\mathcal{M}) = \cap\{\mathcal{L}: \mathcal{X} \setminus \mathcal{L} \in \mu$ and $\mathcal{M} \subseteq \mathcal{L}\}$. A set $\mathcal{M}$ ($\epsilon \mathcal{P}(\mathcal{X})$) is a μ-semi open [3] (resp. μ-α-open [3], μ-preopen [3], semi open [4]), α-open [7], preopen [6]) set if $c_\mu(i_\mu(\mathcal{M})) \supseteq \mathcal{M}$ (resp. $i_\mu(c_\mu(i_\mu(\mathcal{M}))) \supseteq \mathcal{M}$, $i_\mu(c_\mu(\mathcal{M}))) \supseteq \mathcal{M}$, $c_\tau(i_\tau(\mathcal{M})) \supseteq \mathcal{M}$, $i_\tau(c_\tau(i_\tau(\mathcal{M}))) \supseteq \mathcal{M}$, $i_\tau(c_\tau(\mathcal{M})) \supseteq \mathcal{M}$). Also $\mathcal{X}_{\tau_\mu}$ is a τ_μ-topological space (shortly, τ_μ-*TS*). A set $\mathcal{M}$ ($\epsilon \mathcal{P}(\mathcal{X})$) is a τ_μ-preopen [11] set if $i_\tau(c_\mu(\mathcal{M})) \supseteq \mathcal{M}$. A function $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ is said to be (τ_μ, σ)-precontinuous [11] (or) τ_μ-precontinuous [11] if for any $\mathcal{L} \in \sigma$, $g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{PO}(\mathcal{X})$, where τ_μ-$\mathcal{PO}(\mathcal{X}) = \{\mathcal{M}: \mathcal{M} \subseteq \mathcal{X}$ and $i_\tau(c_\mu(\mathcal{M})) \supseteq \mathcal{M}\}$.

3 τ_μ-semiopen Sets

Definition 3.1. Let $\mathcal{M} \epsilon \mathcal{P}(\mathcal{X})$. We represented (i) τ_μ-$\mathcal{SO}(\mathcal{X}) = \{\tau_\mu$-semiopen $\mathcal{M}: c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{M}\}$;

(ii) τ_μ-$\mathcal{SO}(\mathcal{X}) = \{\tau_\mu$-$\alpha$-open $\mathcal{M}: i_\tau(c_\mu(i_\tau(\mathcal{M}))) \supseteq \mathcal{M}\}$; (iii) τ_μ-$s(\mathcal{X}) = \{\tau_\mu$-$s$-set $\mathcal{M}: c_\mu(i_\tau(\mathcal{M})) = i_\tau(\mathcal{M})\}$.

Remark 3.2. The Example 3.3 illustrates that the concepts of $\mathcal{SO}(\mathcal{X})$, $\mu\mathcal{SO}(\mathcal{X})$ and τ_μ-$\mathcal{SO}(\mathcal{X})$ are not related to each other's.

Example 3.3. Consider $\mathcal{X} = \mathcal{R}$, $\tau = \{\varnothing, \mathcal{R}, (-\infty, 0), (0, 1), (1, \infty), (-\infty, 0) \cup (0, 1), (-\infty, 0) \cup (1, \infty), (0, 1) \cup (1, \infty), (-\infty, 0) \cup (0, 1) \cup (1, \infty)$ and $\mu = \{\emptyset, (0, 5), (4, \infty), (0, \infty)\}$. Then $(0, 2) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$, but $(0, 2) \notin \mathcal{SO}(\mathcal{X})$ (resp $\mu\mathcal{SO}(\mathcal{X})$). Also $(-\infty, 0) \cup \{1\} \in \mathcal{SO}(\mathcal{X})$, but $(-\infty, 0) \cup \{1\} \notin \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ (resp. $\mu\mathcal{SO}(\mathcal{X})$). Moreover $(3, \infty) \in \mu\mathcal{SO}(\mathcal{X})$, but $(3, \infty) \notin \mathcal{SO}(\mathcal{X})$ (resp. τ_μ-$\mathcal{SO}(\mathcal{X})$).

Theorem 3.4. Let $\mu = \tau$. Then the concept of semiopen is same in *TS*, *GTS* and τ_μ-*TS*.

Theorem 3.5. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, we can obtain that (i) τ_μ-$\alpha\mathcal{O}(\mathcal{X}) \supseteq \tau$; (ii) τ_μ-$\mathcal{SO}(\mathcal{X})$ (resp. τ_μ-$\mathcal{PO}(\mathcal{X})) \supseteq \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$;

(iii) τ_μ-$\mathcal{PO}(\mathcal{X}) \cap \tau_\mu$-$\mathcal{SO}(\mathcal{X}) = \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$; (iv) $\tau \supseteq \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \cap \tau_\mu$-$s(\mathcal{X})$.

Proof. (i) Suppose $\mathcal{M} \in \tau$. Then $i_\tau(c_\mu(i_\tau(\mathcal{M}))) = i_\tau(c_\mu(\mathcal{M})) \supseteq i_\tau(\mathcal{M}) = \mathcal{M}$. Thus $\mathcal{M} \in \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$. Concluded τ_μ-$\alpha\mathcal{O}(\mathcal{X}) \supseteq \tau$.

(ii) Suppose $\mathcal{M} \in \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$. Then $c_\mu(i_\tau(\mathcal{M})) \supseteq i_\tau(c_\mu(i_\tau(\mathcal{M}))) \supseteq \mathcal{M}$. Hence $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Again $i_\tau(c_\mu(\mathcal{M})) \supseteq i_\tau(c_\mu(i_\tau(\mathcal{M}))) \supseteq \mathcal{M}$. Hence $\mathcal{M} \in \tau_\mu$-$\mathcal{PO}(\mathcal{X})$. Thus τ_μ-$\mathcal{SO}(\mathcal{X})$ (resp. τ_μ-$\mathcal{PO}(\mathcal{X})) \supseteq \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$.

(iii) By (ii), τ_μ-$\mathcal{PO}(\mathcal{X}) \cap \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \supseteq \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$. Conversely, let $\mathcal{M} \in \tau_\mu$-$\mathcal{PO}(\mathcal{X}) \cap \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Then $c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{M}$ and $i_\tau(c_\mu(\mathcal{M})) \supseteq \mathcal{M}$. This indicates that $i_\tau(c_\mu(i_\tau(\mathcal{M}))) = i_\tau(c_\mu(c_\mu(i_\tau(\mathcal{M})))) \supseteq \mathcal{M}$. Hence $\mathcal{M} \in \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$. Therefore τ_μ-$\alpha\mathcal{O}(\mathcal{X}) \supseteq \tau_\mu$-$\mathcal{PO}(\mathcal{X}) \cap \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

(iv) Suppose $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \cap \tau_\mu$-$s(\mathcal{X})$. Then $i_\tau(\mathcal{M}) = c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{M}$. Hence $\mathcal{M} \in \tau$. Therefore $\tau \supseteq \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \cap \tau_\mu$-$s(\mathcal{X})$.

Remark 3.6. The below content illustrates reverse part of (i) and (ii) in Theorem 3.5 doesn't have to be correct.

From the Example 3.3, $(0, \infty) \notin \tau$, but $(0, \infty) \in \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$. Also $(0, 2)$, $(0, 5) \notin \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X})$, but $(0, 2) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ and $(0, 5) \in \tau_\mu$-$\mathcal{PO}(\mathcal{X})$.

Corollary 3.7. If $\mathcal{X}_{\tau_\mu}$ is a τ_μ-TS, then the concepts of α-open and preopen are same in τ_μ-$TS \Leftrightarrow \tau_\mu$-$\mathcal{PO}(\mathcal{X})$ is the subcollection of τ_μ-$\mathcal{SO}(\mathcal{X})$.

Corollary 3.8. If $\mathcal{X}_{\tau_\mu}$ is a τ_μ-TS, then the concepts of α-open and preopen are same in τ_μ-$TS \Leftrightarrow \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ is the subcollection of τ_μ-$\mathcal{PO}(\mathcal{X})$.

Theorem 3.9. For a τ_μ-TS $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \in \mathcal{P}(\mathcal{X})$, the below declarations are the same:

(i) $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$; (ii) $\exists\, \mathcal{K} \in \tau \ni c_\mu(\mathcal{K}) \supseteq \mathcal{M} \supseteq \mathcal{K}$; (iii) $\exists\, \mathcal{K} \in \tau_\mu$-$\alpha\mathcal{O}(\mathcal{X}) \ni c_\mu(\mathcal{K}) \supseteq \mathcal{M} \supseteq \mathcal{K}$;

(iv) $\exists\, \mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \ni c_\mu(\mathcal{K}) \supseteq \mathcal{M} \supseteq \mathcal{K}$; (v) $c_\mu(\mathcal{M}) = c_\mu(i_\tau(\mathcal{M}))$;

(vi) if $\mathcal{N} \in \mathcal{P}(\mathcal{X}) \ni c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{N} \supseteq \mathcal{M}$, then $\mathcal{N} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

Proof. (i) $\Rightarrow$ (ii). Let $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Then $\mathcal{M} \subseteq c_\mu(i_\tau(\mathcal{M}))$. Take $\mathcal{K} = i_\tau(\mathcal{M})$. Then $\mathcal{K} \in \tau \ni \mathcal{K} \subseteq \mathcal{M} \subseteq c_\mu(\mathcal{K})$.

(ii) $\Rightarrow$ (iii). Obtained from the Theorem 3.5(i) and (ii).

(iii) $\Rightarrow$ (iv). Obtained from the Theorem 3.5(ii) and (iii).

(iv) $\Rightarrow$ (i). Suppose that $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \ni \mathcal{K} \subseteq \mathcal{M} \subseteq c_\mu(\mathcal{K})$. Then $\mathcal{K} \subseteq c_\mu(i_\tau(\mathcal{K}))$ and $\mathcal{M} \subseteq c_\mu(c_\mu(i_\tau(\mathcal{K}))) = c_\mu(i_\tau(\mathcal{K})) \subseteq c_\mu(i_\tau(\mathcal{M}))$. Hence $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

(i) $\Leftrightarrow$ (v). Let $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Then $c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{M}$. This indicates that $c_\mu(\mathcal{M}) \supseteq c_\mu(i_\tau(\mathcal{M})) = c_\mu(c_\mu(i_\tau(\mathcal{M}))) \supseteq c_\mu(\mathcal{M})$. Hence $c_\mu(i_\tau(\mathcal{M})) = c_\mu(\mathcal{M})$. Conversely, suppose that $c_\mu(i_\tau(\mathcal{M})) = c_\mu(\mathcal{M})$. Since $c_\mu(\mathcal{M}) \supseteq \mathcal{M}$, this indicates that $c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{M}$. Thus $\mathcal{M} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

(vi) $\Leftrightarrow$ (i). Suppose that $\mathcal{N} \in \mathcal{P}(\mathcal{X}) \ni c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{N} \supseteq \mathcal{M}$. This indicates that $c_\mu(i_\tau(\mathcal{N})) \supseteq c_\mu(i_\tau(\mathcal{M})) \supseteq \mathcal{N} \supseteq \mathcal{M}$. Thus $c_\mu(i_\tau(\mathcal{N})) \supseteq \mathcal{N}$. Hence $\mathcal{N} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. The converse part is straightforward from (vi).

Theorem 3.10. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-TS and $\{\mathcal{M}_\omega : \omega \in \mathcal{J}\}$ be a subcollection of τ_μ-$\mathcal{SO}(\mathcal{X})$, where $\mathcal{J}$ is an arbitrary index set. Then $\bigcup_{\omega\in\mathcal{J}} \mathcal{M}_\omega \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

Proof. Suppose that $\{\mathcal{M}_\omega : \omega \in \mathcal{J}\} \subseteq \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Then $\mathcal{M}_\omega \subseteq c_\mu(i_\tau(\mathcal{M}_\omega))$ for each $\omega \in \mathcal{J}$ and $\bigcup_{\omega\in\mathcal{J}} \mathcal{M}_\omega \subseteq \cup_{\omega\in\mathcal{J}} \rfloor_\mu(i_\tau(\mathcal{M}_\omega)) \subseteq c_\mu(i_\tau(\bigcup_{\omega\in\mathcal{J}} \mathcal{M}_\omega))$. Hence $\bigcup_{\omega\in\mathcal{J}} \mathcal{M}_\omega \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

Remark 3.11. The below content illustrates that $\mathcal{M} \cap \mathcal{N} \notin \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ if $\mathcal{M}, \mathcal{N} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$.

In Example 3.3, $(0, 2), [1, \infty) \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$, but $(0, 2) \cap [1, \infty) = [1, 2) \notin \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$.

Definition 3.12. In a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, the set $\mathcal{M}$ ($\epsilon\ \mathcal{P}(\mathcal{X})$) is called τ_μ-semiclosed if $\mathcal{X} \setminus \mathcal{M}$ is τ_μ-semiopen in $\mathcal{X}$. We represented $\tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$ is the family of all τ_μ-semiclosed sets.

Theorem 3.13. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that $\mathcal{M} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X}) \Leftrightarrow \mathcal{M} \supseteq i_\mu(c_\tau(\mathcal{M}))$.

Proof. Consider $\mathcal{M} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$. Then $\mathcal{M}^c \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$, this indicates that $\mathcal{X} \setminus i_\mu(c_\tau(\mathcal{M})) \supseteq c_\mu(i_\tau(\mathcal{X} \setminus \mathcal{M})) \supseteq \mathcal{X} \setminus \mathcal{M}$. Therefore $\mathcal{M} \supseteq i_\mu(c_\tau(\mathcal{M}))$. Conversely, suppose that $\mathcal{M} \supseteq i_\mu(c_\tau(\mathcal{M}))$. Then $c_\mu(i_\tau(\mathcal{X} \setminus \mathcal{M})) \supseteq \mathcal{X} \setminus i_\mu(c_\tau(\mathcal{M})) \supseteq \mathcal{X} \setminus \mathcal{M}$ and thus $\mathcal{M}^c \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$. Hence $\mathcal{M} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$.

Theorem 3.14. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, the below conditions are the same:

(i) $\mathcal{M} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$; (ii) $\exists\ \mathcal{K} \in \tau^c \ni \mathcal{K} \supseteq \mathcal{M} \supseteq i_\mu(\mathcal{K})$;

(iii) $\exists\ \mathcal{K} \in \tau_\mu\text{-}\alpha\mathcal{C}(\mathcal{X}) \ni \mathcal{K} \supseteq \mathcal{M} \supseteq i_\mu(\mathcal{K})$;

(iv) $\exists\ \mathcal{K} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X}) \ni \mathcal{K} \supseteq \mathcal{M} \supseteq i_\mu(\mathcal{K})$;

(v) $i_\mu(\mathcal{M}) = i_\mu(c_\tau(\mathcal{M}))$; (vi) if $\mathcal{N} \subseteq \mathrm{X} \ni i_\mu(c_\tau(\mathcal{M})) \subseteq \mathcal{N} \subseteq \mathcal{M}$, then $\mathcal{N} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$.

Theorem 3.15. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\{\mathcal{M}_\alpha{:}\alpha \in \mathrm{J}\}$ be a subcollection of $\tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$, where J is an arbitrary index set. Then $\cap_{\alpha\in \mathrm{J}}\ \mathcal{M}_\alpha \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$.

Remark 3.16. The below content illustrates that $\mathcal{M} \cup \mathcal{N} \notin \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$ if $\mathcal{M}, \mathcal{N} \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$.

In Example 3.3, $(-\infty, 0] \cup [2, \infty), (-\infty, 1) \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$, but $(-\infty, 0] \cup [2, \infty) \cup (-\infty, 1) = (-\infty, 1] \cup [2, \infty) \notin \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$.

Definition 3.17. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M}\ \epsilon\ \mathcal{P}(\mathcal{X})$, (i) τ_μ-semi-interior of $\mathcal{M}$ is $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) = \cup\ \{\mathcal{K}{:}\ \mathcal{K} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and $\mathcal{M} \supseteq \mathcal{K}\}$; (ii) τ_μ-semiclosure of $\mathcal{M}$ is $\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) = \cap\ \{\mathcal{L}{:}$ $\mathcal{X} \setminus \mathcal{L} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and $\mathcal{L} \supseteq \mathcal{M}\}$.

Theorem 3.18. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M}\ \epsilon\ \mathcal{P}(\mathcal{X})$, we can obtain that (i) $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and $\mathcal{M} \supseteq \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$;

(ii) $\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and $\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \supseteq \mathcal{M}$; (iii) $\mathcal{M}$ is τ_μ-semiclosed $\Leftrightarrow \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) = \mathcal{M}$;

(iv) $\mathcal{M}$ is τ_μ-semiopen $\Leftrightarrow \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) = \mathcal{M}$; (v) $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})) = \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$; (vi) $\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}))$ $= \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$;

(vii) $\mathcal{X} \setminus \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) = \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{X} \setminus \mathcal{M})$; (viii) $\mathcal{X} \setminus \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) = \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{X} \setminus \mathcal{M})$.

Theorem 3.19. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M}, \mathcal{N}\ \epsilon\ \mathcal{P}(\mathcal{X})$, we can obtain that (i) $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{N}) \supseteq \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$ if $\mathcal{N} \supseteq \mathcal{M}$;

(ii) $\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{N}) \supseteq \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$ if $\mathcal{N} \supseteq \mathcal{M}$; (iii) $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M} \cup \mathcal{N}) \supseteq \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \cup \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{N})$; (iv) $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$ $\cap\ \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{N}) \supseteq \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M} \cap \mathcal{N})$;

(v) $c^s_{\tau_\mu}(\mathcal{M} \cup \mathcal{N}) \supseteq c^s_{\tau_\mu}(\mathcal{M}) \cup c^s_{\tau_\mu}(\mathcal{N})$; (vi) $c^s_{\tau_\mu}(\mathcal{M}) \cap c^s_{\tau_\mu}(\mathcal{N}) \supseteq c^s_{\tau_\mu}(\mathcal{M} \cap \mathcal{N})$.

Remark 3.20. The below content illustrates the sides of the conditions (iii), (iv), (v) and (vi) in Theorem 3.19 doesn't have to be equal.

Example 3.21. Consider $\mathcal{X} = \{e_1, e_2, e_3, e_4\}$, $\tau = \{\varnothing, \mathcal{X}, \{e_1\}, \{e_2\}, \{e_1, e_2\}, \{e_1,e_2, e_3\}\}$ and $\mu = \{\varnothing, \{e_2\}, \{e_1, e_4\}, \{e_2, e_4\}, \{e_1, e_2, e_4\}\}$. (i) Here $i^s_{\tau_\mu}\{e_1, e_4\} = \{e_1\}$, $i^s_{\tau_\mu}\{e_2, e_4\} = \{e_2\}$, $i^s_{\tau_\mu}\{e_1, e_4\} \cup i^s_{\tau_\mu}\{e_2, e_4\} = \{e_1, e_2\}$, $i^s_{\tau_\mu}(\{e_1, e_4\} \cup \{e_2, e_4\}) = \{e_1, e_2, e_4\}$. Therefore, we have that $i^s_{\tau_\mu}\{e_1, e_4\} \cup i^s_{\tau_\mu}\{e_2, e_4\} \subset i^s_{\tau_\mu}(\{e_1, e_4\} \cup \{e_2, e_4\})$.

(ii) Here $i^s_{\tau_\mu}\{e_1, e_3\} = \{e_1, e_3\}$, $i^s_{\tau_\mu}\{e_2, e_3\} = \{e_2, e_3\}$, $i^s_{\tau_\mu}(\{e_1, e_3\} \cap \{e_2, e_3\}) = \emptyset$, $i^s_{\tau_\mu}\{e_1, e_3\} \cap i^s_{\tau_\mu}\{e_2, e_3\} = \{e_3\}$. Hence $i^s_{\tau_\mu}(\{e_1, e_3\} \cap \{e_2, e_3\}) \subset i^s_{\tau_\mu}\{e_1, e_3\} \cap i^s_{\tau_\mu}\{e_2, e_3\}$.

(iii) Here $c^s_{\tau_\mu}\{e_1\} = \{e_1, e_4\}$, $c^s_{\tau_\mu}\{e_2\} = \{e_2, e_4\}$, $c^s_{\tau_\mu}\{e_1\} \cup c^s_{\tau_\mu}\{n\} = \{e_1, e_2, e_4\}$, $c^s_{\tau_\mu}(\{e_1\} \cup \{e_2\}) = \mathcal{X}$. Hence $c^s_{\tau_\mu}\{e_1\} \cup c^s_{\tau_\mu}\{e_2\} \subset c^s_{\tau_\mu}(\{e_1\} \cup \{e_2\})$.

(iv) Take $\mathcal{M} = \{e_1\}$ and $\mathcal{N} = \{e_2\}$. Then $\mathcal{M} \cap \mathcal{N} = \varnothing$, $c^s_{\tau_\mu}\{e_1\} = \{e_1, e_4\}$, $c^s_{\tau_\mu}\{e_2\} = \{e_2, e_4\}$, $c^s_{\tau_\mu}(\{e_1\} \cap \{e_2\}) = \varnothing$, $c^s_{\tau_\mu}\{e_1\} \cap c^s_{\tau_\mu}\{e_2\} = \{e_4\}$. Hence $c^s_{\tau_\mu}(\{e_1\} \cap \{e_2\}) \subset c^s_{\tau_\mu}\{e_1\} \cap c^s_{\tau_\mu}\{e_2\}$.

Theorem 3.22. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that (i) $\{m \in \mathcal{M}: m \in \mathcal{K} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and $\mathcal{K} \subseteq \mathcal{M}$ for some $\mathcal{K}\} = i^s_{\tau_\mu}(\mathcal{M})$; (ii) $\{m \in \mathrm{X}: m \in \mathcal{L} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and $\mathcal{M} \cap \mathcal{L} \neq \emptyset \forall \mathcal{L}\} = c^s_{\tau_\mu}(\mathcal{M})$.

Theorem 3.23. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that (i) $c_\mu(i_\tau(\mathcal{M})) \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$; (ii) $i_\mu(c_\tau(\mathcal{M})) \in \tau_\mu\text{-}\mathcal{SC}(\mathcal{X})$.

Theorem 3.24. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that (i) $i^s_{\tau_\mu}(\mathcal{M}) = \mathcal{M} \cap c_\mu(i_\tau(\mathcal{M}))$; (ii) $c^s_{\tau_\mu}(\mathcal{M}) = \mathcal{M} \cup i_\mu(c_\tau(\mathcal{M}))$.

Definition 3.25. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, the set $\mathcal{M}$ ($\subseteq \mathcal{X}$) is called τ_μ-semi-neighborhood of a point $m \in \mathcal{X}$ if $\exists\, \mathcal{K}_m \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X}) \ni m \in \mathcal{K}_m \subseteq \mathcal{M}$.

Theorem 3.26. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that $\mathcal{M} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X}) \Leftrightarrow$ it is a τ_μ-semi-neighborhood of each of its points.

4 τ_μ-semi-$\mathcal{T}_i$ Spaces and τ_μ-semi-$\mathcal{D}_i$ Spaces

Definition 4.1. A τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_0$ if for each $m \neq n$, $m, n \in \mathcal{X}$, $\exists$ a set $\mathcal{K} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X}) \ni$ either $n \notin \mathcal{K}$ and $m \in \mathcal{K}$ or $m \notin \mathcal{K}$ and $n \in \mathcal{K}$.

Definition 4.2. A τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_1$ if for each $m \neq n$, $m, n \in \mathcal{X}$, $\exists$ sets $\mathcal{K}, \mathcal{L} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ containing m and n respectively $\ni n \notin \mathcal{K}$ and $m \notin \mathcal{L}$.

Definition 4.3. A τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_2$ if for each $m, n \in \mathcal{X}$, $m \neq n$, $\exists$ sets $\mathcal{K}, \mathcal{L} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X}) \ni n \in \mathrm{L}$, $m \in \mathcal{K}$ and $\mathcal{L} \cap \mathcal{K} = \varnothing$.

Definition 4.4. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and the set $\mathcal{M} \in \mathcal{P}(\mathcal{X})$, we represented $\tau_\mu\text{-}\mathcal{SGC}(\mathcal{X}) = \{\tau_\mu$-sg-closed $\mathcal{M}$: $c^s_{\tau_\mu}(\mathcal{M}) \subseteq \mathcal{K}$ when $\mathcal{M} \subseteq \mathcal{K}$ and $\mathcal{K} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})\}$.

Note that τ_μ-$\mathcal{SGC}(\mathcal{X}) \supseteq \tau_\mu$-$\mathcal{SC}(\mathcal{X})$, but the reverse case need not be true.

Definition 4.5. A τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_{\frac{1}{2}}$ if τ_μ-$\mathcal{SGC}(\mathcal{X}) = \tau_\mu$-$\mathcal{SC}(\mathcal{X})$.

Theorem 4.6. In a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, for a point $m \in \mathcal{X}$, $\mathrm{m} \in \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \Leftrightarrow \mathcal{L} \cap \mathcal{M} \neq \emptyset$ for any $\mathcal{L} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \ni m \in \mathcal{L}$.

Theorem 4.7. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that $\mathcal{M} \in \tau_\mu$-$\mathcal{SGC}(\mathcal{X}) \Leftrightarrow \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\{m\}) \cap \mathcal{M} \neq \emptyset$ holds for every $m \in \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$.

Theorem 4.8. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} \subseteq \mathcal{X}$, we can obtain that $\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\{m\}) \cap \mathcal{M} \neq \emptyset$ for every $m \in \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \Leftrightarrow \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \subseteq \mathrm{k}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$ holds, where $\mathrm{k}^{\mathrm{s}}_{\tau_\mu}(\mathcal{E}) = \cap \{\mathcal{L}\colon \mathcal{L} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ and $\mathcal{L} \supseteq \mathcal{E} \forall \mathcal{E} \subseteq \mathcal{X}\}$.

Theorem 4.9. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and $\mathcal{M} (\subseteq \mathcal{X}) \in \tau_\mu$-$\mathcal{SGC}(\mathcal{X})$, we can obtain that $\mathcal{E} \not\subset \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}) \setminus \mathcal{M}$, where $\mathcal{E} \neq \varnothing$ and $\mathcal{E} \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$.

Theorem 4.10. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ and for each $m \in \mathcal{X}$, we can obtain that $\{m\} \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$ or $\mathrm{X} \setminus \{m\} \in \tau_\mu$-$\mathcal{SGC}(\mathcal{X})$.

Theorem 4.11. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, we can obtain that $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathrm{T}_{\frac{1}{2}} \Leftrightarrow$ for each $m \in \mathcal{X}$, $\{m\} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ or $\{m\} \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$.

Theorem 4.12. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, we can obtain that $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_1 \Leftrightarrow$ for any $m \in \mathcal{X}$, $\{m\} \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$.

Remark 4.13. From the Theorems 4.10, 4.11, 4.12, τ_μ-semi-$\mathcal{T}_2 \Rightarrow \tau_\mu$-semi-$\mathcal{T}_1 \Rightarrow \tau_\mu$-semi-$\mathcal{T}_{\frac{1}{2}} \Rightarrow \tau_\mu$-semi-$\mathcal{T}_0$.

The following contents illustrates that the reverse implication does not have to be true.

Example 4.14. Consider $\mathcal{X} = \{e_1, e_2, e_3, e_4\}$, $\tau = \{\varnothing, \mathcal{X}, \{e_1\}, \{e_2,e_4\}, \{e_1, e_2, e_4\}\}$ and $\mu = \{\varnothing, \{e_4\}, \{e_3, e_4\}, \{e_1, e_2, e_4\}, \{e_1, e_3, e_4\}\}$. By Definition 4.1, the τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_0$. Also $\{e_2, e_3\} \in \tau_\mu$-$\mathcal{SGC}(\mathcal{X})$, but $\{e_2, e_3\} \notin \tau_\mu$-$\mathcal{SC}(\mathcal{X})$. Then by Definition 4.5, $\mathcal{X}_{\tau_\mu}$ is not τ_μ-semi-$\mathcal{T}_{\frac{1}{2}}$.

Example 4.15. Consider $\mathcal{X} = \{e_1, e_2, e_3, e_4\}$, $\tau = \{\varnothing, \mathcal{X}, \{e_2\}, \{e_1, e_2\}, \{e_1, e_2, e_4\}\}$ and $\mu = \{\varnothing, \{e_1\}, \{e_1, e_2\}, \{e_2, e_3\}, \{e_1, e_2, e_3\}\}$. Clearly the τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_{\frac{1}{2}}$, but not τ_μ-semi-$\mathcal{T}_1$; since $e_1, e_2 \in \mathcal{X}$, $e_1 \neq e_2$; the sets $\mathcal{X}$, $\{e_1, e_2\}$, $\{e_1, e_2, e_3\}$, $\{e_1, e_2, e_4\} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ and contains both the points e_1 and e_2.

Example 4.16. Consider $\mathcal{X} = \{e_1, e_2, e_3, e_4\}$, $\tau = \{\varnothing, \mathcal{X}, \{e_1, e_2\}, \{e_3, e_4\}\}$ and $\mu = \{\varnothing, \{e_1, e_2, e_3\}, \{e_1, e_3, e_4\}\}$. Clearly the τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_1$, but not τ_μ-semi-$\mathcal{T}_2$; since $e_1, e_2 \in \mathcal{X}, e_1 \neq e_2$; we cannot find disjoint τ_μ-semiopen sets for the distinct points e_1 and e_2.

Definition 4.17. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, the set $\mathcal{M} (\subseteq \mathcal{X})$ is called τ_μ-semi-$\mathcal{D}$ if $\exists$ two sets $\mathcal{K}$, $\mathcal{L} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X}) \ni \mathcal{K} \neq \mathcal{X}$ and $\mathcal{M} = \mathcal{K} \setminus \mathcal{L}$.

Remark 4.18. If $\mathcal{K} (\neq \mathcal{X}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$, then $\mathcal{K}$ is τ_μ-semi-$\mathcal{D}$.

Proof. Consider $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ and $\mathcal{K} \neq \mathcal{X}$. Also $\mathcal{K} = \mathcal{K} \setminus \varnothing$ and $\varnothing \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. By Definition 4.17, $\mathcal{K}$ is τ_μ-semi-$\mathcal{D}$.

The below content illustrates that the reverse part of the Remark 4.18 does not have to be true.

In Example 3.3, $[1, \infty), (1, \infty) \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$. Take $[1, \infty) \setminus (1, \infty) = \{1\}$. Hence $\{1\}$ is a τ_μ-semi-$\mathcal{D}$ set, but $\{1\} \notin \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$.

Definition 4.19. A τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is (i) τ_μ-semi-$\mathcal{D}_0$ if for each $m, n \in \mathcal{X}$, $m \neq n$, $\exists$ a τ_μ-semi-$\mathcal{D}$ set $\mathcal{K} \ni$ either $n \notin \mathcal{K}$ and $m \in \mathcal{K}$ or $m \notin \mathcal{K}$ and $n \in \mathcal{K}$; (ii) τ_μ-semi-$\mathcal{D}_1$ if for each $m \neq n$, $m, n \in \mathcal{X}$, $\exists$ τ_μ-semi-$\mathcal{D}$ sets $\mathcal{K}$ and $\mathcal{L}$ contain m and n respectively $\ni n \notin \mathcal{K}$ and $m \notin \mathcal{L}$; (iii) τ_μ-semi-$\mathcal{D}_2$ if for each $m \neq n$, $m, n \in \mathcal{X}$, $\exists$ τ_μ-semi-$\mathcal{D}$ sets $\mathcal{K}$ and $\mathcal{L} \ni m \in \mathcal{K}$ and $n \in \mathcal{L}$ and $\mathcal{K} \cap \mathcal{L} = \varnothing$.

Remark 4.20. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, we can obtain that $\mathcal{X}_{\tau_\mu}$ is (i) τ_μ-semi-$\mathcal{D}_i \Rightarrow \tau_\mu$-semi-$\mathcal{D}_{i-1}$ for i= 1, 2;

(ii) τ_μ-semi-$\mathcal{T}_i \Rightarrow \tau_\mu$-semi-$\mathcal{D}_i$ for i = 0, 1, 2.

Theorem 4.21. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, we can obtain that $\mathcal{X}_{\tau_\mu}$ is (i) τ_μ-semi-$\mathcal{D}_0 \Leftrightarrow \tau_\mu$-semi-$\mathcal{T}_0$;

(ii) τ_μ-semi-$\mathcal{D}_2 \Leftrightarrow \tau_\mu$-semi-$\mathcal{D}_1$.

Theorem 4.22. If $\mathcal{X}_{\tau_\mu}$ is a τ_μ-*TS*, then τ_μ-semi-$\mathcal{D}_1 \Rightarrow \tau_\mu$-semi-$\mathcal{T}_0$.

Remark 4.23. The below content illustrates that the reverse part of the Theorem 4.22 does not have to be true.

Example 4.24. Let $\mathcal{X} = \{e_1, e_2, e_3, e_4\}$, $\tau = \{\varnothing, \mathcal{X}, \{e_2\}, \{e_1, e_2\}, \{e_1, e_2, e_3\}\}$ and $\mu = \{\varnothing, \mathcal{X}, \{e_3, e_4\}, \{e_1, e_2, e_3\}, \{e_2, e_3, e_4\}\}$. Clearly the τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ is τ_μ-semi-$\mathcal{T}_0$, but not τ_μ-semi-$\mathcal{D}_1$; since $e_1, e_4 \in \mathcal{X}$, $e_1 \neq e_4$; the set $\mathcal{X} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$ and contains both the points e_1 and e_4.

Definition 4.25. For a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, a point $m \in \mathcal{X}$ is called τ_μ-semi-neat if there does not exist any τ_μ-semiopen set containing m other than $\mathcal{X}$.

In Example 4.24, the point d is τ_μ-semi-neat, because d has a τ_μ-semiopen set $\mathcal{X}$ itself.

Theorem 4.26. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS*. Then $\mathcal{X}$ is τ_μ-semi-$\mathcal{D}_1 \Leftrightarrow \mathcal{X}$ has no τ_μ-semi-neat point.

Remark 4.27. For a τ_μ-*TS*$\mathcal{X}_{\tau_\mu}$, we can obtain that $\mathcal{X}$ is τ_μ-semi-$\mathcal{T}_0$ but not τ_μ-semi-$\mathcal{D}_1$ $\Leftrightarrow \exists$ a unique τ_μ-semi-neat point in$\mathcal{X}$. If m and n are both τ_μ-semi-neat points in $\mathcal{X}$ then we can say $m \in \mathcal{K} \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$, but $n \notin \mathcal{K}$. This is a conflict since $\mathcal{K} \neq \mathcal{X}$.

Definition 4.28. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_{\sigma_\nu}$ be a σ_ν-*TS*. A function $g\colon \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_{\sigma_\nu}$ is said to be (τ_μ, σ_ν)-semicontinuous if for any $\mathcal{L} \in \sigma_\nu\text{-}\mathcal{SO}(\mathcal{Y})$, $g^{-1}(\mathcal{L}) \in \tau_\mu\text{-}\mathcal{SO}(\mathcal{X})$.

Example 4.29. Let $\mathcal{X} = \mathcal{Y} = \mathcal{R}$, $\tau = \left\{\varnothing, \mathcal{R}, \left(\frac{-1}{n}, \frac{1}{n}\right)_{n \in Z_+}\right\}$, $\sigma = \{\varnothing, \mathcal{R}, (-1, 1)\}$, $\mu = \{\varnothing, (-\infty, 0), (0, \infty), (-\infty, 0) \cup (0, \infty)\}$ and $\nu = \{\varnothing, (-\infty, -1), (1, \infty), (-\infty, -1) \cup (1, \infty)\}$. Consider a function $g\colon \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_{\sigma_\nu}$, by $g(m) = \frac{m}{n}$, $\forall m \in R$. Then g is (τ_μ, σ_ν)-semi continuous.

Theorem 4.30. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_{\sigma_\nu}$ be a σ_ν-*TS*. If $\}\colon \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_{\sigma_\nu}$ is a (τ_μ, σ_ν)-semicontinuous onto function and $\mathcal{E}$ $(\subseteq \mathcal{Y})$ is a σ_ν-semi-$\mathcal{D}$ set, then $g^{-1}(\mathcal{E})$ $(\subseteq \mathcal{X})$ is a τ_μ-semi-$\mathcal{D}$ set.

Proof. Consider $\mathcal{E}$ ($\subseteq \mathcal{Y}$) is σ_ν-semi-$\mathcal{D}$. Clearly $\exists$ sets $\mathcal{K}, \mathcal{L} \in \sigma_\nu$-$\mathcal{SO}(\mathcal{Y}) \ni \mathcal{E} = \mathcal{K} \setminus \mathcal{L}$, $\mathcal{K} \neq \mathcal{Y}$. Since g is a (τ_μ, σ_ν)-semi continuous function, $g^{-1}(\mathcal{K}), g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Since $\mathcal{K} \neq \mathcal{Y}$, indicates that $\mathcal{X} \neq g^{-1}(\mathcal{K})$. Therefore $g^{-1}(\mathcal{K}) \setminus g^{-1}(\mathcal{L}) = g^{-1}(\mathcal{E})$ is τ_μ-semi-$\mathcal{D}$.

Theorem 4.31. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_{\sigma_\nu}$ be a σ_ν-*TS*. Then $\mathcal{X}$ is τ_μ-semi-$\mathcal{D}_1$ if g: $\mathcal{X}_{\tau_\mu} \to \mathcal{Y}_{\sigma_\nu}$ is a (τ_μ, σ_ν)-semicontinuous, one to one, onto function and $\mathcal{Y}$ is σ_ν-semi-$\mathcal{D}_1$.

Proof. Consider $\mathcal{Y}$ is σ_ν-semi-$\mathcal{D}_1$. Let $m, n \in \mathcal{X}$, $m \neq n$. Since $\mathcal{Y}$ is σ_ν-semi-$\mathcal{D}_1$ and g is one to one and by Theorem 4.30, $\mathcal{G}$ and $\mathcal{H}$ of $\mathcal{Y}$ are σ_ν-semi-$\mathcal{D}$ sets, $g(m) \in \mathcal{G}$, ($\notin \mathcal{H}$), $g(n) \in \mathcal{H}$, ($\notin \mathcal{G}$) and τ_μ-semi-$\mathcal{D}$ sets $g^{-1}(\mathcal{G})$, $g^{-1}(\mathcal{H})$ in $\mathcal{X}$, $m \in g^{-1}(\mathcal{G})$ and $n \in g^{-1}(\mathcal{H})$. Thus $\mathcal{X}$ is τ_μ-semi-$\mathcal{D}_1$.

Theorem 4.32. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_{\sigma_\nu}$ be a σ_ν-*TS*. Then $\mathcal{X}$ is τ_μ-semi-$\mathcal{D}_1 \Leftrightarrow$ for each$m, n \in \mathcal{X}$, $m \neq n$, $\exists$ a (τ_μ, σ_ν)-semicontinuous onto function g: $\mathcal{X}_{\tau_\mu} \to \mathcal{Y}_{\sigma_\nu}$ where $\mathcal{Y}$ is σ_ν-semi-$\mathcal{D}_1 \ni \mathcal{Y}$ containing the distinct points $g(m)$, $g(n)$.

5 (τ_μ, σ)-semicontinuous Functions

Definition 5.1. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a*TS*. A function g: $\mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ is said to be (τ_μ, σ)-semicontinuous if for any $\mathcal{L} \in \sigma$, $g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

Remark 5.2. From the definition of continuous and the Definitions 4.28 and 5.1, every continuous (resp. (τ_μ, σ_ν)-semicontinuous) function is (τ_μ, σ)-semicontinuous. But the below example illustrates that the reverse part does not have to be true.

Example 5.3. Consider $\mathcal{X} = \mathcal{Y} = \mathcal{R}$, $\tau = \{\varnothing, \mathcal{R}, (2, 3)\}$, $\sigma = \{\varnothing, \mathcal{R}, (0, 1), (-1, 1)\}$, $\mu = \{\varnothing, (-\infty, 1), (3, \infty), (-\infty, 1) \cup (3, \infty)\}$ and $\nu = \{\varnothing, (-\infty, 5), (5, \infty), (-\infty, 5) \cup (5, \infty)\}$. Consider a function g: $\mathcal{X}_{\tau_\mu} \to \mathcal{Y}_{\sigma_\nu}$, by $g(\mathrm{m}) = \mathrm{m} - 2$, $\forall \mathrm{m} \in \mathcal{R}$. Then g is (τ_μ, σ)-semicontinuous, but not continuous. Since $(-1, 1) \in \sigma$, but $g^{-1}((-1, 1)) = (1, 3) \notin \tau$. Also g is not (τ_μ, σ_ν)-semicontinuous, since $(-2, 4) \in \sigma_\nu$-$\mathcal{SO}(\mathcal{Y})$, but $g^{-1}((-2, 4)) = (0, 6) \notin \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

Definition 5.4. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a*TS*. A function g: $\mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ is called (τ_μ, σ)-*s*-continuous (resp. (τ_μ, σ)-α-continuous, (τ_μ, σ)-precontinuous [11]) if for any $\mathcal{L} \in \sigma$, $g^{-1}(\mathcal{L}) \in \tau_\mu$-*s*(X) (resp. τ_μ-α$\mathcal{O}(\mathcal{X})$, τ_μ-$\mathcal{PO}(\mathcal{X})$).

Theorem 5.5. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a *TS* and g: $\mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ be a function. Then

(i) (τ_μ, σ)-α-continuous function $\Rightarrow$ (τ_μ, σ)-semicontinuous;

(ii) (τ_μ, σ)-α-continuous function $\Rightarrow$ (τ_μ, σ)-precontinuous;

(iii) (τ_μ, σ)-semicontinuous and (τ_μ, σ)-*s*-continuous function $\Rightarrow$ continuous.

Theorem 5.6. Let g be a function from a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ into a *S* $\mathcal{Y}_\sigma$. Then we have the below conditions are the same:

(i) g is (τ_μ, σ)-semicontinuous; (ii) for each $m \in \mathcal{X}$, $g(m) \in \mathcal{L} \in \sigma$, $\exists$ a set $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ containing $m \ni g(\mathcal{K}) \subseteq \mathcal{L}$. (i.e.) g is (τ_μ, σ)-semicontinuous at each point $m \in \mathcal{X}$; (iii) $g^{-1}(\mathcal{F}) \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$ if $\mathcal{F} \in \sigma^c$; (iv) $g^{-1}(c_\tau(\mathcal{N})) \supseteq c^s_{\tau_\mu}(g^{-1}(\mathcal{N}))$, for each $\mathcal{N} \subseteq$

$\mathcal{Y}$; (v) $c_\tau(g(\mathcal{M})) \supseteq g(\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}))$, for each $\mathcal{M} \subseteq \mathcal{X}$; (vi) $\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(\mathcal{N})) \supseteq g^{-1}(i_\tau(\mathcal{N}))$, for each $\mathcal{N} \subseteq \mathcal{Y}$; (vii) $g^{-1}(c_\tau(\mathcal{N})) \supseteq i_\mu(c_\tau(g^{-1}(\mathcal{N})))$, for each $\mathcal{N} \subseteq \mathcal{Y}$; (viii) $c_\tau(g(\mathcal{M})) \supseteq g(i_\mu(c_\tau(\mathcal{M})))$, for each $\mathcal{M} \subseteq \mathcal{X}$.

Proof. (i) $\Leftrightarrow$ (ii). Take $m \in \mathcal{X}$ and $\mathcal{L} \in \sigma$ containing $g(m)$. Then by (i), $g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Take $\mathcal{K} = g^{-1}(\mathcal{L})$. Therefore, $m \in \mathcal{K}$ and $g(\mathcal{K}) \subseteq \mathcal{L}$. Conversely, suppose that $m \in \mathcal{X}$ and $g(m) \in \mathcal{L} \in \sigma$. Then by (ii), $\exists$ a set $\mathcal{K}_m \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ containing $m \ni g(\mathcal{K}_m) \subseteq \mathcal{L}$. This indicates that $\mathcal{K}_m \subseteq g^{-1}(\mathcal{L})$. Thus $\cup \{\mathcal{K}_m : m \in g^{-1}(\mathcal{L})\} = g^{-1}(\mathcal{L})$. Thus by Theorem 3.10, $g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

(i) $\Leftrightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (iv). Let $\mathcal{N} \subseteq \mathcal{Y}$ and $g^{-1}(c_\tau(\mathcal{N})) \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$. Then $g^{-1}(c_\tau(\mathcal{N})) \supseteq \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(c_\tau(\mathcal{N}))) \supseteq \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(\mathcal{N}))$.

(iv) $\Rightarrow$ (v). Let $\mathcal{M} \subseteq \mathcal{X}$. Then $g(\mathcal{M}) \subseteq \mathcal{Y}$ and by (iv), we obtained that $g^{-1}(c_\tau(g(\mathcal{M}))) \supseteq \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(g(\mathcal{M}))) \supseteq \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M})$. Thus $c_\tau(g(\mathcal{M})) \supseteq g(\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(\mathcal{M}))$.

(v) $\Rightarrow$ (iii). Let $\mathcal{F} \in \sigma^{\mathrm{c}}$. Then by (v), we have that $\mathcal{F} = c_\tau(\mathcal{F}) \supseteq c_\tau(g(g^{-1}(\mathcal{F}))) \supseteq g(\mathrm{c}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(\mathcal{F})))$. Thus $g^{-1}(\mathcal{F}) \supseteq \mathrm{c}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(\mathcal{F}))$. Therefore $g^{-1}(\mathcal{F}) \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$.

(i) $\Leftrightarrow$ (vi). Let $\mathcal{N} \subseteq \mathcal{Y}$. Then $g^{-1}(i_\tau(\mathcal{N})) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Hence $g^{-1}(i_\tau(\mathcal{N})) = \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(i_\tau(\mathcal{N}))) \subseteq \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(\mathcal{N}))$. Conversely, let $\mathcal{L} \in \sigma$. Then $g^{-1}(\mathcal{L}) = g^{-1}(i_\tau(\mathcal{L})) \supseteq \mathrm{i}^{\mathrm{s}}_{\tau_\mu}(g^{-1}(\mathcal{L}))$. Therefore $g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$.

(iii) $\Rightarrow$ (vii). Let $\mathcal{N} \subseteq \mathcal{Y}$. Then $c_\tau(\mathcal{N}) \in \sigma^{\mathrm{c}}$ and by (i), $g^{-1}(c_\tau(\mathcal{N})) \in \tau_\mu$-$\mathcal{SC}(\mathcal{X})$. This indicates that $\mathcal{X} \setminus g^{-1}(c_\tau(\mathcal{N})) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ and we have that $\mathcal{X} \setminus i_\mu(c_\tau(g^{-1}(\mathcal{N}))) = c_\mu(i_\tau(\mathcal{X} \setminus g^{-1}(c_\tau(\mathcal{N})))) \supseteq \mathcal{X} \setminus g^{-1}(c_\tau(\mathcal{N}))$. Hence $g^{-1}(c_\tau(\mathcal{N})) \supseteq i_\mu(c_\tau(g^{-1}(\mathcal{N})))$.

(vii) $\Rightarrow$ (viii). Let $\mathcal{M} \subseteq \mathcal{X}$. Then by (vii), $g^{-1}(c_\tau(g(\mathcal{M}))) \supseteq i_\mu(c_\tau(g^{-1}(g(\mathcal{M})))) \supseteq i_\mu(c_\tau(\mathcal{M}))$ and hence $c_\tau(g(\mathcal{M})) \supseteq g(i_\mu(c_\tau(\mathcal{M})))$.

(viii) $\Rightarrow$ (i). Let $\mathcal{L} \in \sigma$. Then $\mathcal{Y} \setminus \mathcal{L} \in \sigma^{\mathrm{c}}$, $g^{-1}(\mathcal{Y} \setminus \mathcal{L}) \subseteq \mathcal{X}$ and by (viii), $\mathcal{Y} \setminus \mathcal{L} = c_\tau(\mathcal{Y} \setminus \mathcal{L}) \supseteq \mathrm{c}_\tau(g(g^{-1}(\mathcal{Y} \setminus \mathcal{L}))) \supseteq g(i_\mu(c_\tau(g^{-1}(\mathcal{Y} \setminus \mathcal{L}))))$. Therefore $\mathcal{X} \setminus g^{-1}(\mathcal{L}) = g^{-1}(\mathcal{Y} \setminus \mathcal{L}) \supseteq i_\mu(c_\tau(g^{-1}(\mathcal{Y} \setminus \mathcal{L}))) = i_\mu(c_\tau(\mathcal{X} \setminus g^{-1}(\mathcal{L}))) = \mathcal{X} \setminus c_\mu(i_\tau(g^{-1}(\mathcal{L})))$, this indicates that $c_\mu(i_\tau(g^{-1}(\mathcal{L}))) \supseteq g^{-1}(\mathcal{L})$. Hence $g^{-1}(\mathcal{L}) \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$. Thus g is (τ_μ, σ)-semicontinuous.

Theorem 5.7. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a *TS* and $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ be a function. Then g is (τ_μ, σ)-semicontinuous $\Leftrightarrow$ for each $\mathcal{L} \subseteq \mathcal{Y}$, $g^{-1}(i_\tau(\mathcal{L})) \subseteq c_\mu(i_\tau(g^{-1}(\mathcal{L})))$.

Theorem 5.8. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a *TS* and $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ be a one to one, onto function. Then g is (τ_μ, σ)-semicontinuous $\Leftrightarrow$ $i_\tau(g(\mathcal{K})) \subseteq g(\mathrm{i}^{\mathrm{s}}_{\tau_\mu}(\mathcal{K}))$ for each $\mathcal{K} \subseteq \mathcal{X}$.

Theorem 5.9. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS*, $\mathcal{Y}_\sigma$ and $\mathcal{Z}_\eta$ be two *TS*s. If $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ is a (τ_μ, σ)-semicontinuous function and $e: \mathcal{Y}_\sigma \to \mathcal{Z}_\eta$ is a continuous function, then $eog: \mathcal{X}_{\tau_\mu} \to \mathcal{Z}_\eta$ is (τ_μ, η)-semicontinuous.

Theorem 5.10. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a $\mathcal{T}_{\mathrm{i}}$ space and $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ be a (τ_μ, σ)-semicontinuous one to one function. Then $\mathcal{X}$ is τ_μ-semi-$\mathcal{T}_{\mathrm{i}}$, where $\mathrm{i} = 0, 1, 2$.

Definition 5.11. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS* and $\mathcal{Y}_\sigma$ be a*TS*. A function $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ is said to have a (τ_μ, σ)-semi-graph (τ_μ, σ)-$\mathcal{SG}(g)$ if for each $(m, n) \in (\mathcal{X} \times \mathcal{Y}) \setminus (\tau_\mu, \sigma)$-$\mathcal{SG}(g)$,

$\exists$ a set $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$, $m \in \mathcal{K}$ and a set $\mathcal{L} \in \sigma$ containing $n \ni (\mathcal{K} \times \mathcal{L}) \cap (\tau_\mu, \sigma)$-$\mathcal{SG}(g) = \varnothing$, where (τ_μ, σ)-$\mathcal{SG}(g) = \{(m, g(m)): m \in \mathcal{X}\}$.

Lemma 5.12. If $g: \mathcal{X}_{\tau_\mu} \to \mathcal{Y}_\sigma$ has a (τ_μ, σ)-semi-graph $\Leftrightarrow$ for each $(m,n) \in \mathcal{X} \times \mathcal{Y}$ with $n \neq g(m)$, $\exists$ a set $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ and a set $\mathcal{L} \in \sigma$, $m \in \mathcal{K}$, $n \in \mathcal{L} \ni g(\mathcal{K}) \cap \mathcal{L} = \varnothing$.

Theorem 5.13. Let g be a (τ_μ, σ)-semicontinuous function from a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ into a $\mathcal{T}_2$ space $\mathcal{Y}_\sigma$. Then g has a (τ_μ, σ)-semi-graph.

Definition 5.14. In a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$, the set $\mathcal{M}$ $(\epsilon\ \mathcal{P}(\mathcal{X}))$ is τ_μ-semi-compact if every τ_μ-semiopen cover of $\mathcal{M}$ has a finite subcover.

Theorem 5.15. If g has a (τ_μ, σ)-semi-graph from a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ into a *TS* $\mathcal{Y}_\sigma$, then $g(\mathcal{K}) \in \sigma^c$, where $\mathcal{K}$ is τ_μ-semi-compact and $\mathcal{K} \subseteq \mathcal{X}$.

Definition 5.16. Let $\mathcal{X}_{\tau_\mu}$ be a τ_μ-*TS*. Then the τ_μ-semi-frontier of $\mathcal{M}$ $(\subseteq \mathcal{X})$ is represented by $\mathrm{Fr}^s_{\tau_\mu}(\mathcal{M}) = \mathrm{c}^s_{\tau_\mu}(\mathcal{X} \setminus \mathcal{M}) \cap \mathrm{c}^s_{\tau_\mu}(\mathcal{M})$.

Theorem 5.17. Let g be a function from a τ_μ-*TS* $\mathcal{X}_{\tau_\mu}$ into a $S\mathcal{Y}_\sigma$. Then we have the below conditions are the same: (i) g is not (τ_μ, σ)-semicontinuous at$m$; (ii) $m \in \cup \{\mathrm{Fr}^s_{\tau_\mu}(g^{-1}(\mathcal{L})): \mathcal{V} \in \sigma, g(m) \in \mathcal{L}\}$;

(iii) $\exists$ a set $\mathcal{L} \in \sigma$, $g(m) \in \mathcal{L} \ni m \in \mathrm{Fr}^s_{\tau_\mu}(g^{-1}(\mathcal{L}))$.

Proof. (i) $\Rightarrow$ (ii). Let us assume that g is not (τ_μ, σ)-semicontinuous at $m \in \mathcal{X}$. Then $\exists$ a set $\mathcal{L} \in \sigma$, $g(m) \in \mathcal{L} \ni$ for every $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ containing m, $\mathcal{K} \cap (\mathcal{X} \setminus g^{-1}(\mathcal{L})) \neq \varnothing$. Thus $m \in \mathrm{c}^s_{\tau_\mu}(\mathcal{X} \setminus g^{-1}(\mathcal{L}))$. Also $m \in g^{-1}(\mathcal{L}) \subseteq \mathrm{c}^s_{\tau_\mu}(g^{-1}(\mathcal{L}))$. Thus $m \in \mathrm{Fr}^s_{\tau_\mu}(g^{-1}(\mathcal{L}))$ where $\mathcal{L} \in \sigma$ containing $g(m)$.

(ii) $\Rightarrow$ (iii). Obvious.

(iii) $\Rightarrow$ (i). Consider g is (τ_μ, σ)-semicontinuous at $m \in \mathcal{X}$ and any set $\mathcal{L} \in \sigma$, $g(m) \in \mathcal{L}$. Then $\exists$ a set $\mathcal{K} \in \tau_\mu$-$\mathcal{SO}(\mathcal{X})$ containing $m \ni g(\mathcal{K}) \subseteq \mathcal{L}$. Thus $m \in \mathcal{K} \subseteq g^{-1}(\mathcal{L})$ and we obtained that $m \in \mathrm{i}^s_{\tau_\mu}(g^{-1}(\mathcal{L})) \subseteq \mathcal{X} \setminus \mathrm{Fr}^s_{\tau_\mu}(g^{-1}(\mathcal{L}))$. Therefore $m \notin \mathrm{Fr}^s_{\tau_\mu}(g^{-1}(\mathcal{L}))$.

References

1. Crossly, S.G., Hildebrand, S.K.: Semi-topological properties. Fund. Math. **74**, 233–254 (1974)
2. Csaszar, A.: Generalized open sets. Acta Math Hunger. **75**, 65–87 (1997)
3. Csaszar, A.: Generalized open sets in generalized topologies. Acta Math. Hungar. **105**, 53–66 (2005)
4. Levine, N.: Semiopen sets and semi continuity in topological spaces. Am. Mat. Month. **70**, 36–41 (1963)
5. Levine, N.: Generalized closed sets in topology. Rend. Circ. Mat. Palermo **19**, 89–96 (1970)
6. Mashhour, A.S., Abd El-Monsef, M.E., El-Deeb, S.N.: On precontinuous and weak precontinuous mappings. Proc. Math. Phys. Soc. Egypt **53**, 47–53 (1982)
7. Njastad, O.: On some classes of nearly open sets, Pacific. J. Math. **15**, 961–970 (1965)
8. Peng, S.L., Hao, R.X., Pal, S. (eds.): Proceedings of First ICMMS, Advances in Intelligent Systems and Computing, Springer Singapore 2021. https://doi.org/10.1007/978-981-33-4389-4

9. Peng, S.L., Hao, R.X., Pal, S. (eds.): Proceedings of 2nd ICMMCS, Advances in Intelligent Systems and Computing. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
10. Peng, S.L., Hao, R.X., Pal, S, Amsaad, F. (eds.): Proceedings of 3rd ICMMCS. Advances in Intelligent Systems and Computing. Springer, Singapore (2023). https://doi.org/10.1007/978-98199-3611-3
11. Roy, B.: Application on a new type of of preopen sets and related continuity. Mat. Apl. **6**, 191–199 (2017)
12. Saravanakumar, D., Kalaivani, N., Sai Sundara Krishnan, G.: On γ^*-pre-regular-$T_{\frac{1}{2}}$ spaces associated with operations separation axioms. J. Interdisc. Math. **17**, 485–498 (2014)
13. Saravanakumar, D., Kalaivani, N., Sai Sundara Krishnan, G.: $\tilde{\mu}$-open sets in generalized topological spaces. Malaya J. Mat. **3**, 268–276 (2015)
14. Saravanakumar, D., Sai Sundara Krishnan, G.: Generalized mappings via new closed sets. Int. J. Mat. Sci. Appl. **2**, 127–137 (2012)

On $\alpha - (\gamma, \gamma')_{op}(\beta, \beta')_{op}(I_{ide}, J_{ide})$ -Continuous Functions in Ideal Topological Spaces

N. Kalaivani[1(✉)], D. GowriSankar Rao[2], D. Saravanakumar[3], E. Chandrasekaran[1], and N. Kalaivani[1]

[1] Department of Mathematics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
{drkalaivani,drchandrasekarane}@veltech.edu.in

[2] Department of Physics, Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Chennai, India
gshankarrao@veltech.edu.in

[3] Department of Mathematics, St. Joseph's University, Dar es Salaam, Tanzania

Abstract. In this work, the idea of $\alpha - (\gamma, \gamma')_{op}$ I_{ide}-open sets, $(\gamma, \gamma')_{op} - (\beta, \beta\prime)_{op}$ -open sets besides $(\gamma, \gamma')_{op} - (\beta, \beta\prime)_{op} I_{ide}$-open sets in topological spaces have been utilized through its agreeing interior besides closure operators: $\tau_{\alpha(\gamma,\gamma\prime)opI_{ide}}$ -closure, $\tau_{\alpha(\gamma,\gamma\prime)opI_{ide}}$-interior to discuss the concept and properties of $\alpha - (\gamma, \gamma')_{op} - (\beta, \beta')_{op}$ $(I_{ide,}J_{ide,})$-continuous functions, $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-semi-$(I_{ide,}J_{ide,})$-continuous functions, $(\gamma, \gamma')_{op} - (\beta, \beta\prime)_{op}$-pre -$(I_{ide,}J_{ide,})$-continuous functions, $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-semi-$(I_{ide,}J_{ide,})$-open functions and $(\gamma, \gamma')_{op}(\beta, \beta')_{op}$-pre -$(I_{ide,}J_{ide})$-open functions. The interrelationship connecting them has been elaborated. In addition, $\alpha - (\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide,}J_{ide,})$-open functions are presented also their rudimentary properties are premeditated with suitable illustrations. In this way this this work bridges the gap between the dual operation involved -open sets, ideal open sets, dual ideal involved open sets besides the continuous functions which encompassing all the above-mentioned concepts.

Keywords: $\alpha - (\gamma, \gamma')_{op}$-open set · $\alpha - (\gamma, \gamma')_{op}$ I_{ide}-open set · $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-open sets · $\alpha - (\gamma, \gamma')_{op}$-continuous functions · $\alpha_{\gamma,\gamma'_{op}} - (\beta, \beta')_{op}$ $(I_{ide,}J_{ide})$-continuous functions · $\alpha - (\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide,}J_{ide})$-open functions

AMS: 54A05 · 54A10 · 54C08

1 Introduction

The subsequent symbolizations are used in full length of this work: top spa – topological space, top spas – topological spaces, prop-properties, ide-ideal, topo-topology, ope-operation, opes-operators, CM-continuous mapping, subs-subset, subss-subsets, CM-Continuous mapping.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 24–36, 2025.
https://doi.org/10.1007/978-3-031-91008-1_3

Njastad [1] familiarized α -open sets in a top spa also deliberated their prop. The observation of *semi-opensets*, *preopensets* as well *semi-preopensets* were offered individually by *Levine* [2], *Corsonrson*, *Michael* [3] besides *Andrijevic* [5]. The *term* "pre-open" was publicized by *Mashhour et al.* [4] besides they considered its basic prop. *Andrijevic* [6] announced an innovative class of topo engendered by preopen sets as well the compatible *closure and interior* opes.

Kasahara [7] delineated the knowledge of an ope on top spas and offered closed graphs of an ope. *Ogata* [8] labelled the ope α as γ ope and habituated the inkling of τ_γ *which is the gathering of entire* γ*-open sets in a top spa.*

K. Kuratowski [12] *E. Hayashi* [13], *P. Samuels* [14], *D. Jankovic*, and *T.R. Hamlett* [15] premeditated about the ide topo and local properties correspondingly. *Reilly*, *Vamanamurthy* [16] described about the α-continuity in top spa.

Kalaivani, G. Sai Sundara Krishnan [9] announced α-γ_{op} -open sets in a top spa as well as proclaimed the perception of $\tau_{\alpha-\gamma_{op}}$ which is the gathering of entire α-γ_{op} *-opensets* in a top spa. Further *Kalaivani et al* [10, 11] discussed about the $\mathcal{S}$ eparation $\mathcal{A}$ xioms and R_i $\mathcal{S}$ paces with α_{γ_o}-open sets along with $(\gamma,\gamma')^{\alpha-}\Re$ egular $\mathcal{S}$ paces, $(\gamma,\gamma\prime)^{\alpha}$-$\mathbb{N}$ormal$\mathcal{S}$ paces with $(\gamma,\gamma\prime)$ *-opensets* and $\alpha(\gamma,\gamma\prime)$_open sets.

Nagarajan Kalaivani [17] studied about the $\mathcal{O}$*peration* $\mathcal{A}$*pproaches*: $\alpha\left(\gamma,\gamma'\right)_{op}$ I_{ide}*-open sets*, $\alpha\left(\gamma,\gamma'\right)_{op}$ I_{ide}*-*$\mathcal{C}$*ontinuous* $\mathcal{F}$*unctions in* $\mathcal{I}$*eal* $\mathcal{T}$*opological* $\mathcal{S}$*paces*.

In section three, the knowledge of $\alpha(\gamma,\gamma\prime)_{op}$ I_{ide} -open sets in the ide top spa has been offered. Similarly, the idea of $\tau_{\alpha(\gamma,\gamma\prime)_{op}I_{ide}}$- interior besides $\tau_{\alpha(\gamma,\gamma\prime)_{op}I_{ide}}$-closure opes are offered also their props are observed.

In Sector 4,5 the idea of $\alpha-(\gamma,\gamma\prime)_{op}-(\beta,\beta\prime)_{op}(I_{ide},J_{ide})$ -continuity, their properties, $\alpha-(\gamma,\gamma\prime)_{op}-(\beta,\beta\prime)_{op}(I_{ide},J_{ide})$ -semi-continuity, $\alpha-(\gamma,\gamma\prime)_{op}-(\beta,\beta\prime)_{op}(I_{ide},J_{ide})$ -pre-continuity, $\alpha-(\gamma,\gamma\prime)_{op}-(\beta,\beta\prime)_{op}(I_{ide},J_{ide})$- open functions, their props and the connection among them are deliberated.

2 Preliminaries I

Definition 2.1. [1] Let (X_{TOP},τ) be a top spa also $\mathbb{C}$ be a subs of X_{TOP}. Formerly $\complement$ is termed as an α - *openset* if $\complement \subseteq int_{op}(cl_{op}(int_{op}(\complement)))$ and an α- closed set if $cl_{op}(int_{op}(cl_{op}(\complement))) \supseteq \complement$.

Definition 2.2. [7] Let (X_{TOP},τ) be a top spa, an ope γ_{op} on the topo τ is a *mapping from* τ on to the power set P (X_{TOP}) of X_{TOP} alike that $Q \subseteq Q^{\gamma}$ for respective $Q \in \tau$, where Q^{γ} designates the value of γ_{op} at Q. It is signified by means of γ_{op}: $\tau \to$ P (X_{TOP}).

Definition 2.3. [8] Let (X_{TOP},τ) be a top spa and γ_{op} be an ope on τ. Formerly a subs W of X_{TOP} is supposed to be a γ_{op} -Θ open set if for individual $w \in W$, there ensues an Θ open set $\wp$ *aliki that* $w \in \wp$ also $\wp^{\gamma} \subseteq W$. $\tau_{\gamma_{op}}$ designates the set of all γ_{op}- Θ pen sets in (X_{TOP},τ). A *subset* Q of (X_{TOP},τ) is supposed to be a γ_{op} *– closed set* belonging to (X_{TOP},τ) if X_{TOP} $-Q$ is a γ_{op} -Θ *pen set* belonging to (X_{TOP},τ).

Definition 2.4. [8] Let (X_{TOP},τ) be a top spa besides γ be an ope on τ. Formerly $\tau_{\gamma_{op}}$- interior of $\wp$ is demarcated as amalgamation of all γ_{op}-Θ pen sets confined in $\wp$

besides symbolized as $\tau_{\gamma_{op}}$- int ($\wp$). That is $\tau_{\gamma_{op}}$-$int_{op}(\wp) = \cup\{W : W$ is a γ_{op}-*openset* besides$W \subseteq \wp\}$.

Definition 2.5. [8] Assume that (X_{TOP}, τ) be a top spa besides γ_{op} be an ope on τ. At that time $\tau_{\gamma_{op}}$- C losure of E is demarcated as the joint of all γ_{op} -C losed sets encompassing E in addition the thing is designated as $\tau_{\gamma_{op}}$- cl_{op} (E). That is $\tau_{\gamma_{op}}$-$cl_{op}(E) = \cap\{N : N$ is a γ_{op}-*closedset* also $E \subseteq N\}$.

Definition 2.6. [9] Agree that (X_{TOP}, τ) be a top spa besides γ_{op} be an ope on τ. At that time a sub M of X_{Top} is supposed to be a α-γ_{op} -open set on condition that $M \subseteq \tau_{\gamma_{op}}$-$int_{op}(\tau_{\gamma_{op}}$-$cl_{op}(\tau_{\gamma_{op}}$-$int_{op}(M)))$

Definition 2.7. [9] A subs $\wp$ of X_{TOP} is supposed to be α - γ_{op} -C losed set on condition that $X_{Top} - \wp$ is an α - γ_{op} -*openset*.

Remark 2.8. [9] Let (X_{Top}, τ) be a top spa besides γ_{op} be an ope on τ formerly F be a subs of X_{TS}. At that moment F is α - γ_{op} - C losed set contingent upon F$\supseteq$ $\tau_{\gamma_{op}}$-$cl_{op}\big(\tau_{\gamma_{op}} - int_{op}(\tau_{\gamma_{op}} - cl_{op}(\mathrm{F}))\big)$

Definition 2.9. [9] Let (X_{Top}, τ) be a top spa and γ_{op} be an ope on τ and $\mathcal{H}$ be a subs of X_{Top}. At that time $\tau_{\alpha-\gamma_{op}}$- interior of $\mathcal{H}$ is the unification of all α - γ_{op} - Θ pen sets confined in $\mathcal{H}$ and it is signified by $\tau_{\alpha-\gamma_{op}}$-$int_{op}$ $(\mathcal{H})$.

That is $\tau_{\alpha-\gamma_{op}}$-$int_{op}(\mathcal{H}) = \cup\{\mathbb{Q} : \mathbb{Q}$ is an α - γ_{op} - Θ pen set in addition $\mathbb{Q} \subseteq \mathcal{H}\}$.

Definition 2.10. [9] Let (X_{Top}, τ) be a top spa in addition γ_{op} be an ope on τ and be a subs of X_{Top}. Then $\tau_{\alpha-\gamma_{op}}$ C losure of $\mathcal{R}$ is the intersection of all α - γ_{op} - C losed sets comprising $\mathcal{R}$ and it is designated by $\tau_{\alpha-\gamma_{op}}$-$cl_{op}(\mathcal{R})$.That is $\tau_{\alpha-\gamma_{op}}$-$cl_{op}(\mathcal{R}) = \cap\{F : F$ is an α-γ_{op}-C losed set and $\mathcal{R} \subseteq F\}$.

Definition 2.11. [9] A mapping $f_{co} : X_{Top} \to Y_{Top}$ is thought to be (α-γ_{op}, β_{op})- CM if the contrary image of all β_{op} -Θ pen set belonging to Y_{Top} is α-γ_{op}-Θ pen set belonging to $\big(X_{Top}, \tau\big)$.

Definition 2.12. [9] A mapping $f_{co} : X_{Top} \to Y_{Top}$ is thought to be α-(γ_{op}, β_{op})- CM on condition that for any α-β_{op} -Θ pen set $\mathfrak{H}$ of Y_{Top}, f_{co}^{-1} $(\mathfrak{H})$ is an α-γ_{op}-Θ pen set in X_{Top}.

Theorem 2.13. [9] For a mapping $f_{co} : X_{Top} \to Y_{Top}$, the subsequent assertions are analogous:

(i) f_{co} is (α-γ_{op}, β_{op})- CM;
(ii) for each point x in X_{Top} besides individual Θ pen set V in Y_{Top} alike that f_{co} $(x) \in V$, there occurs an Θ pen set W in X_{Top} alike that $xW, f_{co}(W) \subseteq V$;
(iii) The contrary image of respective β_{op}-closed set in Y_{Top} is an α-γ_{op}- C losed set in X_{Top}.

Definition 2.13. [17] A set $G \subseteq X_{Top}$ is supposed to be an $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen set if and only if $G \subseteq \tau_{\alpha_{(\gamma,\gamma')op}}$ -int_{op} ($\tau_{\alpha_{(\gamma,\gamma')op}}$ -cl_{op} ($\tau_{\alpha_{(\gamma,\gamma')op}}$ -int_{op} (G))).

Theorem 2.14. [17] Each $(\gamma,\gamma')_{op}$ -Θ pen set in X_{Top} is an $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen set. Nevertheless, the conflicting argument is not true.

Theorem 2.15. [17] Let $\tau_{\alpha_{(\gamma,\gamma')op}}$ be the family of $\alpha_{(\gamma,\gamma')op}$- Θ pen sets in X_{Top}.Then $\underset{\alpha\in J}{\cup} A_\alpha$ is as well an $\alpha_{(\gamma,\gamma')op}$- Θ pen set.

Remark 2.1. [17] IfP, Q are two $\alpha_{(\gamma,\gamma')op}$- Θ pen sets in X_{Top}, then $P\cap Q$ is not an $\alpha_{(\gamma,\gamma')op}$- Θ pen set.

Remark 2.2. [17] The thoughts of α -Θ pen set and $\alpha_{(\gamma,\gamma')op}$- Θ pen set are autonomous.

Remark 2.3. [17] If X_{Top} is a $(\gamma,\gamma')_{op}$ -regular space, then the knowledge of $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen set and α -Θ pen set coincide.

Definition 2.14. [17] A subs M of X_{Top} is supposed to be an $\alpha_{(\gamma,\gamma')op}$- $\mathbb{C}$ losed set on condition that $X_{Top}-M$ is an $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen set, which is consistently M is an $\alpha_{(\gamma,\gamma')op}$-closed set in case that $M \supseteq \tau_{\alpha_{(\gamma,\gamma')op}}$-cl ($\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ ($\tau_{\alpha_{(\gamma,\gamma')op}}$-$cl_{op}$ (M))).

Definition 2.15. [17] (i) Let $N \subseteq X_{Top}$. Then $\tau_{\alpha_{(\gamma,\gamma')op}}$-interior of N is the unification of the entire $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen sets confined in N, symbolized by $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ (N).

That is given as $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ (N) $=\cup$ {Q: Q is an $\alpha_{(\gamma,\gamma')op}$- open set and $Q \subseteq N$}.

Remark 2.4. [17] Let $\mathbb{C} \subseteq X_{TS}$. Then the ensuing statements holds good:

(i) $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ ($\mathbb{C}$) is the largest $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen set confined in $\mathbb{C}$.
(ii) $\mathbb{C}$ is an $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen set on condition that $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ ($\mathbb{C}$) $=\mathbb{C}$.
(iii) $\tau_{\alpha_{(\gamma,\gamma')op}}$ -int_{op} ($\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ ($\mathbb{C}$)) $=\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ ($\mathbb{C}$)

Theorem 2.16. [17] Let $E, F \subseteq X_{Top}$. Then:

(i) If $E \subseteq F$ then $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ (E) $\subseteq \tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ (F)
(ii) $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ (E) $\cup$ $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ (F) $\subseteq$ $\tau_{\alpha_{(\gamma,\gamma')op}}$-$int_{op}$ ($E\cup F$)

Definition 2.4. [17] Let $Q \subseteq X_{Top}$. Then $\tau_{\alpha_{(\gamma,\gamma')op}}$- C losed set of Q is the intersection of the entire $\alpha_{(\gamma,\gamma')op}$-$C$ losed sets encompassing Q represented by $\tau_{\alpha_{(\gamma,\gamma')op}}$-$cl_{op}$ (Q). That is given as $\tau_{\alpha_{(\gamma,\gamma')op}}$-$cl_{op}$ (Q) $=\cap$ {H: H is an $\alpha_{(\gamma,\gamma')op}$- C losed set and $Q \subseteq H$}.

Remark 2.5. [17] Let X_{Top} be a top spa and γ_{op}, ${\gamma'}_{op}$ are opes on τ. Formerly.

(i) The $\tau_{\alpha_{(\gamma,\gamma')op}}$-$cl_{op}$ (P) is an $\alpha_{(\gamma,\gamma')op}$- C losed set encompassing P.
(ii) P is an $\alpha_{(\gamma,\gamma')op}$-$C$ losedset in case that $\tau_{\alpha_{(\gamma,\gamma')op}}$-$cl_{op}$ (P) $= P$.

Theorem 2.17. [17] Let $\{A_\alpha : \alpha \in J\}$ be the assortment of entire $\alpha_{(\gamma,\gamma')op}$-$\Theta$ pen sets in X_{Top}.Then $\bigcup_{\alpha\in J} A_\alpha$ is also an $\alpha_{(\gamma,\gamma')op}$ -Θ pen set inX_{Top}.

Definition 2.16. [17] A mapping is alleged to be an $\alpha_{(\gamma,\gamma')(\beta,\beta')op}$ -CM contingent upon for each $\alpha_{(\beta,\beta')op}$-$\Theta$ pen set, N ofY_{TS}, the contrary image $f_{co}^{-1}(N)$ is an $\alpha_{(\gamma,\gamma')op}$ -Θ pen set in X_{Top}..

Theorem 2.18. [17] A mapping $f_{co} : X_{Top} \to Y_{Top}$ is an $\alpha_{(\gamma,\gamma')(\beta,\beta')op}$ -CM if and only if for each point e in X_{Top} and each $\alpha_{(\beta,\beta')op}$ -neighbourhood E of f_{co} (e), there is an $\alpha_{(\gamma,\gamma')op}$ -neighbourhood B of b such that f_{co} $(B) \subseteq E$.

Theorem 2.19. [17] Let $f_{co} : X_{Top} \to Y_{Top}$ be a mapping. At that juncture the subsequent declarations are comparable:

(i) $f_{co} : X_{Top} \to Y_{Top}$ is an $\alpha_{(\gamma,\gamma')(\beta,\beta')op}$-CM;
(ii) f_{co} $(\tau_{\alpha_{(\gamma,\gamma')op}}$ -cl_{op} $(H))\subseteq \sigma_{\alpha_{(\beta,\beta')op}}$-$cl_{op}$ $(f_{co}$ $(H))$ holds for every subset H of X_{Top};
(iii) For every $\alpha_{(\beta,\beta')op}$-closed set $\mathfrak{I}$ belongs to Y_{Top}, $f^{-1}(\mathfrak{I})$ is an $\alpha_{(\gamma,\gamma')op}$ -closed set in X_{Top}.

3 Preliminaries II

Based the Idea of $\alpha(\gamma, \gamma')_{op}I_{ide}$-Open Sets in Ideal Topological Spaces

Here X_{TOP} signifies the ide top spa (X_{TOP}, τ, I) besides Y_{TOP} designates the top spa (Y_{TOP}, σ). The operations $\gamma_{op} : \tau \to P(X_{TOP})$ in addition $\beta_{op} : \sigma \to P(Y_{TOP})$ on τ,σ are demarcated.

Definition 3.1. Accredit X_{TOP} be a top spa,I_{ide} be an ide of subsets of X_{TOP}.γ_{op} besides γ'_{op} are operations on $\tau.\tau^*_{(\gamma,\gamma')op}$ (I, $\tau_{(\gamma,\gamma')}$) is the assortment of all $V - I_{ide}$ such that $V \in \tau_{(\gamma,\gamma')op}$.

Formerly $\tau^*_{(\gamma,\gamma')op}$ (I, τ) = $\{V - I$: $V \in \tau_{(\gamma,\gamma')}$ and $I \in I_{ide}\}$.

Definition 3.2. Let X_{TOP} be a top spa and I_{ide} be an ide of subss ofX_{TOP}. Formerly, for a subs $B \subset X_{TOP}$, $\tau_{(\gamma,\gamma')op}$- C^* (I_{ide},$\tau_{(\gamma,\gamma')op}$) = $\{x \in X_{TOP}$: $V \cap C \notin I_{ide}$ for each $(\gamma, \gamma')_{op}$-open set V of $x\}$ is entitled the local function of C through deference to I_{ide} also $\tau_{(\gamma,\gamma')op}$ using the operations γ_{op},γ'_{op} on τ. It is written as $\tau_{(\gamma,\gamma')op}$- C^* instead of $\tau_{(\gamma,\gamma')op}$- C^* (I_{ide},$\tau_{(\gamma,\gamma')op}$).

Definition 3.3. Let C be a subs of X_{TOP} and γ_{op},γ'_{op} be regular operations on τ. Formerly the Kuratowski* closure operator is demarcated as $\tau_{(\gamma,\gamma')op}$-$cl^*_{op}$ (C) =$C \cup \tau_{(\gamma,\gamma')op}$- C^*, where $\tau_{(\gamma,\gamma')}$- C^* is the local function of B through veneration to I_{ide} in addition $\tau_{(\gamma,\gamma')op}$.

Definition 3.4. Let C be a subs of X_{TOP}. Then $\tau_{(\gamma,\gamma')op}$-$int^*_{op}$ (C) is defined as the unification of all $(\gamma, \gamma')_{op}$ -Open sets U in $\tau^*_{(\gamma,\gamma')op}$ such that $U \subseteq C$.

It is symbolized as $\tau_{(\gamma,\gamma')op}$-$int^*_{op}$ $(C) = \cup \{ U \in \tau^*_{(\gamma,\gamma')op}$: $U \subseteq C\}$

Theorem 3.1. Accredit X_{TOP} be an idea top spa and γ_{op},γ'_{op} be operations on τ. Formerly the succeeding declarations hold good.

(i) $\tau_{(\gamma,\gamma')op}$-$cl^*_{op}$ $(D)\subseteq \tau_{(\gamma,\gamma')op}cl_{op}$ (D)

(ii) $\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D)\subseteq \tau_{(\gamma,\gamma')op}$-$int^{*}_{op}\ (D)$
(iii) $\tau_{(\gamma,\gamma')op}$- $cl^{*}_{op}\ (\tau_{(\gamma,\gamma')op}$-int $(D))\subseteq (\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D))^{*}\cup\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D)$
(iv) $(\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D))^{*}\subseteq \tau_{(\gamma,\gamma')op}$-$cl_{op}\ (\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D))$
(v) $\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D\cup\tau_{(\gamma,\gamma')op}D^{*})\subseteq \tau_{(\gamma,\gamma')op}$-$int_{op}\ (\tau_{(\gamma,\gamma')op}$-$cl_{op}\ (D))$
(vi) $\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D)\subseteq \tau_{(\gamma,\gamma')op}$-$int_{op}\ (\tau_{(\gamma,\gamma')op}$-$cl^{*}_{op}\ (\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D)))$
(vii) $Q\cap(\tau_{(\gamma,\gamma')op}$-$D^{*})\subseteq(Q\cap\tau_{(\gamma,\gamma')op}$-$D)^{*}$ where $Q\in\tau_{(\gamma,\gamma')op}$ and γ_{op},γ'_{op} are regular operations.

Remark 3.1. if $I_{ide}=\{\varnothing\}$, Formerly $\tau_{(\gamma,\gamma')op}$-$\mathrm{cl}^{*}\ (D)=\tau_{(\gamma,\gamma')op}$-$cl_{op}\ (D)$.

Definition 3.5. A subset D of X_{TOP} is supposed to be an $\alpha(\gamma,\gamma')_{op}I_{ide}$ - open set-in case that $D\subseteq\tau_{(\gamma,\gamma')op}$-$int_{op}\ (\tau_{(\gamma,\gamma')op}$-$cl^{*}_{op}\ (\tau_{(\gamma,\gamma')op}$-int $(D)))$. The assortment of all $\alpha(\gamma,\gamma')_{op}I_{ide}$ -open sets in X_{TOP} is symbolized by $\tau_{\alpha(\gamma,\gamma')opI_{ide}}$.

Definition 3.6. A subset of an ide top spa X_{TOP} is thought to be

(i) a $(\gamma,\gamma')_{op}$ semi I_{ide} -open set-in case that $D\subseteq\tau_{(\gamma,\gamma')op}$-$cl^{*}_{op}\ (\tau_{(\gamma,\gamma')op}$-$int_{op}\ (D))$
(ii) a $(\gamma,\gamma')_{op}$ pre I_{ide} -open set-in case that $D\subseteq\tau_{(\gamma,\gamma')op}$-$int_{op}\ (\tau_{(\gamma,\gamma')op}$-$cl^{*}_{op}\ ((D))$

Theorem 3.2. Let X_{TOP} be an ide top spa. γ_{op},γ'_{op} be operations on τ. Formerly,
(i) Each $\alpha(\gamma,\gamma')_{op}I_{ide}$ -open set is an $\alpha(\gamma,\gamma')_{op}$-open set.
(ii) Each $(\gamma,\gamma')_{op}$ semi I_{ide} -open set is a $(\gamma,\gamma')_{op}$ semi-open set.
(iii) Each $(\gamma,\gamma')_{op}$ pre I_{ide} - open set is a $(\gamma,\gamma')_{op}$ pre-open set.

Theorem 3.3. Let X_{TOP} be an ide top spa and γ_{op} be an operation on τ. At that time,
(i) Every single $\alpha(\gamma,\gamma')_{op}I_{ide}$ -open set is a $(\gamma,\gamma')_{op}$ semi I_{ide} -open set.
(ii) Every single $\alpha(\gamma,\gamma')_{op}I_{ide}$ -open set is a $(\gamma,\gamma')_{op}$ pre I_{ide} -open set.

Theorem 3.4. Each $(\gamma,\gamma')_{op}$-open set of an ide top spa is an $\alpha((\gamma,\gamma')_{op}I_{ide}$ -open set.

Theorem 3.5. **A** subs $\mathcal{L}$ of X_{TOP} is an $\alpha(\gamma,\gamma')_{op}I_{ide}$-open set on the assumption that it is a $((\gamma,\gamma')_{op}$ semi I_{ide}-open and $(\gamma,\gamma')_{op}$ pre I_{ide}-open set.

Lemma 3.1. Let $\mathfrak{J}$ be a subs ofX_{TOP}. Suppose γ_{op},γ'_{op} be regular operations on τ. If M is a $(\gamma,\gamma')_{op}$ -open set in (X_{TOP},τ,I_{ide}), at that time $\mathrm{M}\cap\tau_{(\gamma,\gamma')op}$-$cl^{*}_{op}\ (\mathfrak{J})\subseteq\tau_{(\gamma,\gamma')op}$-$cl^{*}_{op}$ $(\mathrm{M}\cap\mathfrak{J})$.

Theorem 3.6. Let D be a subset of X_{TOP} and γ_{op},γ'_{op} be regular opes on τ,σ. If $\{D_{\alpha}:\alpha\epsilon J\}$ be the assortment of entire $\alpha(\gamma,\gamma')_{op}I_{ide}$- open sets in (X_{TOP},τ,I), formerly $\cup_{\alpha\epsilon J}D_{\alpha}$ is also an $\alpha((\gamma,\gamma')_{op}I_{ide}$ - open set.

Definition 3.7. **A** subset D of X_{TOP} is alleged to be an $\alpha(\gamma,\gamma')_{op}I_{ide}$-closed set supposing $X_{TOP}-D$ is an $\alpha(\gamma,\gamma')_{op}I_{ide}$-open set, which is unvaryingly a subset D of X_{TOP} is an $\alpha(\gamma,\gamma')_{op}I_{ide}$-closed set on the assumption $D\supseteq\tau_{(\gamma,\gamma')op}$ -$cl_{op}\ (\tau_{(\gamma,\gamma')op}$ -$int^{*}_{op}\ (\tau_{(\gamma,\gamma')op}$ -$cl_{op}\ (D)))$.

Definition 3.8. Let M be a subs of X_{TOP}. Then $\tau_{\alpha(\gamma,\gamma')opI_{ide}}$ interior of M is the unification of all $\alpha(\gamma,\gamma')_{op}I_{ide}$-open sets confined in M, which is designated as $\tau_{\alpha(\gamma,\gamma')opI_{ide}}$-$int_{op}\ (M)$.

$\tau_{\alpha(\gamma,\gamma')opI_{ide}}$-$int_{op}\ (D)=\cup\{V\colon V$ is an $\alpha(\gamma,\gamma')_{op}I_{ide}$ -open set besides $V\subseteq D\}$

Definition 3.9. Let $\varkappa$ be a sub of X_{TOP} then $\tau_{\alpha(\gamma,\gamma')opI_{ide}}$ closure of $\varkappa$ is the intersection of entire $\alpha(\gamma, \gamma')_{op}$ I -closed sets comprising $\varkappa$. It is symbolized as $\tau_{\alpha(\gamma,\gamma')opI_{ide}}$- cl_{op} $(\varkappa)$.

$\tau_{\alpha(\gamma,\gamma')opI_{ide}}$-$cl_{op}$ $(\varkappa) = \cap\{F: F$ is an $\alpha(\gamma, \gamma')_{op}I_{ide}$-closed set and $\varkappa \subseteq F\}$.

Theorem 3.7. Let (X_{TOP}, τ, I_{ide}) be an ide top spa. γ_{op},γ'_{op} be regular operations on τ, σ.

(i) If $I = \{\varnothing\}$, then $\tau_{\alpha(\gamma,\gamma')opI_{ide}} = \tau_{\alpha(\gamma,\gamma')op}$

(ii)If $I = P$ (X_{TOP}), then $\tau_{\alpha(\gamma,\gamma')opI_{ide}} = \tau_{(\gamma,\gamma')op}$

Theorem 3.1. Let $\mho$ be a subs of X_{TOP}. then

(a) If $I_{ide} = \varnothing$, formerly.

(i) The notions of $\alpha(\gamma, \gamma')_{op}I_{ide}$-open set, (γ,γ') pre I_{ide} -open set and $(\gamma, \gamma')_{op}$ pre-open set are all comparable.

(ii) $\mho$ is a $(\gamma, \gamma')_{op}$ semi I_{ide} -open set in the event that $\mho$ is a $(\gamma, \gamma')_{op}$ semi-open set.

(iii) $\mho$ is a $(\gamma, \gamma')_{op}\beta$ I_{ide} -open set-in case that $\mho$ is a $(\gamma, \gamma')_{op}\beta$ - open set.

4 $\alpha - (\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide}, J_{ide})$ -Continuous Functions in Ideal Topological Spaces

Throughout this segment $f_{\mathcal{CON}}$ signifies a function $f_{CON}: (X_{\mathcal{TOP}}, \tau, I_{ide}) \to (Y_{\mathcal{TOP}}, \sigma, J_{ide})$,$X_{\mathcal{TOP}}$,$Y_{\mathcal{TOP}}$ denotes the ideal topological spaces $(X_{\mathcal{TOP}}, \tau, I_{ide})$,$(Y_{\mathcal{TOP}}, \sigma, J_{ide})$ along with the operations defined as $\gamma_{ope} : \tau \to P(X_{TOP})$, $\gamma'_{ope} : \sigma \to P(Y_{TOP})$ are operations onτ, σ.

Definition 4.1. A function $f_{CON} : X_{\mathcal{TOP}} \to Y_{\mathcal{TOP}}$ is supposed to be:

(i) an $\alpha - (\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide}, J_{ide})$-continuous function if for each $\alpha - (\beta, \beta')_{op}J_{ide}$-open set $\mathring{A} \in \sigma$, the contrary image ${f_{CON}}^{-1}$ $(\mathring{A})$ is an $\alpha-(\gamma, \gamma')_{op}I_{ide}$-open set in$(X_{TOP}, \tau, I_{ide})$.

(ii) a $(\gamma, \gamma')_{op}$ semi (I_{ide}, J_{ide}) -continuous function if for individual $(\beta, \beta')_{op}$ semi J_{ide}-open set, $\mathring{A} \in \sigma$, the contrary image ${f_{CON}}^{-1}$ (N) is a $(\gamma, \gamma')_{op}$ semi I_{ide} -open set in(X_{TOP}, τ, I_{ide})).

(iii) a $(\gamma, \gamma')_{op}$ pre (I_{ide}, J_{ide}) -continuous function if for individual $(\beta, \beta')_{op}$*semi* J_{ide}-open set $\mathring{A} \in \sigma$, the contrary image ${f_{CON}}^{-1}$ (N) is a $(\gamma, \gamma')_{op}$ pre I_{ide}-open set in (X_{TOP}, τ, I).

Example 4.1. Let $X_{TOP}=\{a,b,c\}$, $\tau=\{\phi,X_{TOP},\{a\},\{c\},\{a,b\},\{a,c\}\}$, and $I_{ide}=\{\varphi,\{b\}\}$.

Describe γ_{op},γ'_{op} on τ such that $D^{\gamma_{op}}=\begin{cases}D\cup\{c\}\ if\ D\neq\{a\}\\ D\ if\ D=\{a\}\end{cases}$ and $D^{\gamma'_{op}}=cl_{op}(D)$ for all $D\in\tau$.

Formerly $\tau_{\alpha-(\gamma,\gamma')op}=\{\varnothing,X_{TOP},\{a\},\{c\},\{a,c\}\}$ besides
$\tau_{\alpha-(\gamma,\gamma')opI_{ide}}=\{\varnothing,X_{TOP},\{a\},\{c\},\{a,b\},\{a,c\}\}$.
Let $Y_{TOP}=\{a,b,c\}$,$\sigma=\{\phi,Y_{TOP},\{a\},\{c\},\{a,c\},\{b,c\}\}$, $J_{ide}=\{\varphi,\{a\}\}$.

Announce β_{op},β'_{op} on σ such that $D^{\beta_{op}}=\begin{cases}D\cup\{c\}\ if\ D\neq\{a\}\\ D\ if\ D=\{a\}\end{cases}$ and $D^{\beta'_{op}}=cl_{op}(D)$ for all $D\in\tau$.

Formerly $\sigma_{\alpha-(\beta,\beta')op}=\{\varnothing,X_{TOP},\{a\},\{c\},\{a,c\}\}$ besides
$\sigma_{\alpha-(\beta,\beta')opJ_{ide}}=\{\varnothing,X_{TOP},\{a\},\{c\},\{a,c\}\}$.

Designate a function f_{CON} as f_{CON} (a) = c; f_{CON} (b) = b; f_{CON} (c) = a. Formerly for each $\alpha-(\beta,\beta')_{op}J_{ide}$ -open set $V\in\sigma$, the contrary image ${f_{CON}}^{-1}(V)$ is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set in X_{TOP}. Hence f_{CON} is an $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$-continuous function.

Theorem 4.1. If a function $f_{CON}:X_{TOP}\to Y_{TOP}$ is an $\alpha-(\gamma,\gamma')_{op}(\beta,\beta')_{op}(I_{ide},J_{ide})$-continuous (respectively $(\gamma,\gamma')_{op}(\beta,\beta')_{op}$ semi(I_{ide},J_{ide})-continuous, $(\gamma,\gamma')_{op}(\beta,\beta')_{op}$ pre (I_{ide},J_{ide}) -continuous) function, then f_{CON} is an $\alpha_{-}(\gamma,\gamma')_{op}(\beta,\beta')_{op}$ -continuous (respectively $(\gamma,\gamma')_{op}(\beta,\beta')_{op}$ semi-continuous, $(\gamma,\gamma')_{op}(\beta,\beta')_{op}$ - pre-continuous) function.

Proof. Proof trails after the 3.2. Theorem.

Theorem 4.2. Let $f_{CON}:X_{TOP}\to Y_{TOP}$ be a *function*, formerly the succeeding declarations are comparable:

(i) f_{CON} is an $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$ - continuous function;

(ii) For individual $\wp\in X_{TOP}$ besides separate $\alpha-(\beta,\beta')_{op}J_{ide}$ -open set $\mathcal{W}\subseteq Y_{TOP}$ containing $f_{CON}(\wp)$, there exists a $\mathcal{H}\in\tau_{\alpha(\gamma,\gamma')opI_{ide}}$ such that $\wp\in\mathcal{H}$, $f_{CON}(\mathcal{H})\subseteq\mathcal{W}$;

(iii) The contrary image of individual $\alpha-(\beta,\beta')_{op}J_{ide}$ -closed set in Y_{TOP} is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-closed set;

(iv) $\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$int^{*}_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $({f_{CON}}^{-1}$ $(\mathcal{B}))))\subseteq {f_{CON}}^{-1}$ $(\sigma_{\alpha(\beta,\beta')op}-cl_{op}(\mathcal{B}))$ for apiece $\mathcal{B}\subseteq Y_{TOP}$;

(v) f_{CON} $(\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$int^{*}_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(\mathcal{A})))\subseteq$ $\sigma_{\alpha(\beta,\beta')op}$-$cl_{op}$ $(f_{CON}(\mathcal{A}))$ for each $\mathcal{A}\subseteq X_{TOP}$.

Proof. (i) implies (ii) Let $\wp\in X_{TOP}$ also $\mathcal{W}$ be an $\alpha-(\beta,\beta')_{op}J_{ide}$ -open set of $\mathcal{W}$ comprising $f(\wp)$. Set $\mathcal{H}={f_{CON}}^{-1}(\mathcal{W})$, then by Definition 4.1.,$\mathcal{H}$ is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set encompassing $\wp$ and $f(\mathcal{H})\subseteq\mathcal{W}$.

(ii) implies (iii) Let E be an $\alpha-(\beta,\beta')_{op}J_{ide}$ -closed set of Y_{TOP}. Set $W=Y_{TOP}-E$, then W is an $\alpha-(\beta,\beta')_{op}J_{ide}$ - open set in Y_{TOP}. Let $\wp\in{f_{CON}}^{-1}(\mathcal{W})$, by (ii), there exists an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set $\mathcal{G}$ of X_{TOP} containing $\wp$ alike that $f(\mathcal{G})\subseteq W$. We attain $\wp\in\mathcal{G}\subseteq\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$cl^{*}_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}$ $(\mathcal{G})\subseteq\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}$

$(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ ({f_{CON}}^{-1}(\mathcal{W}))))$. This displays that ${f_{CON}}^{-1}(\mathcal{W})$ is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set in X_{TOP}. Hence ${f_{CON}}^{-1}(E)=X_{TOP}-{f_{CON}}^{-1}(Y_{TOP}-E))=X_{TOP}-{f_{CON}}^{-1}(W)$ is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-closed set in X_{TOP}.

(iii) implies (iv) Let $\mathcal{B}$ be any subs of Y_{TOP}. Since $\sigma_{\alpha(\beta,\beta')op}\text{-}cl_{op}(\mathcal{B})$ is a closed set in Y_{TOP}, by (iii), ${f_{CON}}^{-1}(\sigma_{\alpha(\beta,\beta')op}cl_{op}(\mathcal{B}))$ is an $-(\gamma,\gamma')_{op}I_{ide}$-closed set and $X_{TOP}-{f_{CON}}^{-1}(\sigma_{\alpha(\beta,\beta')op}cl_{op}(\mathcal{B}))$ is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set. Thus, $X_{TOP}-{f_{CON}}^{-1}(\sigma_{\alpha(\beta,\beta')op}cl_{op}(\mathcal{B}))\subseteq\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (X_{TOP}-{f_{CON}}^{-1}(\sigma_{\alpha(\beta,\beta')op}cl_{op}(\mathcal{B})))))=X_{TOP}-(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}(\sigma_{\alpha(\beta,\beta')op}cl_{op}(\mathcal{B}))))))$. Hence $\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}\ (E))))\subseteq{f_{CON}}^{-1}\ (\sigma_{\alpha(\beta,\beta')op}-cl_{op}\ (E))$.

(iv) implies (v) Assume $\mathcal{A}$ be any subs of X_{TOP}. Via the result (iv), $\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}\ ({f_{CON}}\ (\mathcal{A})))\subseteq{f_{CON}}^{-1}\ (\sigma_{\alpha(\beta,\beta')op}-cl_{op}\ ({f_{CON}}\ (\mathcal{A}))$. Hence ${f_{CON}}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\mathcal{A}))))\subseteq\sigma_{\alpha(\beta,\beta')op}\text{-}cl_{op}\ ({f_{CON}}\ (\mathcal{A}))$

(v) implies (i) Assume $\mathcal{V}$ be an $\alpha-(\beta,\beta')_{op}J_{ide}$ -open set ofY_{TOP}. Then through the result (v) ${f_{CON}}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}\ (Y_{TOP}-\mathcal{V})))))\subseteq\sigma_{\alpha(\beta,\beta')op}cl_{op}({f_{CON}}\ ({f_{CON}}^{-1}(Y_{TOP}-\mathcal{V})))\subseteq\sigma_{\alpha(\beta,\beta')op}cl_{op}(Y_{TOP}-\mathcal{V})=Y_{TOP}-\mathcal{V}$.Henceforth, $\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}\ (Y_{TOP}-\mathcal{V})))))\subseteq{f_{CON}}^{-1}(Y_{TOP}-\mathcal{V})\subseteq X_{TOP}-{f_{CON}}^{-1}(\mathcal{V})$. Thus attained as, ${f_{CON}}^{-1}(\mathcal{V})\subseteq\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\mathcal{V})))$. This gives the result as ${f_{CON}}^{-1}(\mathcal{V})$ is an $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set. Thus f_{CON} is an $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$ - continuous function.

Corollary 4.1. Let $f_{CON}:X_{TOP}\to Y_{TOP}$ be an $\alpha-\left(\gamma,\gamma'\right)_{op}-\left(\beta,\beta'\right)_{op}(I_{ide},J_{ide})$ - continuous function, formerly.

(i) ${f_{CON}}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\mathcal{M}))\subseteq\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}\ (\mathcal{M}))$ for individual $\mathcal{M}\in(\gamma,\gamma')_{op}$-PIO (X_{TOP}).

(ii)$\tau_{\alpha(\gamma,\gamma')op}\text{-}\ cl^*_{op}\ ({f_{CON}}^{-1}\ (\aleph))\subseteq\ {f_{CON}}^{-1}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\aleph))$ for each $\aleph\in(\gamma,\gamma')_{op}$- PIO (Y_{TOP}).

Proof. (i) Let $\mathcal{M}\in(\gamma,\gamma')_{op}$-PIO (X_{TOP}), then $\mathcal{M}\subseteq\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\mathcal{M}))$. Subsequently, by means of 4.2. Theorem, ${f_{CON}}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\mathcal{M}))\subseteq\ {f_{CON}}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\mathcal{M}))\subseteq{f_{CON}}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\mathcal{M}))))\subseteq{f_{CON}}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\mathcal{M}))))\subseteq\tau_{\alpha(\gamma,\gamma')op}\text{-cl}({f_{CON}}\ (\mathcal{M}))$.

(ii) Let $\aleph\in(\gamma,\gamma')_{op}$-PIO (Y_{TOP}). By means of 4.2.Theorem in addition using the statement (i), $\tau_{\alpha(\gamma,\gamma')op}\text{-}\ cl^*_{op}\ ({f_{CON}}^{-1}\ (\aleph))\subseteq\ \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}\ (\aleph))\subseteq\ \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ ({f_{CON}}^{-1}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\aleph))))\subseteq\ \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}[{f_{CON}}^{-1}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\aleph)))]))))\subseteq\ \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int^*_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ [{f_{CON}}^{-1}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^*_{op}\ (\aleph)))]))\subseteq{f_{CON}}^{-1}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}\ cl^*_{op}\ (\aleph))))\subseteq{f_{CON}}^{-1}\ (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}\ (\aleph))$.

Theorem 4.3. A function $f_{CON}: X_{TOP} \to Y_{TOP}$ is an $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$-continuous function in case that it is a $(\gamma,\gamma')_{op}-(\beta,\beta')_{op}$ semi (I_{ide},J_{ide}) -continuous and $(\gamma,\gamma')_{op}-(\beta,\beta')_{op}$ pre (I_{ide},J_{ide}) -continuous function.

Proof. Demonstration trails from the 4.1. Theorem.

5 $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$ - Open Functions in Ideal Topological Spaces

All over this division f_{co} signifies the function$f_{co}: (X_{TO},\tau.I_{ide}) \to (Y_{TO},\sigma,J_{ide})$, X_{TO} symbolizes the top spa(X_{TO},τ,I_{ide}), Y_{TO} signifies the ide top spa (Y_{TO},σ,J_{ide}). Assume $\gamma_{op}:\tau \to P(X_{TO})$ $\gamma'_{op}:\sigma \to P(Y_{TO})$ are operations on τ,σ.

Definition 5.1. (i) A function f_{co} is considered to be an $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$ -open function if the image of individual $(\gamma,\gamma')_{op}I_{ide}$-open set in X_{TO} is an $(\beta,\beta')_{op}J_{ide}$ -open set of Y_{TO}.

(ii) A function f_{co} is assumed to be a $(\gamma,\gamma')_{op-}$ $(\beta,\beta')_{op}$ semi (I_{ide},J_{ide}) -open (resp. $(\gamma,\gamma')_{op}$ $(\beta,\beta')_{op}$ _pre (I_{ide},J_{ide}) -open, $(\gamma,\gamma')_{op}$ $(\beta,\beta')_{op}$ $\boldsymbol{\beta}(I_{ide},J_{ide})$-open-function in case that the image of respective $(\gamma,\gamma')_{op}$ semi I_{ide} -open (resp. $(\gamma,\gamma')_{op}$ pre I_{ide} -open,$(\gamma,\gamma')_{op}\beta$ I_{ide} - open set of X_{TO} is a $(\beta,\beta')_{op}$ semi J_{ide} -open (resp. $(\beta,\beta')_{op}$ pre J_{ide} -open,$(\beta,\beta')_{op}$ J_{ide} -open set ofY_{TO}.

Example 5.1. Let $X_{TO}=\{e,f,g\}$,$\tau=\{\phi,X_{TO},\{e,g\}\}$,$Y_{TO}=\{e,f,g\}$, $\sigma=P(Y_{TO})$, $I_{ide}=\{\varphi,\{g\}\}$ and $J_{ide}=\{\varphi,\{e\}\}$.

Describe γ_{op},γ'_{op} on τ such that $\mathcal{L}^{\gamma_{op}} = \begin{cases} L\cup\{g\}\ if\ L=\{e\} or\{f\} \\ L\cup\{a\}\ if\ L=\{g\} \\ L\ if\ L\neq\{e\},\{f\} and\{g\} \end{cases}$ and $\mathcal{L}^{\gamma'_{op}} =$ $int_{op}(\mathcal{L})$ for everyone $\mathcal{L}\in\tau$.

Describe β_{op},β'_{op} on σ such that $\mathfrak{I}^{\beta_{op}} = \begin{cases} L\cup\{g\}\ if\ L=\{e\} or\{f\} \\ L\cup\{a\}\ if\ L=\{g\} \\ L\ if\ L\neq\{e\},\{f\} and\{g\} \end{cases}$ and $\mathfrak{I}^{\beta'_{op}} =$ $int_{op}(\mathfrak{I})$ for everyone $\mathfrak{I}\in\sigma$.

Formerly $\tau_{\alpha(\gamma,\gamma')I}=\{\varnothing,Y_{TO},\{e,f\},\{f,g\},\{e,g\}\}$ and $\sigma_{\alpha(\beta,\beta')J}=\{\varnothing,Y_{TO},\{e,f\},\{f,g\},\{e,g\}\}$.

Consider a function f_{co} as $f_{co}(e)=g$;$f_{co}(f)=f$;$f_{co}(g)=e$. Then, the image of every $\alpha-(\gamma,\gamma')_{op}I_{ide}$-open set in X_{TO} is an $\alpha-(\beta,\beta')_{op}J_{ide}$ open set in Y_{TO}. Henceforth f_{co} is an $\alpha-(\gamma,\gamma')_{op}-(\beta,\beta')_{op}(I_{ide},J_{ide})$-open function.

Theorem 5.1. A function $f_{co}: (X_{TO},\tau,I_{ide}) \to (Y_{TO},\sigma,J_{ide})$ is considered to be an $\alpha-(\gamma,\gamma')_{op}(\beta,\beta')_{op}(I_{ide},J_{ide})$-open function in case that f_{co} is a $(\gamma,\gamma')_{op}$ semi I_{ide} -open and $(\gamma,\gamma')_{op}$ pre I_{ide} -open function.

Proof. Authentication reviews from the 4.1. Theorem.

Theorem 5.2. A function $f_{co} : (X_{TO}, \tau) \to (Y_{TO}, \sigma, I_{ide})$, is thought to be a $\alpha - (\gamma, \gamma')_{op} I_{ide}$ -open function contingent upon for separate $\alpha - (\gamma, \gamma')_{op} I_{ide}$ subs $P \subseteq Y_{TO}$ and respective closed set F of X_{TO} encompassing ${f_{co}}^{-1}(P)$, there exists an $\alpha - (\beta, \beta')_{op} J_{ide}$-closed set $Q \subseteq Y_{TO}$ comprising P such that ${f_{co}}^{-1}(Q) \subseteq F$.

Proof. Let $N = Y_{TO} - f_{co}(X_{TO} - H)$. Since ${f_{co}}^{-1}(M) \subseteq H$, $f_{co}(X_{TO} - H) \subseteq Y_{TO} - M$. Since f_{co} is an $\alpha(\gamma, \gamma')_{op} I_{ide}$- open function, then N is an $\alpha(\gamma, \gamma')_{op} I_{ide}$-closed set and $f_{co}^{-1}(N) = X_{TO} - f_{co}^{-1}(f_{co}(X_{TO} - H)) \subseteq X_{TO} - (X_{TO} - H) = H$.

Contrarywise, let E be any open set of X_{TO} and $M = Y_{TO} - f_{co}(E)$. At that time, $f_{co}^{-1}(M) = X_{TO} - f_{co}^{-1}(f_{co}(E)) \subseteq X_{TO} - E$ and $X_{TO} - E$ is a closed set. By proposition, there occurs an $\alpha - (\gamma, \gamma')_{op} I_{ide}$-closed set N of Y_{TO} comprising M alike that $f_{co}^{-1}(N) \subseteq X_{TO} - E$. Then, $f_{co}^{-1}(N) \cap E = \emptyset$ and $N \cap f_{co}(E) = \emptyset$. Consequently, $Y_{TO} - f_{co}(E) \supseteq N \supseteq M = Y_{TO} - f_{co}(E)$ and $f_{co}(E)$ is an $\alpha - (\gamma, \gamma')_{op} I_{ide}$-open set in Y_{TO}. This infers that f_{co} is an $\alpha - (\gamma, \gamma')_{op} I_{ide}$-open function.

Corollary 5.1. If $f_{co} : (X_{TO}, \tau) \to (Y_{TO}, \sigma, I_{ide})$ is an $\alpha - (\gamma, \gamma')_{op}(\beta, \beta')_{op}(I_{ide}, J_{ide})$-open function, formerly the ensuing properties hold:

(i) $f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-cl}(C)))) \subseteq \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(f_{co}^{-1}(C))$ for each set $C \subseteq Y_{TO}$.

(ii) $f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^{*}_{op}(W)) \subseteq \tau_{\alpha(\gamma,\gamma')}\text{-}cl_{op}(f_{co}^{-1}(W))$ for each $(\gamma, \gamma')_{op}$ -preopen set W of Y_{TO}.

Proof. (i) Consider C as a subs of Y_{TO}, at that time $\tau_{(\gamma,\gamma')op}\text{-}cl_{op}(f_{co}^{-1}(C))$ is a closed set in X_{TO}. Through 4.2. Theorem, there occurs an $\alpha - (\gamma, \gamma')_{op}(\beta, \beta')_{op}(I_{ide}, J_{ide})$-closed set $K \subseteq Y_{TO}$ encompassing C alike that $f_{co}^{-1}(K) \subseteq \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(f^{-1}(C))$. Subsequently $Y_{TO} - K$ is an $\alpha - (\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide}, J_{ide})$ - open set, $f_{co}(Y_{TO} - K) \subseteq f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int_{op}(Y_{TO} - K))))$ and $X_{TO} - f_{co}^{-1}(K) \subseteq f_{co}^{-1}(Y_{TO} - (\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(K))))) = X_{TO} - f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(K))))$.Thus, $f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^{*}_{op}(\tau_{(\gamma,\gamma')op}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(C)))) \subseteq f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl^{*}_{op}(K)))) \subseteq f_{co}^{-1}(K) \subseteq \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(f_{co}^{-1}(C))$. Consequently, $f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(C)))) \subseteq \tau_{\alpha(\gamma,\gamma')op}\text{-}cl^{*}_{op}(f_{co}^{-1}(C))$.

(ii) Let W be any $(\gamma, \gamma')_{op}$-preopen set of Y_{TO}. Through (i) $f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-cl}^{*}(W)) \subseteq f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(W)) \subseteq f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-int}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(W)))) \subseteq f_{co}^{-1}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(\tau_{\alpha(\gamma,\gamma')}\text{-}int^{*}_{op}(\tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(W)))) \subseteq \tau_{\alpha(\gamma,\gamma')op}\text{-}cl_{op}(f_{co}^{-1}(W))$.

Theorem 5.3. A function $f_{co} : (X_{TO}, \tau) \to (Y_{TO}, \sigma, I_{ide})$ is a $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$ pre (I_{ide}, J_{ide})-open (resp. $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$ semi (I_{ide}, J_{ide})-open, $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}\beta$ I_{ide} -open) function on condition that for individual subset $E \subseteq Y_{TO}$ besides respective closed set M of X_{TO} encompassing $f_{co}^{-1}(E)$, there occurs a $pre(I_{ide}, J_{ide})$ -closed (resp. $(\gamma, \gamma')_{op}$ semi (I_{ide}, J_{ide}) - closed, $(\gamma, \gamma')_{op}\beta(I_{ide}, J_{ide})$ -closed) set $K \subseteq Y_{TO}$ containing E such that, $f_{co}^{-1}(K) \subseteq M$.

Proof. Proof is alike that of 5.2. Theorem.

Corollary 5.2. Accredit $f_{co} : (X_{TO}, \tau) \to (Y_{TO}, \sigma, I_{ide})$ be a function.

(i) If f_{co} is a $(\gamma, \gamma')_{op}$ semi (I_{ide}, J_{ide}) -open function, at that moment f_{co}^{-1} $(\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}^{*}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(D)))\subseteq$ $\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(f_{co}^{-1}$ $(D))$ aimed at any subs D of Y_{TO}.

(ii) In case f_{co} pre (I_{ide}, J_{ide}) -open function, formerly f_{co}^{-1} $(\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}^{*}$ $(D))) \subseteq \tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$ $(f^{-1}$ $(D))$ for any subset D of Y_{TO}.

(iii) If f_{co}. is a $(\gamma, \gamma')_{op}\beta$ (I_{ide}, J_{ide}). -open function, at that time f_{co}^{-1} $(\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}$ $(\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$. $(\tau_{\alpha(\gamma,\gamma')op}$-$int_{op}^{*}$ $(D))))\subseteq$ $\tau_{\alpha(\gamma,\gamma')op}$-$cl_{op}$. $(f_{co}^{-1}$ $(D))$ for a subs D of Y_{TO}.

Proof. Authentication is analogous to that of 5.1. Corollary.

6 Applications and Implications

The novel application enriched concept of $\alpha(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$ $(I_{ide,}J_{ide,})$-$\mathcal{C}$ontinuous $\mathcal{F}$unctions, $\alpha(\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide,}J_{ide,})$- $\mathcal{F}$unctions be applied and implied to study new concepts alike: $\alpha - (\gamma, \gamma')_{op}(\beta, \beta')_{op}$ - contra continuous $\mathcal{F}$unctions, closed functions, Hausdorff spaces, $\mathcal{C}$ onnected spaces, $\mathcal{C}$ ompact spaces, Regular spaces, Normal spaces. Further the idea of $\alpha(\gamma, \gamma')_{op}(\beta, \beta')_{op}(I_{ide,}J_{ide,})$- *continuousfunctions*.can be utilized to extend the idea to various types of *Continuous Functions*. Like: Totally and strongly continuous functions, generalized continuous functions.

7 Conclusion

The operators namely -int_{op}, cl_{op} int_{op}^{*}., cl_{op}^{*} are properly utilized to explain the thought, properties as well interrelationship among the novel *continuousfunctions*: $\alpha(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$ $(I_{ide,}I_{ide,})$-$\mathcal{C}$ ontinuous $\mathcal{F}$ unctions, $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-semi-$(I_{ide,}I_{ide,})$-uous $\mathcal{F}$ unctions, $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-pre -$(I_{ide,}I_{ide,})$-$\mathcal{C}$ ontinuous $\mathcal{F}$ unctions, $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-semi-$(I_{ide,}I_{ide,})$-open functions and $(\gamma, \gamma')_{op} - (\beta, \beta')_{op}$-pre -$(I_{ide,}I_{ide,})$-open functions are explained in this article. In addition, $\alpha(\gamma, \gamma')_{op} - (\beta, \beta')_{op}(I_{ide,}I_{ide,})$-open functions are obtained with their basic properties. They are premeditated through suitable illustrations and their nature has been learnt.

References

1. Njåstad, O.: On some classes of nearly open sets. Pac. J. Math. **15**(3), 961–970 (1965). https://doi.org/10.2140/pjm.1965.15.961
2. Levine, N.: Semi-open sets and semi-continuity in topological spaces. Am. Math. Mon. **70**(1), 36–41 (1963). https://doi.org/10.1080/00029890.1963.11990039
3. Corson, H.H., Michael, E.: Metrizability of certain countable unions. Ill. J. Math. **8**(2), 351–360 (1964)

4. Mashhour, A.S.: On precontinuous and weak precontinuous mappings. In: Proc. Math. Phys. Soc. Egypt. Vol. 53, pp. 47–53 (1982)
5. Andrijevic, D.: Semi-preopen sets. Mat. vesnik **38**, 24–32 (1986)
6. Andrijević, D.: On the topology generated by preopen sets. Matematički Vesnik **39**(100), 367–376 (1987)
7. Kasahara, S.: Operation-compact spaces. Math. Japon. **24**, 97–105 (1979)
8. Ogata, H.: Operations on topological spaces and associated topology. Math. Japon. **36**, 175–184 (1991)
9. Kalaivani, N., Krishnan, G.S.S.: Operation approaches on α-γ-open sets in topological spaces. Int. J. Math. Anal. **7**(10), 491–498 2013. https://www.m-hikari.com/ijma/ijma-2013/ijma-9-12-2013/kalaivaniIJMA9-12-2013.pdf
10. Kalaivani, N., Saravanakumar, D.: Certain Separation Axioms and R _ i R i Spaces with α _ γ _ o α γ o-open sets. In: Proceedings of First International Conference on Mathematical Modeling and Computational Science: ICMMCS 2020, pp. 601–613. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4_55
11. Kalaivani, N., Chandrasekaran, E., Hachimi, H.: A Study About (γ, γ) α–Regular Spaces, Normal Spaces with (γ, γ)–Open Sets and α (γ, γ)–Open Sets. In: Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science: ICMMCS 2021, pp. 1–10. Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9_1
12. Kuratowski, K.: Topology: Volume I, Vol. 1. Elsevier (2014)
13. Hayashi, E.: Topologies defined by local properties. Math. Ann. **156**(3), 205–215 (1964)
14. Samuels, P.: A topology formed from a given topology and ideal. J. Lond. Math. Soc. **2**(4), 409–416 (1975). https://doi.org/10.1112/jlms/s2-10.4.409
15. Janković, D., Hamlett, T.R.: New topologies from old via ideals. Am. Math. Mon. **97**(4), 295–310 (1990). https://doi.org/10.1080/00029890.1990.11995593
16. Reilly, I., Vamanamurthy, M.: On α-continuity in topological spaces. Acta Math. Hungar. **45**(1–2), 27–32 (1985). https://doi.org/10.1007/bf01955019
17. Kalaivani, N.: On Operation Approaches on -open sets and -Continuous Functions in Ideal Topological Spaces. (submitted)
18. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
19. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
20. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4

Fog Computing-Based Fault Tolerant Data Management Model (FC-FTDMM) for Smart Healthcare

J. Devagnanam[1], D. Balaganesh[2(✉)], Saurabh Adhikari[3], and Srividhya Murali[4]

[1] Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankularhur, Chengalpattu (DT), TN, India
devagnaj@srmist.edu.in

[2] Berlin School of Business and Innovation GmbH, Karl-Marx-Straße 97-99, 12043 Berlin, Germany
duraisamy.balaganesh@berlinsbi.com

[3] School of Engineering, Swami Vivekananda University, Barrackpore, India

[4] Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology (SRMIST), Kattankulathur, Chennai, India
srividhb@srmist.edu.in

Abstract. Cloud computing has revolutionized healthcare data management, leading to better patient care. Most healthcare organizations now use cloud-based software and related services to provide superior healthcare facilities. The primary goals of fog computing are to address the issues of cloud computing's energy usage, network latency, and bandwidth. Managing data generated by healthcare IoT devices is another important application of fog computing. Data generated by healthcare IoT devices is enormous and requires efficient processing with low latency, zero failures, low energy consumption, and low cost. Hence this paper, Fog Computing based Fault Tolerant Data Management Model (FC-FTDMM), has been proposed for healthcare data management. Processing and encrypting the collected physiological signals are done using the Advanced Secured Encryption Algorithm (ASEA) before its transmission to the cloud. Healthcare IoT device data is structured and handled effectively in FC-FTDMM using well-defined components and stages. FTDM provides a two-way fault-tolerant mechanism for tasks and node failures: task-based and node-based fault tolerance. The findings display the FC-FTDMM for performance assessment data management ratio of 92.1% and 93.2%, latency of 0.21 ms and 0.2 ms, and decision-making ratio of 96.5% compared to other methods.

Keywords: Cloud Computing · Fog Computing (FC) · Advanced Secured Encryption Algorithm (ASEA) · Healthcare

1 Introduction

The IoT refers to a new interconnected network that allows for the wireless transmission and reception of data from nearby smart devices and objects. [1]. Almost every piece of physical equipment these days is internet-enabled; this includes smart kegs, drones, smart

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 37–47, 2025.
https://doi.org/10.1007/978-3-031-91008-1_4

ovens, smart household appliances, smart watches, and healthcare gadgets [2]. Daily, this IoT produces enormous amounts of data. Due to the many ways in which IoT devices have the potential to enhance patient and disease management, the healthcare sector is one of the largest users of these devices [3]. With fewer medical professionals and fewer facilities, better management is also essential. However, communication overhead would rise with such massive device connectivity [4]. Conventional clouds are experiencing problems with bandwidth, energy consumption, resilience, delay, and latency problems due to the increased demand [5]. A developing concept known as fog computing has emerged to address these issues and to improve the cloud's bandwidth, delay, and latency [6]. Public databases, healthcare organizations, and insurance firms are some of the places that may get healthcare data. With the use of the cloud, healthcare institutions are trying to manage patient data better to provide better treatment [7]. Healthcare system development using third-party cloud computing resources will make things easier [8]. Most of these services fall into one of many categories, including computing, storage, databases, security, management tools, or migration. In the cloud, these web services revolutionized data intake, storage, and processing [9].

Fog computing allows for synchronising storage, processing, and network capabilities provided by traditional cloud data centres with IoT devices [1]. Reducing latency, cutting energy use, and providing efficient fault tolerance mechanisms remain areas where fog computing has room to grow in the healthcare IoT. Hence, to show how these limitations affect fog computing-based efficient data management for healthcare IoT.

The main contribution of this paper.

i) Designing the proposed FC-FTDMM has been proposed for gathering and managing the data in healthcare.
ii) The proposed FC-FTDMM uses the Advanced Secured Encryption Standard algorithm (ASEA) to secure data transmission in the cloud.
iii) A numerical analysis has been conducted, and the suggested FC-FTDMM is used to achieve execution time, latency, network utilization, execution cost, and energy consumption.

The upcoming section is as follows: Sect. 2 describes the related works, Sect. 3 deliberates the proposed methodology, Sect. 4 discusses the numerical results and discussion, and Sect. 5 concludes the overall paperwork.

2 Related Works

The blockchain-based patient-centric healthcare information management framework (BCP-CHIMF) provides secure data storage and access [10]. Blockchain technology is a promising new solution for protecting the privacy of real-time control systems. With the right amount of luck, this will provide the groundwork for a blockchain-based security system for medical videos. This is accomplished using the blockchain system's hashing capabilities, which record all data throughout the system in case of a major security breach.

Attribute-Based Encryption (ABE) Metaverse Healthcare Data Sharing Scheme (ABE-MHDSS) for metaverse ciphertext validity and equivalence detection capabilities [11]. A novel method of delegation of authority has been developed, which utilizes attribute-based re-encryption. Several servers work together to provide offline intermediate ciphertexts, which users may use to aid with encryption.

Internet of Things (IoT)-based real-time remote patient monitoring system (R-TRPMS) to guarantee the precision of the critical real-time signal [12]. The suggested technique communicates with the website using the MQTT protocol, which transmits the critical real-time signal. This effort aims to assess and interpret patients' vital signs while reducing signal transmission delay.

Artificial intelligence-powered decentralized framework (AI-PDF) for healthcare data management to gather distant patient medical data and maintain PHR will be implemented [13]. Smart contracts are enhanced with an extra layer of rule-based AI that can identify malicious nodes and make smart judgments.

Interplanetary file systems (IPFSs) with blockchain technology provide a scalable EHR-sharing system for e-health apps in the cloud [14]. Cloud-based data management, Data optimization, and medical data security [16–20] have been elaborately described in the related previous proceedings and research papers. To ensure the security of shared healthcare data, they have created a reliable access control technique using smart contracts. The effectiveness of the suggested strategy is examined using a compatibility test using a cloud-based IoT setup. The study showed that the suggested method may work in many e-health environments.

3 Proposed Methodology

The high number of connections, fog computing, a novel paradigm in computing also has efficiency concerns. This paper suggests a systematic approach to enhance the reliability and performance of fog computing for healthcare IoT data management. It suggests implementing two tiers of fault tolerance: one for jobs and another for devices/nodes. The proposed FC-FTDMM for the healthcare Internet of things (IoT). The article offers fault-tolerant mechanisms for transfer and task retry at the fog device/node level and FTDM at the task level respectively.

The suggested model's design is laid out in this section. The overall structure of FC-FTDMM is shown in Fig. 1. The decision maker comes in last, followed by the data analyst and scheduler, the fault-tolerant provider, and the data collector. These four parts make up FC-FTDMM. In addition to organising and managing healthcare data (such as BP, HR, RR, and BT) produced by IoT devices, the FC-FTDMM scheme offers dual FT at the task and device/node levels.

IoT devices generate patient healthcare data, which the "Data Collector" collects. Data is then analysed and scheduled using the "Data Analyser and Scheduler" component. Data-related activities are also assigned to fog computing resources by this portion. If tasks are done successfully, the "Decision Maker" component receives the outcome. If not, FTDM will be used. This level's "FTDM" addresses "Task-based fault tolerance (TFT)" and "IoT devices/nodes-based fault tolerance (IoT-FT)." If a node fails, "TFT" tasks are re-executed at other fog nodes if the scheduler keeps a copy of the job until

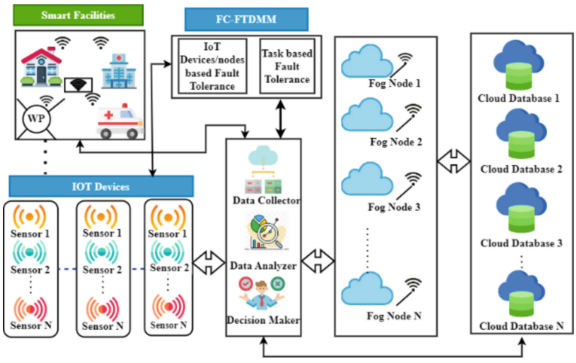


Fig. 1. The proposed FC-FTDMM

they are done. Second, "IoT-FT" claims that if a node fails in a fog, its duties are transferred to a non-failing node using the retained tasks. Data from the "Data Analyser" is sent to the "Decision Maker". This component classifies data as normal or abnormal. Patient health data is commonly stored in data centres. Aberrant data endangers patients. The ESP8266 Crypto library implements AES for the module. A 128-bit key is used for Cypher block chaining (CBC) mode encryption and Base64 encoding to secure sensitive data. Uploading to the cloud. AES is used to encrypt sensor readings since it may be implemented in hardware with the correct software library.

On top of that, it strikes a nice balance between computational speed and complexity. The IoT module incorporates several biomedical sensors that measure critical vital signs to avoid needing a local server or an intermediary mobile app. The data is then processed by a Wi-Fi-based microcontroller using the AES algorithm and sent directly to the cloud database over Wi-Fi. Patients with mobility issues or who are old may find this process more comfortable since it is automated and does not need their active participation."Decision Maker" will alert both the patient's and the consultant's devices when it receives data that is out of the ordinary. Various configurations of nodes for sensors, edge devices, and cloud data centres have been considered in the fog-based computing environment. In a healthcare setting, the end users, patients, acquire healthcare data from sensors placed at the far end of a geographic region. For the application scenario's sake, they presumed that patients would have various sensors implanted throughout their bodies to track their vital signs and other health-related data. A fog database would house the healthcare data temporarily for decision-making before it is permanently saved in cloud data centres for future reference. Algorithm 1 establishes the sequential process of the FTDM scheme.

Algorithm 1: FTDM

Input: δ represents the IoT devices-based healthcare Data, ρ explores the data storage

Output: α examines the IoT devices-based Healthcare Data

1. Procedure FTDM (δ)
2. Data Collector ()
3. **While** data analysis and data scheduling task/ node failed ()
4. **do**
5. FT provider ()
6. **then**
7. Analysis of IoT Data
8. Decision making ()
9. Data Storage for ρ ()
10. **Exit**

The first algorithm describes FTDM in depth. The Data Collector gathers healthcare-related IoT data from sensors including respiration rate, temperature, blood pressure, and heart rate. After receiving the raw data, the Data Collector will categorise vital indications including heart rate, blood pressure, temperature, and blood sugar. Healthcare IoT data will be planned and analysed using Data Analyser. Internet of Things devices analyse patient vital signs. These include the patient's temperature, heart rate, blood pressure, breathing, and blood sugar. Many methods are being developed to analyse medical data to determine whether it is normal. Such techniques demand computing resources. Next, organise the resources needed to complete the tasks obtained from the assessed data. When tasks or nodes fail, the FTDM takes over. The FT Provider will retry a task if it fails.

Many fog nodes are available for work dispersal. If a fog node issued a work fails, the Scheduler will replicate it on another node. The Scheduler is intended to retain a copy of fog node tasks until they are done. The same assumption applies to proposed work. The decision-maker receives data after reviewing and completing tasks. First, divide the data into normal and abnormal. Data Storage will store regular data in cloud data centres. This patient health data is accurate. Unusual data endangers patients and should be avoided. The "Decision Maker (DM)" alerts the patient and consultant when aberrant data is detected.

Figure 2 displays the suggested healthcare system that is built on the cloud. Data in healthcare environments come from various sources, including clinical and non-clinical settings. Genome sequencing data, x-ray, ultrasound, and magnetic resonance imaging (MRI) pictures, digitized data from medical equipment, and data from wearable and sensing devices make up the clinical data. Some examples of non-clinical data include survey results, social media information, and insurance claim records. Clinical data from healthcare organizations is the primary focus of the suggested design. Information being ingested, stored, and processed are the primary phases of the suggested healthcare web architecture. A collection of cloud services may manage data to activate the process

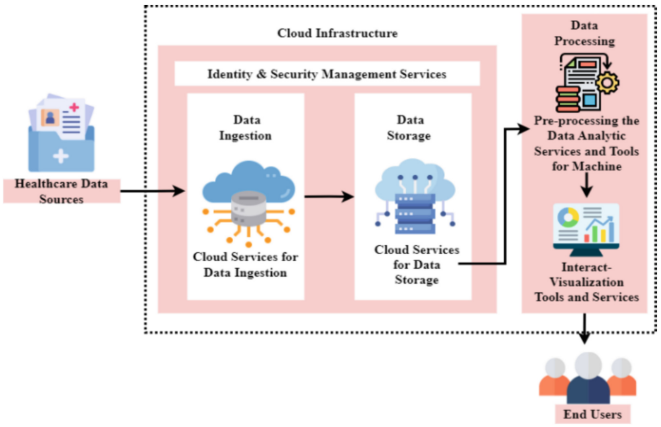


Fig. 2. Healthcare Data Management Based on Cloud Infrastructure

across all phases. In the healthcare lifecycle, data intake is the first stage. At this point, gathering raw data from all over the healthcare system's data sources. Data intake may utilise a wide range of cloud services tailored to a certain use case. The data is saved in the cloud once cleaned and filtered. Whether or not data stored in the right cloud will be required for analytics or processing in the future depends on the data. Data processing to conclude is the final step. The people who would ultimately benefit from this cloud-based solution are those involved in healthcare. To complete the work, data may be managed using the right cloud services from a cloud provider at each step.

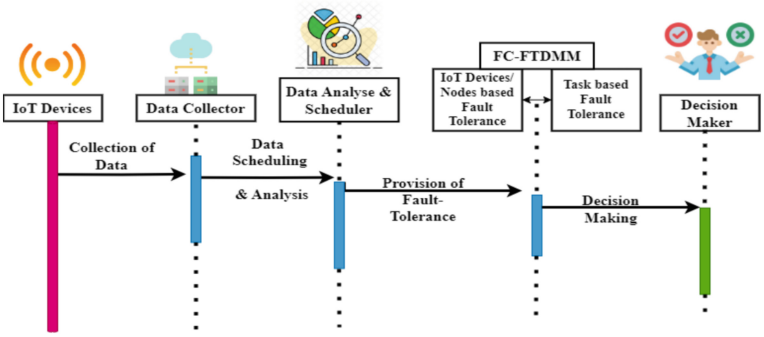


Fig. 3. Sequence Diagram of Proposed FC-FTDMM

Figure 3 depicts the data flow in FTDM. After patients provide data via Internet of Things (IoT) devices, the Data Collector will store the information in a database or fog device. After data collection, it is forwarded to the Data Analyzer and Scheduler to check for accuracy and allocate resources to run tasks. If anything goes wrong with any nodes or jobs, the FT Provider part will try again or move them to another node. Following a successful examination and execution, the DM will have the data necessary to make an appropriate choice. Two groups will be created from the data: normal and

abnormal. Patients' health and future data usage will be protected by cloud data centres' preservation of normal data.

On the other hand, if aberrant data is detected, an alert will be sent to both the patient's and the consultant's IoT devices. Fog computing is an infrastructure for highly virtualized computing that uses a vast network of geographically dispersed fog nodes to supply resources. Nodes in the fog computing network handle various processing and computational jobs. Avoiding FT approaches causes nodes and tasks in cloud and fog environments to fail, as it aims to maintain financial profit. As a result, we included two mechanisms—"TFT" and "IoT-FT"—to aid in fault tolerance. If the Scheduler ensures that each fog node has a copy of the job until it's finished, tasks with "TFT" are re-executed at other nodes if one node fails. Secondly, by "IoT-FT," if one node in an environment of fog fails, the other nodes will execute the tasks previously executed on the failed node using the duplicates of the tasks. This simulation-based study uses the fog computing simulator to test the efficacy of the suggested FTDM method.

4 Results and Discussion

Therefore, FC-FTDMM has been suggested in this article for managing healthcare data. The gathered physiological signals are processed and encrypted using the Advanced Secured Encryption Algorithm (ASEA) before their transfer to the cloud. Thanks to FC-FTDMM's clearly defined components and phases, data from healthcare IoT devices is organized and processed efficiently. FTDM deals with failures in tasks and nodes by two methods: TFT and IoT-FT.

Dataset Description: Data scientists, ML specialists, and data analysts will find this synthetic healthcare dataset invaluable. With its realistic representation of healthcare data, users may hone their data manipulation and analysis abilities while gaining valuable experience in the field. With detailed information on patients, their admittance, and healthcare services included in each column, this dataset is ideal for a wide range of healthcare-related data analysis and modelling projects [15].

Experimental Setup: There are 20, 40, 60, 80, 100, 120, 140, and 150 IoT devices statistical test cases in the database of use cases for the remote medical platform. This division is based on the number of patients: 10, 20, 30, 40, and 50. Electronic health record (EHR) medical history is the database's test case. Table 1 shows the test's fundamental scenario.

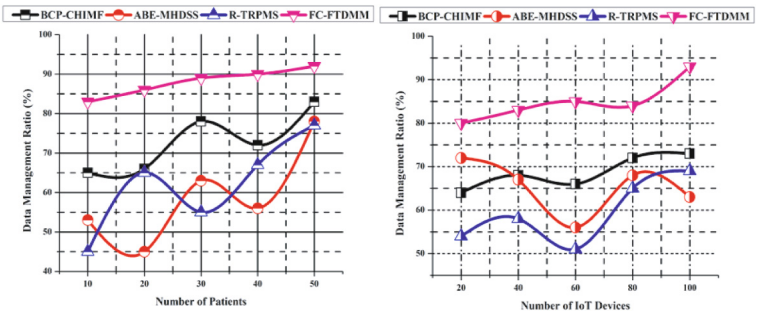
i) Data Management Ratio (%)

When some nodes in a fog computing architecture fail, the data will still be available continuously because of the redundancy and failover techniques included in the design.

This fault tolerance reduces the possibility of data loss and keeps vital applications running, which is especially important in the healthcare industry where data availability is paramount. By spreading the workload over several nodes, fog computing makes data management scalable. Figure 4 (a) and (b) show the data management ratio. The ability to rapidly adapt to different data loads helps healthcare providers accommodate regular

Table 1. Test's Fundamental Scenario

Number of Parameters	Value
Number of Patients	10, 20, 30, 40, 50
Number of IoT Devices	20, 40, 60, 80, 100, 120, 140, 150
Simulation Time	120 s
Average response time	$\leq$ 20 s
Average CPU Usage	$\leq$ 80%

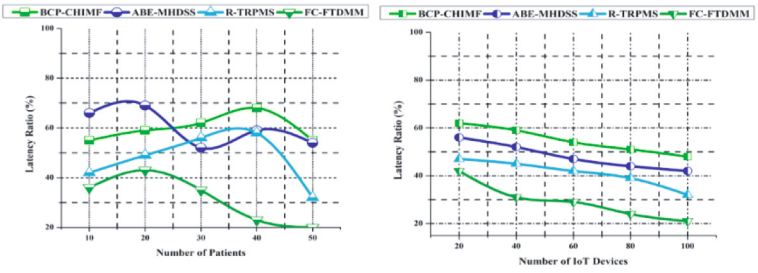


(a) (b)

Fig. 4. Data Management Ratio (%)

patients and large-scale medical imaging data without sacrificing efficiency. Fog nodes process data locally, reducing bandwidth consumption by sending the most critical data to the cloud. This innovation is especially useful for medical imaging and continuous monitoring of data streams in healthcare facilities.

ii) Latency Ratio (%)



(a) (b)

Fig. 5. Latency Ratio (%)

Figure 5 shows the latency ratio in both (a) and (b). For instance, sensors, monitoring, and medical supplies are Internet of Things devices that might benefit from fog computing since it puts hardware and software closer to the data source. Fog computing is also becoming more popular in the healthcare industry. To reduce latency, this proximity is crucial for applications in the healthcare industry that need real-time processing and retrieval. Some examples of these kinds of applications include patient monitoring and emergency response. A few examples of Internet of Things devices that might profit from fog computing are sensors, monitors, and healthcare devices. This is because fog computing puts the abilities of computers closer to the data source, which is beneficial in healthcare situations. The ability to pre-fetch data that will be requested shortly and cache data that is often accessed is something that fog nodes can do. Caching helps reduce latency by eliminating the need to repeatedly retrieve data from remote servers, a common occurrence in healthcare systems. Repetitive data access patterns are usual in many healthcare systems. To reduce latency, this proximity is crucial for applications in the healthcare industry that need immediate data collection and retrieval. Some examples of these applications include monitoring patients and emergency response.

iii) Decision Making Ratio (%)

There is a possibility that the network connectivity in healthcare facilities would be unpredictable. Fog computing enables important healthcare services to continue operating despite connectivity issues, enabling the processing and storage of data using local resources. Fog computing makes it possible to analyze data instantaneously at the edge, enabling real-time analytics. This is made possible by limiting the impact of interruptions related to fog computing.

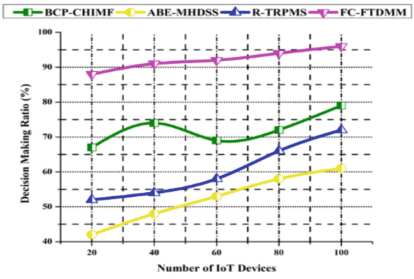


Fig. 6. Decision-Making Ratio (%)

A discussion of the decision-making ratio is shown in Fig. 6. The capability of local fog nodes to gather and assess data from various sources, including ambulance telemetry and patient histories, enables local fog nodes to facilitate speedy decision-making in emergencies. Nodes may process data in the fog near the network's edge, where it originated. Local processing avoids the need to transfer data to remote cloud servers and back again, enabling rapid analysis and decision-making while removing the latency associated with sending data to cloud servers. Because of the use of this capability in predictive analytics and other healthcare applications, it is feasible to achieve better

patient results and make more efficient use of the resources available in the healthcare system.

5 Conclusion

The purpose of this study is to demonstrate FC-FTDMM as a way of handling data related to healthcare. Processing and encryption of the obtained physiological signals are performed with the help of the ASEA before they are uploaded to the cloud. Because of its well-defined components and phases, FC-FTDMM can quickly organize and handle data from other Internet of Things devices in the healthcare industry. FTDM provides a two-pronged approach to fault tolerance. One of these approaches takes into consideration tasks, while the other takes into account nodes. Results show that the FC-FTDMM performs well on a data management ratio of 92.1% and 93.2%, a latency of 0.21 ms and 0.2 ms, and a decision-making ratio of 96.5% compared to other methods.

References

1. Parks, R.F., Wigand, R.T., Benjamin Lowry, P.: Balancing information privacy and operational utility in healthcare: proposing a privacy impact assessment (PIA) framework. Eur. J. Inf. Syst. **32**(6), 1052–1069 (2023)
2. Panwar, A., Bhatnagar, V., Khari, M., Salehi, A.W., Gupta, G.: A blockchain framework to secure personal health record (PHR) in IBM cloud-based data lake. Compu. Intell. Neurosci. **2022**, 1–19 (2022). https://doi.org/10.1155/2022/3045107
3. Miyachi, K., Mackey, T.K.: HOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf. Process. Manage. **58**(3), 102535 (2021)
4. Enticott, J.C., et al.: A learning health system framework to operationalize health data to improve quality care: an Australian perspective. Front. Med. **8**, 730021 (2021)
5. Rathee, G., Sharma, A., Saini, H., Kumar, R., Iqbal, R.: A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology. Multimed. Tools Appl. **79**(15), 9711–9733 (2020)
6. Kamath, V., Lahari, Y., Mohanchandra, K.: Blockchain based framework for secure data sharing of medicine supply chain in health care system. Int. J. Artific. Intell. **9**(1), 32–38 (2022)
7. Iqbal, N., Jamil, F., Ahmad, S., Kim, D.: A novel blockchain-based integrity and reliable veterinary clinic information management system using predictive analytics for provisioning of quality health services. IEEE Access **9**, 8069–8098 (2021)
8. Egala, B.S., Pradhan, A.K., Badarla, V., Mohanty, S.P.: Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. IEEE Internet Things J. **8**(14), 11717–11731 (2021)
9. Chamola, V., Goyal, A., Sharma, P., Hassija, V., Binh, H.T.T., Saxena, V.: Artificial intelligence-assisted blockchain-based framework for smart and secure EMR management. Neural Comput. Appl. **35**(31), 22959–22969 (2023)
10. Taloba, A.I., et al.: A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare. Alex. Eng. J. **65**, 263–274 (2023)
11. Zhang, T., Shen, J., Lai, C.F., Ji, S., Ren, Y.: Multi-server assisted data sharing supporting secure deduplication for metaverse healthcare systems. Futur. Gener. Comput. Syst. **140**, 299–310 (2023)

12. Alshammari, H.H.: The internet of things healthcare monitoring system based on MQTT protocol. Alex. Eng. J. **69**, 275–287 (2023)
13. Puri, V., Kataria, A., Sharma, V.: Artificial intelligence-powered decentralized framework for Internet of Things in Healthcare 4.0. Trans Emerging Tel Tech **35**(4), e4245 (2024)
14. Chinnasamy, P., Albakri, A., Khan, M., Raja, A.A., Kiran, A., Babu, J.C.: Smart contract-enabled secure sharing of health data for a mobile cloud-based E-health system. Appl. Sci. **13**(6), 3970 (2023)
15. https://www.kaggle.com/datasets/prasad22/healthcare-dataset
16. Peng, S.-L., Jhanjhi, N. Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
17. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4
18. Pal, S., Jhanjhi, N.Z., Shawkat Abdulbaqi, A., Akila, D., Alsubaei, F.S., Almazroi, A.A.: An intelligent task scheduling model for hybrid internet of things and cloud environment for big data applications. Sustainability **15**(6), 5104 (2023). https://doi.org/10.3390/su15065104
19. Tuan, N.A., Akila, D., Pal, S., Sarkar, B., Tran, T.K., et al.: Dynamic data optimization in iot-assisted sensor networks on cloud platform. Comput, Mater. Continua **72**(1), 1357–1372 (2022). https://doi.org/10.32604/cmc.2022.024096
20. Doss, S., Paranthaman, J., Gopalakrishnan, S., Duraisamy, A., Pal, S., et al.: Memetic optimization with cryptographic encryption for secure medical data transmission in iot-based distributed systems. Comput. Mater. Continua **66**(2), 1577–1594 (2021). https://doi.org/10.32604/cmc.2020.012379

A Cramer-Shoup Algorithm and 5D Hyper-Chaotic System as Pseudo Random Number Generator

Zainab Khalid Ibrahim(✉) and Ekhlas Abbass Albahrani

Mustansiriyah University, Baghdad, Iraq
Zainab86khalid48@gmail.com, akhlas_abas@uomustansiriyah.edu.iq

Abstract. Worldwide, random numbers are used in many different applications. It's challenging to generate high-quality random numbers using just a simple encryption technique, particularly for Internet of Things (IoT) sensors as well as other devices with limited hardware capabilities. In the presented work, a new pseudorandom number generator is designed based upon a 5D hyper-chaotic system and the Carmer-Shoup encryption algorithm. The benefit of the suggested algorithm is its simplicity, which makes it easy to carry out for Graphics processing unit (GPU) hardware or internet of thing(IoT) systems with extremely limited processing capacity. The generated random numbers show encouraging statistical behavior and satisfy the requirements regarding the NIST statistical suite where ratio η of p-value concerns the first set of sequences within the range of [0.99247, 0.99949], correlation coefficient between generated sequences are good where Pearson's correlation coefficient distributions are within the range of [−0.1055,0.1055], hamming distance coefficients belong to [0.415,0.555], all Summation of absolute difference (SAD) results within the range of [0.338054,0.378866] are near optimal values, and key space of the suggested PRNG is very large, which was 2^{266}.

Keywords: Cramer-Shoup algorithm · 5D hyper-chaotic · pseudo-random number · internet of thing (IOT) · NIST statistical suite

1 Introduction

Random number generation is highly valued in numerous fields of computer science, such as Monte Carlo simulations, cryptography, and other computer applications (R. F. W. Coates, G. J. Janacek et al., 1988) [1]. Pseudorandom number generators (PRNGs) have drawn a lot of research attention, and random numbers were produced using a variety of mathematical techniques, including chaos theory and number theory. Data is encrypted and decrypted with the use of public as well as secret keys in asymmetric cryptography, which is referred to as the public-key cryptography as well. Large integers that had been paired together but aren't identical (asymmetric) serve as the keys. Some of those huge numbers are prime numbers (for example, P & Q in RSA), while others are random numbers that are used to produce session keys, making unpredictability the

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 48–64, 2025.
https://doi.org/10.1007/978-3-031-91008-1_5

most crucial factor in ensuring the veracity of a system. In 1984, T. ElGamal introduced a public-key system depending upon discrete logarithms. Also, digital signature standard (DSS) uses ElGamal cryptosystem. One feature that both keys have in common is that it is not computationally possible to generate private key from a public key. As with symmetric encryption, brute-force attacks can break public-key encryption systems. Use huge keys for the same solution. A compromise should be thought of nonetheless. An invertible mathematical function is used in public-key systems. With more bits in the key, the complexity of calculating these functions could increase more quickly than linearly (W. Stallings 2023) [2]. Hellman and Diffie developed a solution that addressed both issues (key distribution, Diffie wondered), and achieved a remarkable breakthrough in 1976. Among the most popular PKE schemes is the ElGamal scheme. The degree of difficulty of the DDH (i.e., Decisional Diffie–Hellman) problem determines its indistinguishability under chosen plaintext attacks (IND-CPA) security. Since Cramer-Shoup algorithm is the first effective indistinguishability under the chosen cipher-text attacks (IND-CCA) secure scheme in a standard model, it is significant (D. Pointcheval et al., 2022) [3]. There are two keys used by the Cramer-Shoup algorithm, Diffie-Hellman, and RSA to encrypt and decrypt public and private keys. Pseudorandom number sequences are often employed in communication and digital computer applications. Never repeat a bit of pattern in an entirely random order. It is quite challenging to construct such a practical system sequence (R. Oppliger, version 2021) [4]. A random yet user-predictable disappearance is required by various programs. Repeatability and rapidity of sequences, which demand less memory for algorithm storage, are the primary benefits of the generator (J. J. Bird, A. Ekárt at al., (2020) [5]; (C. E. Shannon, (1998) [6]. The unique characteristics of randomness and apparent chaos have drawn a lot of interest to the field of mathematics known as chaos theory. Diverging and disorderly sequences which seem random, yet are predictable and highly sensitive to initial conditions could be produced by chaotic systems (S. Oishi et al., (1976) [7]. Those characteristics make chaotic systems a preferable option for the PRNGs. While a great deal of research was done on chaos-based PRNGs, not as much has been done on chaotic maps (J.-R. Chazottes, 2010) [8]. The outline of this study may be abstracted as follows: Sect. 4 shows fundamental hypothesis of hyperchaotic system and Cramer–Shoup encryption algorithm; Sect. 5 presents the proposed PRNG and Sect. 6 exhibits statistical as well as security investigation regarding the suggested system before the conclusion.

1.1 Objectives

1) This study aims to design an algorithm for the generation of pseudorandom numbers through benefitting from properties of public key algorithms, in particular the Carmer-Shoup encryption algorithm. Since this algorithm has proven its ability to resist an adaptive chosen ciphertext attack.
2) Utilize the cramer-shoup encryption algorithm as a reliable pseudo -random key generator.
3) In each iteration, the proposed generator creates 250 different integer numbers, which makes this generator suitable for applications that require numerous different numbers
4) The suggested system is investigated and analyzed with the use of various tests to assess their correlation, key space, and key sensitivity. They are further tested utilizing

the NIST statistical test suite. To conduct the testing, 1000 unique random binary sequences each of 1500 bits with close initial values were produced. To confirm the performance of the suggested PRNG, the randomness and correlation are verified for each string that is created.

It may be crucial to consider the proposed PRNG's ease of implementation in hardware or software packages when making real-world implementations.

2 Related Works

Numerous studies in the literature have been published that build on the construction of PRNGs based on various types of public key algorithms and chaotic maps. (Alexie et al., 1988) [9] demonstrate how to construct pseudorandom sequences using the RSA exponentiation. (Blume et al., 1986) [10] investigate squaring-based pseudorandom sequences, assuming that quadratic residuality is intractable. In general, computationally secure pseudo-random generators enable users to boost security by choosing more difficult cases of the intractable issue. The efficiency of sequence generation, on the other hand, comes at a cost. Using chaotic systems as PRNGs has lately been the subject of numerous proposals (Q. Deng et al., 2020) [11]; (F. Yu et al., 2021) [12]; (F. Yang et al. 2020) [13]; (F. Yu, (2020) [14]; (Q. Wan et al., 2020) [15]; (Z. Wen et al., 2020) [16]. A wide range of current areas, such as PRNG (Y. Li et al., 2020) [17]; (Xiu et al., 2021) [18] and secure communication (F. Yu et al., 2021) [19]; (L.-H. Dong et al. 2016) [20]; (F. Yu et al., (2019) [21]; (M. Tuna, (2020) [22], heavily utilize chaotic systems. A random number generator for various entropy sources depending on 3D quadratic hyper-chaotic systems is provided by (Chen et al., 2020) [23]. The generated 3D entropy sources have been subjected to the XOR operation in order to create random sequences with excellent characteristics that passed the NIST and ENT tests. A futuristic method for a chaotic map protected through gene dominance and depending on PRNG was suggested by (S. Krishnamoorthi et al., 2021) [24]. A 2D logistic map was made more random by using biological gene dominance. The sequences that are generated are validated using NIST SP800-22 test suite. Results showed that every sequence passed testing. Parameters such as key sensitivity, information entropy, and others have been simulated in order to make sure they can be used in cryptographic applications. In (M. M. Al-Mhadawi et al., 2023) [25], an innovative chaotic PRNG relies upon a combination of SHA2(256) randomization and randomization of three 2-D chaotic systems: 2-D Tinkerbell map, 2-D Kaplan-Yorke map, and 2D Henon map. Six floating-point numbers are used as a key in the suggested chaotic generator to generate the initial values that are supplied to chaotic maps. Those values are used as input into SHA2 (256) in order to generate chaotic maps' starting values. Next, using binary XOR operation and the 2-D shifting scrambling approach, chaotic binary sequence is processed to increase sequence complexity.

In this study, powerful pseudo-random numbers are designed using the Cramer-Shoup encrypted method and 5^{th}D hyper-chaotic system to generate 1500 integer numbers in one iteration. Along with 250 integer numbers, the five initial values—floating point numbers with a precision value of (10^{-16}) and falling within a range of [0, 1]—are fed into the hyper-chaotic system to generate the Carmer–Shoup algorithm's encryption key. Carmer-Shoup approach is used for the purpose of encrypting each of such integers,

and the resultant encrypted value is split into six integer values within the interval [0-255].

3 Paper Organization

The outline of the present study can be abstracted as follows: Sect. 4 shows the fundamental hypothesis of hyperchaotic system and Cramer–Shoup encryption algorithm; Sect. 5 presents the proposed PRNG and Sect. 6 exhibits the statistical as well as security investigation regarding the suggested system before the conclusion.

4 Related Theory

The suggested technique in this study is based on the 5-D Lorenz method and the Cramer-Shoup encrypted technique.

4.1 5D Hyper Chaotic System

The conventional Lorenz system (N. Lorenz, 1963) [26] can be expressed as:

$$\begin{aligned} \mathrm{X}_1 &= \sigma \mathrm{y}_0 - \sigma \mathrm{x}_0, \\ \mathrm{Y}_1 &= r\mathrm{x}_0 - \mathrm{y}_0 - \mathrm{x}_0\mathrm{z}_0, \\ \mathrm{Z}_1 &= \mathrm{x}_0\mathrm{y}_0 - b\mathrm{z}_0 \end{aligned} \tag{1}$$

Regarding the 2D Rayleigh-Benard thermal convection process, a fluid that is contained between 2 plates positioned in perpendicular manner to gravitational attraction of Earth is cooled from above and heated from below. Reference (B.-W. Shen, 2014) [27] had looked into Lorenz model in 5 dimensions, that can be expressed in following equation (C. C. Felicio, 2018) [28]:

$$\begin{aligned} \mathrm{X}_1 &= \sigma(y_0 - x_0), \\ Y_1 &= rx_0 - y_0 - x_0z_0, \\ \mathrm{Z}_1 &= x_0y_0 - bz_0 - x_0v_0, \\ \mathrm{V}_1 &= x_0z_0 - 2x_0u_0 - (1+2b)v_0, \\ \mathrm{U}_1 &= 2x_0v_0 - 4bu_0 \end{aligned} \tag{2}$$

In which (x0, y0, z0, v0, u0) denote initial values and the system is hyperchaotic in a case where the values of constant parameters are $\sigma = 10$, b = 8/3, and r = 100. Equation 1 and Eq. 2 differ in that two new 1st-order ordinary differential equations and 2 extra dynamical variables, u and v, have been added. There are 2 additional non-linearities also: xu in v formula and xv in u & z equations. Due to the fact that the non-linearities are the chaos source, it is expected that the system solutions (2) will have a higher level of chaos in comparison with system solutions (1).

4.2 Cramer-Shoup Algorithm

R. Cramer and V. Shoup were the scientists that presented the algorithm of Cramer-Shoup encrypted as mentioned in 1998, which is a system of public key encryption that has been based on 2 concepts that are employed often in the modern cryptography: discrete logarithm problem and decisional Diffie-Hellman assumption. It uniquely combines flexibility, security, and efficiency. In contrast to some other methods of encryption, Cramer-Shoup method provides provable guarantees of security against the chosen cipher-text attacks, making it one of the popular choices in the applications where it is critical to have a high level of security. An interactive chosen-cipher-text attack where attackers provide numerous cipher-texts to be decrypted and after that utilize results of those decryptions for choosing new cipher-texts. The Cramer-Shoup is highly effective as well and could be deployed for swiftly encrypting massive data volumes, this algorithm is adaptable enough as well for supporting a wide range of the cryptographic primitives that include secure digital signatures and hash functions (R. Cramer et al., 1998) [29]. Below are Cramer-Shoup encryption/decryption steps:

A. ***Key Generation*:** Assuming G is a prime order group q, in which q denotes large and clear text that which is parts of G. Additionally, a universal family of 1-way hash functions which map size bit strings to the Zq elements has been utilized.

- Generation of the public key: first choose 2 random numbers, g_1 & $g_2 \in G$, 5 numbers x_1, x_2, y_1, y_2 & $z \in Zq$ and H a 1-way hash function. Public key includes x_1, x_2, g_1, g_2, H, y_1, z, & y_2.
- The generation of private keys: calculating additional values, c, d, & h, with the use of the equations below:

$$c = g_1^{x1} g_2^{x2} \tag{3}$$

$$d = g_1^{y1} g_2^{y2} \tag{3}$$

$$h = g_1^{z} \tag{4}$$

Private key consists of c, d, & h.

B. ***Encryption***: in a case where plaintext is $r \in Zq$ and $m \in G$ where r represents a random number, then calculate:

$$u_1 = g_1^{r} \tag{6}$$

$$u_2 = g_2^{r} \tag{7}$$

$$e = h^r m \tag{8}$$

$$\alpha = H(u_1, u_2, e) \tag{9}$$

$$v = c^r d^{r\alpha} \tag{10}$$

The resulting cipher text is (u_1, u_2, e, v) v).

C. ***Decryption***: let ciphertext (u_1, u_2, e, v), then plaintext m may be retrieved by initially calculating α with theuse of Eq. (9) and check if condition $u_1^{x_1+y_1\alpha} u_2^{x_2+y_2\alpha} = v$ isn't true, then the algorithm of decryption returns "reject"; in the other case, it give back original message m as depicted below:

$$m = \frac{e}{u_1^z} \tag{11}$$

5 Proposed PRNG

The proposed algorithm consists of two main steps which are:

- **Initial step:** in this step, the key encryption for the Cramer-Shoup algorithm and 250 integer numbers are created through using 5D hyperchaotic system Eq. (2) as shown in the following:

  a. The initial values (x_o, y_o, z_o, v_o, u_o) are floating point values a (10^{-16}) precision with [0,1] range, and control parameters (σ, , r, & b) are input variables to Eq. (2).
  b. The 5-D hyperchaotic system is iterated for a number of times until the generation of all of the Cramer-Shoup keys that are prime number q, 2 integer numbers (g_l & g_2) < q, and 5 numbers x_l, y_l, x_2, y_2, z ∈ Zq.
  c. 5D hyper-chaotic system is iterated for a number of times again for the purpose of generating 250 integer numbers. In each iteration, the outputs of chaotic system are converted into integer numbers using the following equation:

$$out_i = \text{floor}\left(I_i \text{X} 10^6\right) mod\ 999 \tag{12}$$

  where i = 0, 1…5, I_0 is one output of the resulting five hyper-chaotic system and out_i is an array of the 250 resulting integer numbers.

- **Generation step:** in this step, 1500 integer numbers are generated as shown in the following:

a. Each value in the *out* array is encrypted using the Cramer-Shoup algorithm with the keys (q, g_1, g_2, x_1, x_2, y_1, y_2, z) where they are generated in the initial step.

b. Each encrypted result from the Cramer-Shoup algorithm is divided repeatedly into a set of integer numbers until it becomes zero based on the following three equations:

$$\text{R} = \text{C}\ mod 997 \tag{13}$$

$$\text{Ni} = \text{R}\ mod 256 \tag{14}$$

$$\text{C} = CDIV\,256 \tag{15}$$

where C is the encrypted result from the Cramer-Shoup algorithm, Ni is the resulting integer number, and i = 1, 2…n.

For example, let C= 1.7936e X 10^{13} then first iterate R= 154, Ni=154, and C=7.0062X 10^{10}, then second iterate R=429, Ni=173, and C=273678336, third iterate R=839, Ni=71, and C=1069056, and so on, then the results of the variable Ni referred to in the above equation (14) are collected in array ss = [154,173,71,16,188,16].

c. Steps a and b are repeated until 1500 integer numbers are generated.

These steps are repeated more times when the required random number is more than 1500.

6 Experimental Results

The sequence generated by the Cramer-Shoup and 5D hyperchaotic systems can be tested for efficacy. The sequences should be highly random.

6.1 Statistical Analysis

Numerous tests, including the NIST tests, coefficient, and hamming distance, are applied to binary sequences and are randomly examined in statistical analysis.

A. **Randomness evaluation: -** The NIST test suite's 15 statistical tests have been employed, and the NIST's recommendations were taken into consideration (A. Rukhin et al., 2023) [30]. A binary sequence is deemed successful if the null hypothesis value of 0.01 is accepted. A ratio η is defined for each test as the percentage of successfully passed sequences for numerous sequences tested simultaneously. The confidence interval is used to compare the ratio to an acceptable ratio, where the range of permitted proportions can be indicated as follows:

$$p \pm 3\sqrt{\frac{p(1-p)}{n}} \tag{16}$$

For our PRNG, the ratio η is $0.99 \pm 3\sqrt{\frac{0.99 \times 0.01}{1000}} = 0.99 \pm 0.00943$. This indicates that the percentage should fall within the range [0.99943, 0.98056]. Based on the length of the binary sequence, NIST tests are divided into two sets. Sequences longer than 100 bits should be subjected to the first set, while sequences longer than 1000000 bits should be subjected to the second set. For the first set, the proposed PRNG creates 1000 files, each comprising 1500 bits. These 1000 files are concatenated to perform one binary sequence file as the second set. The outcomes of the NIST tests run on the two sets have been shown in Tables 1 and 2.

B. Pearson's coefficient of correlation for the pair of sequences $x = [x_1, \ldots\ldots, x_N]$ and $y = [y_1, \ldots\ldots, y_N]$ is (R. Cybulski, 2021) [31]; (T. K. Alshekly et al., 2022) [32].

$$C_{s1_s 2_2} = \frac{\sum_{i=0}^{n-1} (x - x') \cdot (y - y')}{\sqrt{\sum_{i=0}^{n-1} (x - x')^2 \cdot \sum_{i=0}^{n-1} (y - y')^2}} \tag{17}$$

Table 1. NIST test results for the first and second sets of 1000 produced binary sequences, where the η ratio concerns the first set and p-value concerns the second set.

Test	Number. of individual	Result	p-value of concatenate	Result
Frequency	0.99498	passing	0.06288	passing
Block frequency	0.99699	passing	0.62398	passing
Runs	0.99548	passing	0.75007	passing
Longest Run	0.99699	passing	0.32500	passing
Rank	0.99899	passing	0.73226	passing
F.F.T.	0.99949	passing	0.22227	passing
Non-overlapping	0.99941	passing	0.12815	passing
Serial one	0.99247	passing	0.86375	passing
Serial two	0.99599	passing	0.99774	passing
Cumulative sums	0.99548	passing	0.04928	passing

Mean values:

$$X' = \frac{\sum_{i=0}^{n-1} x_i}{N} \tag{18}$$

$$Y' = \frac{\sum_{i=0}^{n-1} y_i}{N} \tag{19}$$

It is one of the standards for statistical analysis that considers binary sequences and figures out how to compare each of the two-binary series. Pearson correlation coefficient (PCC) measures the correlation between each of the two sequences. Figure 1 shows that the higher PCC is in the range of [0.005 - 0.0115], while the correlation coefficient value falls between [−0.1055 - 0.1055]. This suggests that there is little association between the sequences which were created.

C. **Hamming Distance**

The number of the locations where the matched symbols differ determines hamming distance between 2 equal-length symbol strings (L.F. Jalil et al., 2015) [33]; (N. H. Ghayad et al., 2019) [34].

$$(S, S') = \frac{1}{n} \sum_{J=0}^{M-1} (S_j \oplus S'_J) \tag{20}$$

True random binary sequences should have a hamming distance proportion of roughly 0.50 (D (S, S') / L). Figure 2 displays a distribution histogram of all the hamming values that were found for each one of the pairs of the 1000 sequences that were produced.

Table 2. NIST test results for 2nd set of 1000 generated binary sequences.

Test	p-value of concatenate	Result
Overlapping	0.87996	Passing
Universal	0.04391	Passing
Linear complexity	0.14353	Passing
Approximate Entropy	0.55409	Passing
Random Excursions (8p-values)	0.80643 0.48454 0.946083 0.719262 0.15089 0.29068 0.47160 0.89361	Passing
Random E-variant (18 values)	0.35114 0.49333 0.35442 0.25540 0.27092 0.19494 0.47254 0.85122 0.758982 0.08316 0.13081 0.77138 0.84318 0.70468 0.86175 0.74869 0.63455 0.89552	Passing

6.2 Security Analysis

Always provide some security evaluations with any new PRNG proposals. When doing the analysis, all crucial aspects of the cryptographic and cryptosystem needs could be considered. Key space, key sensitivity, and SAD evaluation of the outputs are the points that were examined.

A. **Key space: -** Keeping brute-force attacks in mind, the suggested PRNG should have a large key space. Furthermore, a key space with a size of $< 2^{128}$ is insufficiently secure. Since an attacker will attempt to decrypt an intercepted image using every possible key combination, a message with a larger key space will be more resistant to an analytical attack (M. M. Al-Mhadawi et al., 2019) [35]. The key space in the

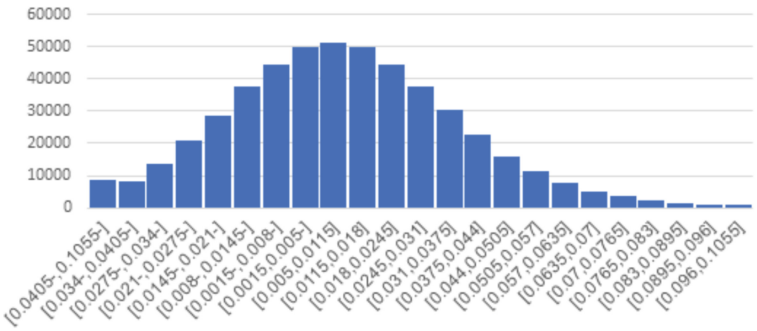


Fig. 1. Histogram of PCC of proposed PRNG.

suggested PRNG is comprised of the initial values regarding 5D hyper-chaotic x0, y0, z0, v0, and u0 ∈ [0, 1] where they are floating point values with 10^{-16} precision. So, the total key space is $((10^{16})^5) \approx 2^{266}$.

B. **Key sensitivity: -** Any key stream generator must be sensitive to changes in key parameters (F. Yu et al., 2019) [36]. An essential element of PRNG is the key's sensitivity. Stated differently, the resultant binary sequences must be uncorrelated if the initial values differ by a little amount (B. A. Hameedi et al., 2022) [37]. To verify the sensitivity regarding the key, 2 tests have been conducted between 4 large binary key-stream sequences, Z2, Z1, Z4, and Z3, each having a length of N = 1500,000 bits and generated from somewhat different initial values as indicated in Table 3: the Hamming distance and PCC. Pearson's Correlation Coefficient hamming distance results for 4 generated binary sequences have been displayed in Table 3. The findings demonstrate how closely related the four sequences are to one another.

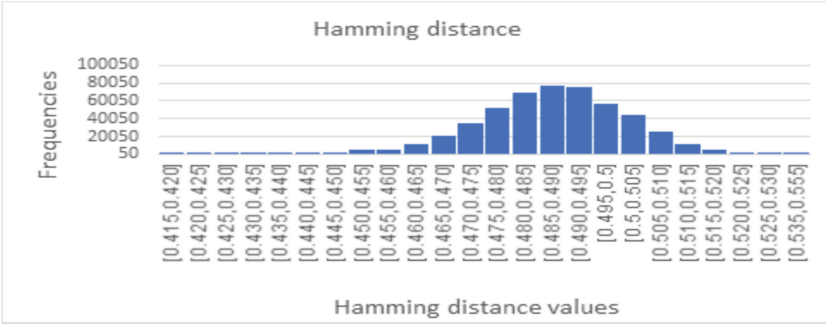


Fig. 2. Hamming distance Histogram for 1000 produced sequences on the interval [0.415 - 0.555].

C. **Summation of Absolute Difference (SAD):-** It calculates the absolute sum of the difference between the bits of the binary sequence and divides it along the binary sequence. This test investigates and regulates how a small number of input pairs affect corresponding output pairs. The most likely key that has been utilized for supplying a

keystream sequence can be found using this approach. The four binary sequences—Z2, Z1, Z4, and Z3—that are utilized to confirm the suggested generator security against differential attacks are displayed in Table 4. With the use of equation, the SAD between each pair of sequences is modified (S. Du et al., 2023) [38]:

$$\text{SAD} = \frac{\sum_{j=0}^{N-1} \left| Z(i) - Z'(i) \right|}{N} \tag{21}$$

In which N represents the binary sequence's length.

Table 4 presents the SAD results. The ideal value of 1/3 is extremely close to all SAD values in Table 4, suggesting that the suggested chaotic PRNG generator is quite resistant to such kind of attacks. Figure 3 shows us that the number of repetitions of bits regarding all values is 0.338054, which is the lowest value in the second series' convergence of bits and the maximum value in the binary sequence's convergence of bits, which is 0.378866.

Table 3. Initial values for four sequences that have been created by the suggested chaotic PRNG.

Binary Sequence	Initial value
Z1 Sequences	Xo = 0.6543215423138654 Yo = 0.2346742132426692 Zo = 0.3493873221362159 Vo = 0.4597865434218874 Uo = 0.4586754389328762
Z2 Sequences	Xo = 0.6543215423137654 Yo = 0.2346742132425692 Zo = 0.3493873221462159 Vo = 0.4597865434218974 Uo = 0.4586754389348765
Z3 Sequences	Xo = 0.653215423137554 Yo = 0.2346742132425682 Zo = 0.3493873221462259 Vo = 0.4597865434218774 Uo = 0.4586754389338762
Z4 Sequences	Xo = 0.6543215423237554 Yo = 0.2346742132435682 Zo = 0.3493873221463259 Vo = 0.459786534217874 Uo = 0.4586754389338772

6.3 Speed Analyses

Another important component of any PRNG is the algorithm's execution time. The implementation time limitation of an algorithm is just as significant in real-time applications as the algorithm's result. A PC running Windows11, Core (TM) i5-10500H CPU

Table 4. Hamming distance, Pearson's correlation coefficient, and SAD amongst four binary sequences, Z2, Z1, Z4, and Z3

Tests	Correlation coefficient	Hamming distance	Summation of absolute difference
Z1/Z2	0.0264	0.4765	0.378866
Z1/Z3	0.0328	0.4825	0.352994
Z1/Z4	−0.00083	0.4961	0.369997
Z2/Z3	0.087	0.4891	0.338054
Z2/Z4	0.0072	0.4906	0.339121
Z3/Z4	0.0056	0.4965	0.352758

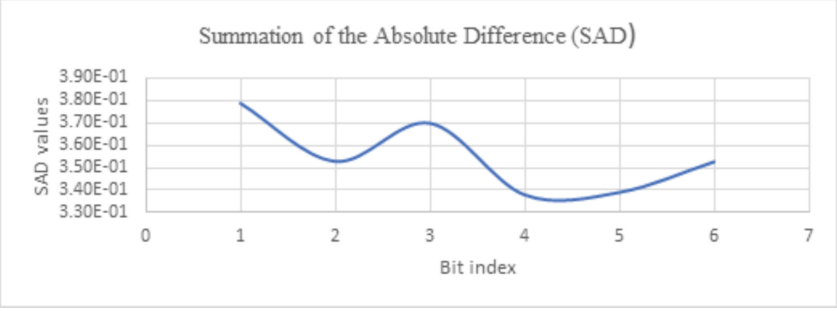


Fig. 3. Histogram of SAD values between four binary sequences.

running at 2.50GHz, and MATLAB (v. R-2021-B) software are used to conduct the speed performance analysis. A total of 4 binary sequences of various length values are produced by this technique, and their execution times are computed. In a linear connection, time grows in proportion to the series' length. Table 5 displays the speed performance regarding the proposed PRNG method.

Table 5. Speed analyses of proposed PRNG

Sequence name	Sequence length in Mb	Speed in Mbps
Z1	1 Mb	2.697685
Z2	1.5 Mb	7.990189
Z3	2 Mb	15.384911
Z4	2.5 Mb	24.884740

7 Comparison of Different PRNG Methods

However, only modern PRNG algorithms based on chaotic systems and asymmetric encryption algorithms bear comparison to the proposed approach. Several other PRNG techniques are comparable to it. The NIST results of the suggested approach are compared to five distinct PRNG algorithms as in [25, 34, 35] (F. Yu, et al., 2021) [39]; (S. Cang et al., 2021) [40] as shown in Table 6. The key space size, entropy analyses, correlation analysis, NPCR, PSNR, MSE, and UACI are some of the crucial criteria we chose to enable us to compare algorithms included (R. N. AL-Zubaidy et al., 2018) [41] from different angles as can be listed from Table 7. Key sensitivity results of every algorithm are compared in Table 8. Every algorithm has completed every test, as can be seen from the results of the comparison. The assessments vary, though, depending upon the test type. For example, our recommended algorithm can generate a higher number of bits in every iteration than other algorithms, but it can still come close to the optimal result for some tests, such as some NIST results and key space, which implies that the suggested PRNG is similar to its competitors concerning both security and efficiency.

Table 6. Comparison results of the NIST suite

NIST	PRNG	(M.M et al.,2023)[25]	(N.H et al2019)[34]	(M.M et al.,2023)	(M.M et al.,2023)	(S.Cang et al.,2018) [40]
Frequency	0.062885	0.493775	0.016305	(M.M et al.,2023)	(M.M et al.,2023)	0.933056
Block frequency	0.623989	0.461850	0.973046	0.154719	0.001030	0.999446
Runs	0.750074	0.845096	0.306669	0.378780	0.779188	0.094921
Longest Run	0.325007	0.449349	0.463475	0.824662	0.037566	0.270854
Rank	0.732261	0.214816	0.017461	0.775032	0.637119	0.163913
FFT	0.222278	0.905040	0.117107	0.790145	0.719747	0.147084
Non-overlapping	0.128152	0.396311	0.031318	0.418218	0.983453	0.303428
Serial- one	0.863758	0.430696	0.064610	0.449137	0.000000	0.521320
Serial -two	0.997743	0.223485	0.017822	0.529291	–	0.258425
Cumulative sums	0.049280	0.590388	0.031041	0.897325	0.080519	0.988063
Overlapping	0.879968	0.387742	0.506101	0.626731	0.275709	0.730712
Universal	0.043911	0.707283	0.171345	0.476473	0.983454	0.024228
Linear complexity	0.143530	0.754221	0.279591	0.393639	0.595549	0.205766
Approximate Entropy	0.554097	0.719241	1	0.0127361	0.000000	0.451267
Random Excursions	0.946083	0.994202	0.943313	0.897009	0.982743	0.899358

Table 7. Comparison results in key space, number of the bits in every one of the iterations, and correlation coefficient results.

system	Key space	No. of bits in every one of the iterations	Person correlation coefficient results
Proposed PRNG	2^{266}	2000	[0.005 - 0.0115]
(M.M et al.,2023[25]	2^{319}	128	[−0.03.0.03]
(N.H et al2019)[34]	2^{213}	64	[−0.009,0.009]
(M.M etal,2019)[35]	2^{213}	160	[−0.0002,0.0004]
(R.N.et al.,2018)[41]	2^{133}	64	[−0.0072,0.0204]
(S.Cang et al.,2018) [40]	2^{192}	–	[−0.005,0.005]

Table 8. Comparisons of Pearson's correlation coefficient results and Hamming distance results with related works.

Sequences	Pearson's correlation coefficient				Hamming distance			
	PRNG	(M.M et al.,2023)[25]	(N.H et al2019)[34]	(M.M etal,2019)[35]	PRNG	(M.M et al.,2023)[25]	(N.H et al2019)[34]	(M.M etal,2019)[35]
Z1/Z2	0.0264	0.00011	0.006	−0.0002	0.4765	0.49994	0.424	0.50015
Z1/Z3	0.0328	−0.00018	0.006	0.0002	0.4825	0.50009	0.437	0.50013
Z1/Z4	−0.00083	−0.00108	−0.0008	0.0002	0.4961	0.50054	0.4344	0.49985
Z2/Z3	0.087	0.00096	0.004	0.0004	0.4891	0.49951	0.333	0.49977
Z2/Z4	0.0072	0.00033	−0.0032	−0.0008	0.4906	0.49983	0.4275	0.50043
Z3/Z4	0.0056	0.00030	−0.003	0.0009	0.4965	0.49984	0.431	0.50048

8 Conclusion

This study develops a new PRNG model for IoT devices that may be applied to a wide range of cryptographic applications. It produces random sequences with a large key space. This study suggested that the pseudo-randomness properties regarding a chaos-based PRNG be enhanced by employing the Carmer-Shoup approach, one of the public key encryption algorithms. The basic idea is to build an array of 5D chaotic map findings and use the Cramer-Shoup method for encrypting them. Every massive encryption is utilized to produce a set of whole numbers. 1500 integer numbers are generated in one iteration. The algorithm's sensitivity to initial values (keys), large key space size, the level of security against multiple attacks, and the quality of the generated keystream sequences are just a few of the various attributes that make the suggested PRNG useful in a wide range of cryptographic applications.

References

1. Coates, R.F.W., Janacek, G.J., Lever, K.V.: Monte Carlo simulation and random number generation. IEEE J. Sel. Areas Commun. **6**(1), 58–66 (1988). https://doi.org/10.1109/49.192730

2. Stallings, W.: Cryptography and network security: Principles and practice, global edition, 8th ed., Pearson Education, London, England (2023). ISBN: 978-0-13-609704-4
3. Pointcheval, D., A.: Cryptography, Primitives and Protocols (ISTE Ltd). John Wiley and Sons Inc. (2022)
4. Oppliger, R.: version 2021 Artech House. Cryptography 101 From Theory TO Practice (2020). ISBN: 978-1-63081-846-3
5. Bird, J.J., Ekárt, A., Faria, D.R.: On the effects of pseudorandom and quantum-random number generators in soft computing. Soft. Comput. **24**(12), 9243–9256 (2020). https://doi.org/10.1007/s00500-019-04450-0
6. Shannon, D.E.: Communication theory of secrecy systems. 1945. MD Comput., vol. 15, no. 1, pp. 57–64 (1998)
7. Oishi, S., Inoue, H.: Pseudo-random number generators and chaos. IEICE Trans **65**(9), 534–541 (1976). https://doi.org/10.1016/j.ifacol.2015.11.046
8. Chazottes, J.-R., Fernandez, B. (eds.): Dynamics of coupled map lattices and related spatially extended systems. Springer, Berlin, Germany (2010). https://doi.org/10.22630/MGV.2016.25.1.2
9. Alexi, W., Chor, B., Goldreich, O., Schnorr, C.P.: RSA and rabin functions: certain parts are as hard as the whole. SIAM J. Comput. **17**(2), 194–209 (1988). https://doi.org/10.1137/0217013
10. Blum, L., Blum, M., Shub, M.: A simple unpredictable pseudo-random number generator. SIAM J. Comput. **15**(2), 364–383 (1986). https://doi.org/10.1137/0215025
11. Deng, Q., Wang, C., Yang, L.: Four-wing hidden attractors with one stable equilibrium point. Int. J. Bifurcat. Chaos **30**(06), 2050086 (2020). https://doi.org/10.1142/S0218127420500868
12. Yu, E., Shen, H., Zhang, Z., Huang, Y., Cai, S., Du, S.: A new multi-scroll Chua's circuit with composite hyperbolic tangent-cubic nonlinearity: Complex dynamics, Hardware implementation, and Image encryption application. Integration (Amst.) **81**, 71–83 (2021). https://doi.org/10.1016/j.vlsi.2021.05.011
13. Yang, E., Mou, J., Ma, C., Cao, Y.: Dynamic analysis of an improper fractional-order laser chaotic system and its image encryption application. Opt. Lasers Eng. **129**(106031), 106031 (2020). https://doi.org/10.1016/j.optlaseng.2020.106031
14. Yu, E.: CCII and FPGA Realization: A Multistable Modified Fourth-Order Autonomous Chua's Chaotic System With Coexisting Multiple Attractors. Complexity pp. 1–17 (2020). https://doi.org/10.1155/2020/5212601
15. Wan, Q., Zhou, Z., Ji, W., Wang, C., Yu, F.: Dynamic analysis and circuit realization of a novel no-equilibrium 5D memristive hyperchaotic system with hidden extreme metastability. 2020," Complexity, pp. 1–16 (2020). https://doi.org/10.1155/2020/7106861
16. Wen, Z., Li, Z., Li, X.: Bursting dynamics in parametrically driven memristive Jerk system, Chinese," J. Phys. **66**, 327–334 (2020). https://doi.org/10.1016/j.cjph.2020.04.009
17. Li, Y., Li, Z., Ma, M., Wang, M.: Generation of grid multi-wing chaotic attractors and its application in video secure communication system, Multimed", Multimed. Tools Appl **79**, 29161–29177 (2020). https://doi.org/10.1007/s11042-020-09448-7
18. Xiu, R.Z., Zhao, S., Xu, G.: Memristive hyper chaos secure communication based on sliding mode control. Nonlinear Dyn. **104**(1), 789–805(2021). https://doi.org/10.1007/s11071-021-06302-9
19. Yu, D., et al.: Pseudorandom number generator based on a 5D hyperchaotic four-wing memristive system and its FPGA implementation: PRNG based on a 5D hyperchaotic four-wing memristive system and its FPGA implementation. Eur. Phys. J. Spec. Top. **230**(7–8), 1763–1772 (2021). https://doi.org/10.1140/epjs/s11734-021-00132-x
20. Dong, L.-H., Yao, G.-L.: Method for generating pseudo random numbers based on cellular neural network. J. Comm. **37**(Z1), 85–91 (2016). https://doi.org/10.11959/j.issn.1000-436x.2016252

21. Yu, D., et al.: Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map. IEEE Access **7**, 181884–181898 (2019). https://doi.org/10.1109/access.2019.2956573
22. Tuna, M.: A novel secure chaos-based pseudo random number generator based on ANN-based chaotic and ring oscillator: design and its FPGA implementation, Analog Integer. Analog Integer. Circuits Signal Process **105**(2), 167–181 (2020). https://doi.org/10.1007/s10470-020-01703-z
23. Chen, X.: Pseudorandom Number Generator Based On Three Kinds of Four- Wing Memristive Hyperchaotic System and Its Application in Image Encryption. Complexity, 1–17 (2020). https://doi.org/10.1155/2020/8274685
24. Krishnamoorthi, S., Jayapaul, P., Rajasekar, V.: A modernistic approach for chaotic based pseudo random number generator secured with gene dominance. Sādhanā **46**(1), 1–12 (2021). https://doi.org/10.1007/s12046-020-01537-5
25. Al-Mhadawi, M.M., Albahrani, E.A., Lafta, S.H.: Efficient and secure chaotic PRNG for color image encryption. Microprocess. Microsyst. **101**(104911), 104911 (2023). https://doi.org/10.1016/j.micpro.2023.104911
26. Lorenz, N.: Deterministic nonperiodic flow. J. Atmos. Sci. **20**(2), 130–141 (1963). https://doi.org/10.1175/1520-0469(1963)020%3c0130:DNF%3e2.0.CO;2
27. Shen, B.-W.: Nonlinear feedback in a five-dimensional Lorenz model. J. Atmos. Sci. **71**(5), 1701–1723 (2014). https://doi.org/10.1175/JAS-D-13-0223.1
28. Felicio, D.C., Rech, P.C.: On the dynamics of five- and six-dimensional Lorenz models. J. Phys. Commun. **2**(2), 025028 (2018). https://doi.org/10.1088/2399-6528/aaa955
29. Cramer, R., Shoup, V.: A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Advances in Cryptology — CRYPTO '98, pp. 13–25. Springer Berlin Heidelberg, Berlin, Heidelberg (1998). https://doi.org/10.1007/BFb0055717
30. Rukhin, A., et al.: A statistical test suite for random and pseudorandom number generators for cryptographic applications. Nist. gov (2023). https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762
31. Cybulski, R.: Pseudo-random number generator based on linear congruence and delayed Fibonacci method: Pseudo-random number generator based on linear congruence and delayed Fibonacci method," Tech. Sci., no. 2021 (2021). https://doi.org/10.31648/ts.7238
32. Alshekly, T.K., Albahrani, E.A., Ayed, L.B.: A novel parallel gray image cryptosystem based on hyperchaotic system and learning with error post quantum cryptography. In: 2022 3rd Information Technology to Enhance e-learning and Other Application (IT-ELA) (2022). https://doi.org/10.1109/IT-ELA57378.2022.10107955
33. Jalil, L.F., Saleh, H.H., Albhrany, E.A.: New pseudo-random number generator system based on jacobian elliptic maps and standard map. Iraqi Journal Of Computers, Communications, Control (2015). ISSN: 1811-9212
34. Ghayad, N.H., Albahrani, E.A.: A combination of two-dimensional hénon map and two-dimensional rational map as key number generator. In: 2019 First International Conference of Computer and Applied Sciences (CAS), pp. 107–112 (2019). https://doi.org/10.1109/CAS47993.2019.9075731
35. Al-Mhadawi, M.M., Albahrani, E.A.: Hybrid method as pseudo-random bits generator. In: 2019 First International Conference of Computer and Applied Sciences (CAS). pp. 250–255 (2019). https://doi.org/10.1109/CAS47993.2019.9075715
36. Yu, D., et al.: Design and FPGA implementation of a pseudorandom number generator based on a four-wing memristive hyperchaotic system and Bernoulli map. IEEE Access. **7**, 181884–181898 (2019). https://doi.org/10.1109/access.2019.2956573
37. Hameedi, B.A., Hattab, A.A., Laftah, M.M.: A pseudo-random number generator based on new hybrid LFSR and LCG algorithm. Iraqi J. Sci. 2230–2242 (2022). https://doi.org/10.24996/ijs.2022.63.5.35

38. Du, S., Ye, G.: IWT and RSA based asymmetric image encryption algorithm. Alex. Eng. J. **66**, 979–991 (2023). https://doi.org/10.1016/J.aej.2022-10-066
39. Yu, D., et al.: Design and FPGA implementation of a pseudo-random number generator based on a hopfield neural network under electromagnetic radiation, 9. Frontiers in Physics (2021). https://doi.org/10.3389/fphy.2021.690651
40. Cang, S., Kang, Z., Wang, Z.: Pseudo-random number generator based on a generalized conservative Sprott-A system. Nonlinear Dyn. **104**(1), 827–844 (2021). https://doi.org/10.1007/s11071-021-06310-9
41. AL-Zubaidy, R.N., Al-Bahrani, E.: New key generation algorithm based on dynamical chaotic substitution box. Al-Mansour International Conference on New Trends in Computing, Communication, and Information Technology, NTCCIT. Al-Mansour: IEEE (2018). https://doi.org/10.1109/NTCCIT.2018.8681187



Enhancing Safety and Accessibility with Integrated KNN and Repeated Median Regression in Wearable IoT Solutions

Harsh Vazirani[1(✉)], Xiaofeng Wu[1], Anurag Srivastava[2], Debajyoti Dhar[3], Divyansh Pathak[3], Sanskaar Srivastava[4], Sudip Banerjee[3], and Santosh Kumar Shahi[5]

[1] School of Aerospace, Mechanical and Mechatronic Engineering University of Sydney, Sydney, NSW, Australia
hvaz8919@uni.sydney.edu.au, xiaofeng.wu@sydney.edu.au
[2] Department of Engineering Sciences, ABV-Indian Institute of Information Technology and Management, Gwalior, India
[3] Department of Computer Science, ABV-Indian Institute of Information Technology and Management, Gwalior, India
[4] Department of Chemical Engineering, Indian Institute of Technology, Kanpur, India
sanskaars22@iitk.ac.in
[5] Department of Computer Science, Australian Institute of Higher Education, Sydney, NSW, Australia

Abstract. Throughout technological developments, women's safety in today's society continues to be a critical problem. The disadvantages of current treatments are frequently their mass, discretion lessness, and efficacy. In response, this study presents a brand-new wearable technology that combines regression and kNN algorithms to improve women's safety. The main goals are to design a small and easy-to-use gadget, utilize the kNN algorithm to forecast the closest safe location, and apply repeated median regression to analyze critical sensor data. This initiative intends to allow women to manage their personal and professional lives with security and confidence by eliminating the shortcomings of earlier systems. The suggested method ensures accessibility and adaptability by allowing for human activation in addition to automating emergency notifications. Furthermore, the system is a viable choice for broad adoption because to its affordability and simplicity of use. To further increase accuracy and efficacy, future improvements may integrate real-time environmental elements like crowd density and time of day. This study represents a major advancement in the use of technology to make spaces safer for women.

Keywords: kNN algorithm · robust repeated median regression · wearable IoT · safety technology · location tracking · accessibility

1 Introduction

Despite advances in technology and societal awareness, women's safety is a chronic dilemma [1] in modern society. Incidents of harassment and violence against women persist despite severe penalties for offenders, underscoring the need for creative solutions.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 65–73, 2025.
https://doi.org/10.1007/978-3-031-91008-1_6

Although a number of technologies have been developed to solve this problem, many of them have practical drawbacks such as bulkiness, lack of discretion, and limited efficacy in practical situations [1]. These flaws highlight the need for a more advanced and user-centered strategy for women's safety.

This study aims to provide a new wearable technology that is based on the Internet of Things and is particularly made to improve the safety of women. This technology prioritizes discretion, comfort, and user-friendliness in an effort to address the drawbacks of current alternatives. The gadget intends to enable women to pursue their career and personal interests fearlessly by blending in perfectly with normal clothing.

1.1 Objectives

User-Friendly Design. Create a wearable device that prioritizes ease of use, comfort, and discretion, ensuring that women can incorporate it seamlessly into their daily routines.

Enhanced Safety Features. Develop a compact and in conspicuous device equipped with vital sensors, GPS, and communication modules to provide real-time assistance in potentially risky situations.

Access Control Mechanisms. Implement robust access control mechanisms to ensure that only authorized individuals can activate and access the safety features of the device, minimizing the risk of misuse or tampering.

2 Literature Review

This research draws inspiration from existing studies in the field of women's safety technology. Specifically, a smart device proposed in previous research automates emergency alerts using various sensors to detect potential threats without requiring user interaction. While this system represents a significant advancement, it still faces challenges such as cost, accessibility, and reliance on wearable devices that may be easily identified and compromised by attackers [2].

2.1 Drawbacks of Existing Systems

Cost and Accessibility. The affordability and accessibility of existing safety devices may limit their effectiveness, particularly in economically disadvantaged communities.

Bulky and Non-Wearable Designs. Many existing de vices are cumbersome and conspicuous, making them impractical for everyday use. Even wearable solutions may be easily identified by attackers, compromising their effectiveness.

False Sense of Security. Relying solely on safety devices may lead to a false sense of security among users, potentially discouraging them from seeking additional assistance or taking precautionary measures.

In response to these challenges, this research proposes a comprehensive approach to women's safety that integrates wearable technology with advanced algorithms to

provide both automatic and manual assistance in emergency situations. By addressing the limitations of existing systems, this project aims to empower women to navigate their daily lives with confidence and security.

3 Methodology

This section outlines the comprehensive methodology employed in the development and implementation of the IoT based self-security system tailored for women's safety. The system integrates various components seamlessly to provide a comfortable, user-friendly, and effective solution, ensuring real-time monitoring, panic assistance, and location tracking capabilities [3].

3.1 System Architecture Design

The system architecture is structured around the integration of a wearable device, equipped with essential sensors and communication modules. Components include a smartwatch, vital sensor, fingerprint sensor, GPS, GSM, camera, and algorithms for location classification and vital data analysis.

3.2 Wearable Device Selection

A smartwatch is chosen as the primary wearable device due to its ubiquitous nature, ease of use, and compatibility with various sensors and communication technologies. The selected smartwatch offers a comfortable and unobtrusive form factor for continuous wear.

3.3 Sensor Integration

Vital sensors are incorporated into the wearable device to monitor crucial physiological parameters in real-time, ensuring timely assistance in case of distress. A fingerprint sensor is integrated for user authentication, ensuring that only authorized individuals can access the system's functionalities.

3.4 Communication Modules

GPS and GSM modules are utilized for location tracking and emergency communication. GPS enables accurate location fetching, while GSM facilitates the transmission of the user's current location and SOS messages to registered contacts. User privacy concerns are mitigated by following the principles of data reduction, which means that only the essential data needed for the system's operation is collected.

3.5 Image Capture Capability

A camera module is integrated into the wearable device to capture images of potential threats or perpetrators in the vicinity. This feature enhances the user's safety by providing visual evidence and aiding law enforcement authorities in identifying and apprehending suspects.

3.6 Algorithm Implementation

The KNN (K-Nearest Neighbors) algorithm is deployed to classify locations as safe or unsafe based on historical data and user-defined parameters. Regression using multiple medians is employed for vital sensor data analysis, allowing for the detection of anomalies and early warning signs indicative of distress [4].

3.7 User Interface Design

The system's user interface is designed to be intuitive, with simple navigation and clear feedback mechanisms [5]. Special attention is given to user experience, ensuring that individuals can easily access emergency features and initiate SOS protocols when needed.

3.8 False Positives and User Fatigue

In order to reduce the occurrence of incorrect positive results, we employ adaptive thresholding algorithms to modify the responsiveness of warnings according on user activity patterns and contextual information. To mitigate user fatigue, a hierarchical alert system is used, wherein minor notifications are consolidated, and only major alerts are given priority for instant user notice [9–11].

4 KNN Algorithm

Central to the system's functionality is the utilization of the K-Nearest Neighbors (KNN) algorithm for location classification, enhancing user safety by identifying safe and unsafe areas. The paper outlines the methodology, algorithm implementation, and practical considerations in designing and testing the system, emphasizing user-centric design principles and continuous improvement efforts. Results demonstrate the efficacy and reliability of the proposed solution in empowering women with enhanced security and peace of mind.

4.1 Working of KNN

The kNN algorithm is used to predict the nearest safe place based on the user's current location. It gathers and stores safe place coordinates as a dataset, then executes calculations using the user's location data. The algorithm's selection is crucial for effectively classifying safe places and determining the closest one, aligning with data classification requirements. The dataset includes diverse safe locations.

4.2 Implementation

Collection of Dataset. To gather our dataset, we initiated the process by identifying safe places within a specific area using Google Maps. This involved pinpointing lo cations like police stations, bus stands, and public areas deemed safe. For each identified place,

we recorded its latitude and longitude coordinates. This process was repeated iteratively until we accumulated 100 data points. This meticulously curated dataset serves as the cornerstone for our predictive algorithm, enabling swift and accurate determination of the nearest safe place for users within our self-security system. Table 1 provides a sample representation of the dataset.

Table 1. Sample Representation of the Dataset

Latitude	Longitude	Label
30.2029	93.6584	Police Station
18.6654	97.9488	Safe Area
18.1989	79.856	Public Place
17.6807	94.8041	Hospital
34.9227	80.3286	Police Station
31.0168	83.6724	Safe Area
13.4653	70.2462	Safe Area
37.1229	70.8667	Police Station
17.0906	68.1001	Safe Area

Choosing Suitable K Value. Determining the appropriate value for k in the kNN algorithm is critical for optimizing accuracy. This decision is contingent upon the dataset's characteristics, where accuracy serves as the primary metric for evaluation. Instead of manually adjusting k, a systematic approach involves plotting accuracy against different k values.

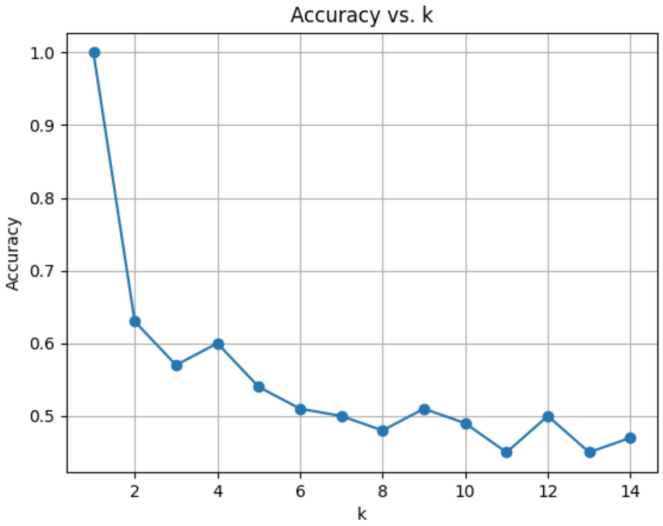


Fig. 1. A plot of accuracy vs the k values

In Fig. 1., it is evident that as k increases, accuracy tends to decrease. However, there exists a distinct point where accuracy peaks before declining. From the graphical representation, it is discernible that $k = 1$ or $k = 2$ yields the highest accuracy for the dataset. This data-driven methodology ensures the selection of the most suitable k value, thereby enhancing the performance and efficacy of the kNN algorithm within our self-security system.

Evaluation of kNN Algorithm. For the evaluation of the kNN algorithm, the confusion matrix is employed as a crucial tool. This two-dimensional matrix delineates predicted outputs in its rows and actual outputs in its columns, facilitating a comprehensive assessment of the algorithm's performance. By comparing predicted and actual outputs, insights into the algorithm's efficacy and accuracy can be gleaned.

Accuracy. In our evaluation, when the test data comprises 50% of the dataset, the training data also consists of 50%. This balanced distribution ensures that the algorithm receives an equal amount of data for prediction. Consequently, the algorithm achieves an accuracy rate of 87.5%, signifying its robust performance in accurately predicting results based on the provided data.

5 Robust Repeated Median Regression

The repeated median algorithm stands as a robust U-statistic, where nested medians replace the single mean, preserving a high 50% breakdown value and resilience against outliers, even when they account for a substantial portion of the data [7].

Formally, within a limited time frame denoted by $s = 1 \ldots n$ and $n \leq t$ wherein $\mu(t)$ represents the level of the linear function at the rightmost time point t, and $\beta(t)$ signifies

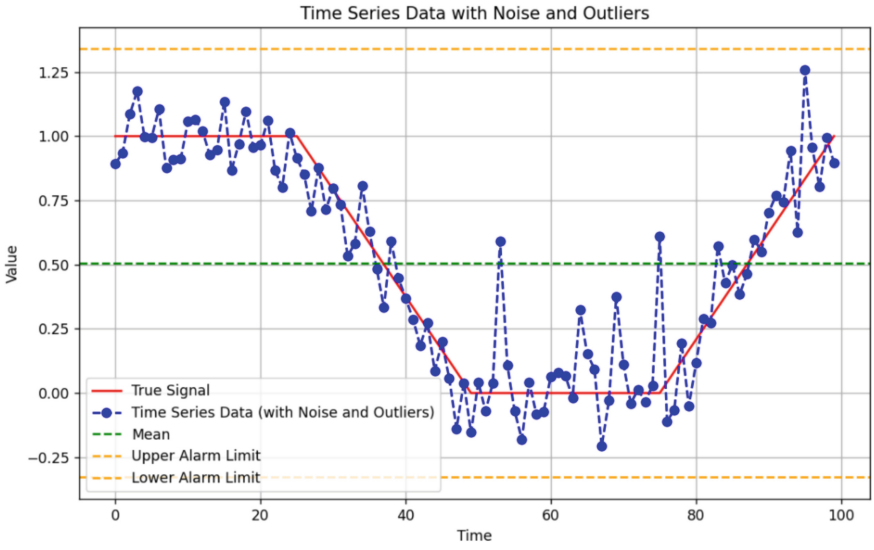


Fig. 2. Time series data consisting of the true signal overlaid with noise and outliers.

the associated slope within the time window. In the online context, the rightmost window time point t corresponds to the current time point. The Repeated Median (RM) estimates of $\mu(t)$ and $\beta(t)$ are derived accordingly. The methodology begins by assuming a constant rate of change akin to a straight line within a short period. This line.

$$\mu(t-n+s) \approx \mu(t) + \beta(t).(s-n) \tag{1}$$

$$\widehat{\beta^{RM}}(t) = \underset{s\varepsilon\{1,\ldots,n\}}{med}\left\{\underset{v\neq s, v\in\{1,\ldots,n\}}{med}\left\{\frac{y(t-n+s)-y(t-n+v)}{s-v}\right\}\right\},$$
$$\widehat{\mu^{RM}}(t) = \underset{s\varepsilon\{1,\ldots,n\}}{med}\left\{y(t-n+s)+\widehat{\beta^{RM}}(t)\cdot(s-n)\right\} \tag{2}$$

encapsulates two essential attributes: the level (initial value) and the slope (rate of change). It dynamically adjusts the window size as new data streams in, akin to zooming in or out on the graph based on the requisite level of detail to accurately capture evolving patterns, as illustrated in Fig. 2, which shows the time series data consisting of the true signal overlaid with noise and outliers.

Subsequently, within this adaptable window, it computes the median of differences between every pair of data points, facilitating the estimation of the line's slope. Once the slope is determined, the level of the line is estimated utilizing the Repeated Median method [2]. This entails identifying the median of points adjusted by subtracting the slope times their distance from the end of the window. The process of computing these differences and estimating the slope is depicted in Fig. 3, which demonstrates the aoRM algorithm.

In essence, the algorithm continually refines its perspective on the data, striving to identify the most linear trend within the current view. This linear trend serves as the basis for estimating the value at the present moment, ensuring robustness against sudden fluctuations and outliers in the data stream [8].

The efficacy of the robust repeated median regression is demonstrated through signal estimations, wherein sudden changes in the data result in overshooting by the solid

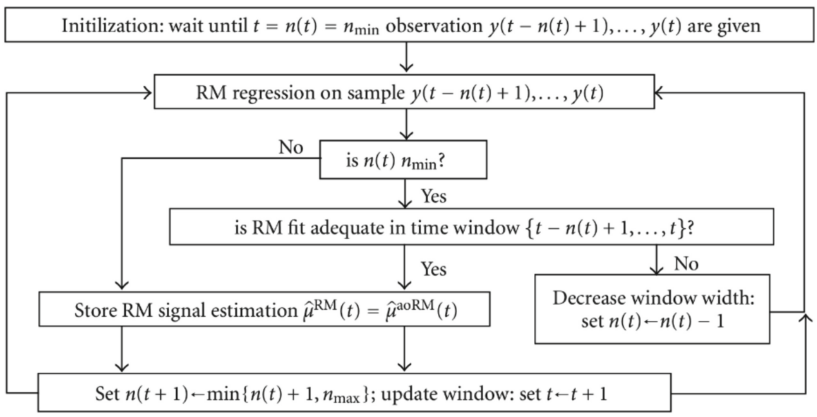


Fig. 3. The aoRM algorithm.

estimation curve, as shown in Fig. 4, which illustrates the aoRM signal estimations (solid) overshooting after sudden changes in the data (dotted).

Notably, the algorithm maintains stability even amidst spikes in vital signals, thereby enabling timely notification of potential anomalies or critical events.

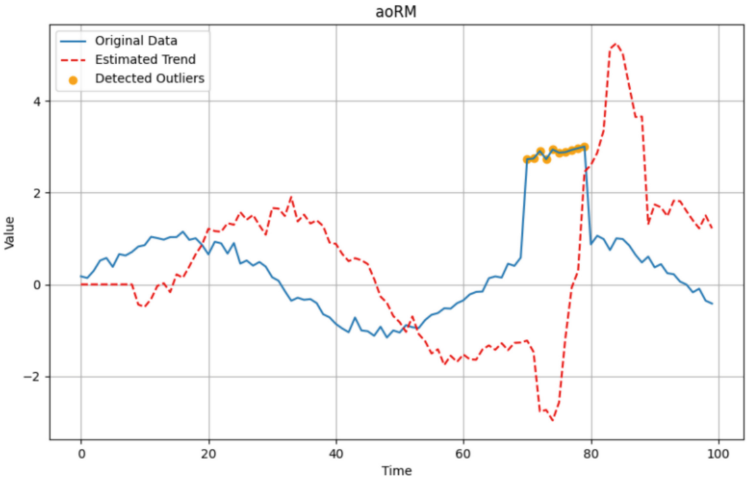


Fig. 4. aoRM signal estimations (solid) overshoot after sudden changes in the data (dotted).

6 Conclusion

In conclusion, our proposed smart device for women's safety represents a significant advancement in leveraging technology to safeguard individuals in vulnerable situations. By automating the emergency alert system and providing swift response mechanisms, our system ensures rapid assistance without the need for direct interaction from the user [6]. The integration of both automatic and manual functionalities adds versatility and empowers users to choose the mode of operation based on their preference or the severity of the situation.

Moreover, the cost-efficiency and user-friendly design make our system accessible to a wide range of users, addressing the need for practical solutions in ensuring women's safety. Looking ahead, further enhancements such as incorporating real-time crowd monitoring, time-of-day considerations, and alerts for potential snatching incidents could augment the accuracy and efficiency of our system.

References

1. Yaswanth, B.S., Darshan, R.S., Pavan, H., et al.: Smart Safety and Security Solution for women using KNN algorithm and IOT. Third International Conference on Multimedia Processing, Communication; Information Technology (MPCIT) (2020). https://doi.org/10.1109/mpcit51588.2020.9350431

2. Gupta, P., Goyal, Y., Gulati, D., et al.: Women's safety device based on internet of things. IEEE International Conference on Mobile Networks and Wireless Communications (ICMNWC) (2021). https://doi.org/10.1109/icmnwc52512.2021.9688529
3. Lee, S.-W., Mase, K.: Activity and location recognition using wearable sensors. IEEE Pervasive Comput. **1**, 24–32 (2002). https://doi.org/10.1109/mprv.2002.1037719
4. Siegel, A.F.: Robust regression using repeated medians. Biometrika **69**, 242 (1982). https://doi.org/10.2307/2335877
5. Hyndavi, V., Nikhita, N.S., Rakesh, S.: Smart wearable device for women safety using IOT. 2020 5th International Conference on Communication and Electronics Systems (ICCES) (2020). https://doi.org/10.1109/icces48766.2020.9138047
6. Hameed, R.T., Mohamad, O.A., Tapus, N.: Health Monitoring System based on wearable sensors and cloud platform. 20th International Conference on System Theory, Control and Computing (ICSTCC) (2016). https://doi.org/10.1109/icstcc.2016.7790722
7. Fried, R., Schettlinger, K., Borowski, M.: Robfilter: Robust Time Series filters. CRAN: Contributed Packages (2008). https://doi.org/10.32614/cran.package.robfilter
8. Davies, P.L., Fried, R., Gather, U.: Robust signal extraction for on-line monitoring data. J. Stat. Plan. Infer. **122**, 65–78 (2004). https://doi.org/10.1016/j.jspi.2003.06.012
9. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
10. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
11. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4

Best Co-positive Approximation in Weighted Space

Mohammed Khalaf(✉) and Alaa Adnan Auad

Department of Mathematics, College of Education for Pure Science, University of Anbar, Ramadi, Iraq
{moh21u2006,alaa.adnan.auad}@uoanbar.edu.iq

Abstract. In this work, the direct theorems of unrestrained mappings via some linear operators in terms of Ditzian-Totik and module of continuity have been considered and we got the best approximation by arriving at $\|h - \Upsilon_k\|_{p,v} \leq C_2\Omega_\varphi$, approximate these functions via a piecewise constant function, used Minkowski's inequality and employing certain algebraic polynomials on closed intervals. The direct approximation co-positive theorems for unbounded functions have also been demonstrated. Moreover, The distinguishing features of this paper over previous papers are finding unconstrained functions in space and their rapid approximation with minimal error using algebraic polynomials.

Keywords: Weighted space · unbounded function algebraic polynomial · Ditzian-Totik · module of continuity

1 Introduction

Recently, 1-sided approximation of limited mappings using trigonometric polynomials in terms of K-functional was discovered in 1979 by Totkov and Popov et al. [1, 2], Nurnberger delete 1985 explored unity in one-sided L_1 approximation and quadrature equations [3]. Consequently, Petras (1991) provided the error constants indicative of square errors for a one-sided approximation to L_1 [4]. Therefore, Babenko and Glushko studied the exclusivity of a function of the better approximations in the space L_1 $[a, b]$ in 1994. They also expressed the problems of the better 1-sided approximation of continuously differentiable functions and the better approximation and better (α,β)-approximation of continuous functions [5]. In 2003 Jianl and Songp described the better approximation rate of 1-sided in L_p spaces [6]. For certain classes of differentiable functions in L_1, Pas'ko and Motornyi were able to produce a better 1-sided approximation in 2004 [7].

The better 1-sided approximat. of a mappings by algebraic polynomials in the space L_1 was accurately estimated by Motornaya, Motornyi, and Nitiema in 2010 [8]. By using Bernstein operators, Al-Saidy and Husain [9] discovered the grade of better approximat. of unrestrained mappings, using the mean continuity coefficient as a measure, Alaa and Mousa (2016) examined a few constructive factors for the 1-sided approximation of the unlimited mappings in the weighted space $L_{p,\alpha}(X)$ and estimated a grade of the better 1-sided approximati. in 2017 Auad and Al-jumali existing the grade of better co-positive

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 74–85, 2025.
https://doi.org/10.1007/978-3-031-91008-1_7

approximat. of unrestrained functions by linear operators which belong to weight space in terms of modulus of smoothness [7], in 2019 Hussein and Adnan explain the better simultaneous approximation of unrestrained functions use some well-known linear operators in weighted space [8], in 2021 Fayyadh and Auad, the direct and converse theorems to approximate of unrestrained functions using linear operators have been proved [9]. In addition, Klaeif and Auad, 2022 investigate some characteristics of better co-proximinal and co-Chebyshev of unrestrained functions in weighted space [10]. Moreover, in 2023 Xiong, etc. studied some characteristics of Baskakov–Durrmeyer operators with multivariables to approximate varies functions via modified K-functional in Orlicz space [11]. Finally, we advise researchers to read the references [12, 13, 14].

The main objective of this note to find solving of problem the difficult properties of functions in weighted space by approximate its to some operators as be algebraic polynomials in terms Ditzian-Totik of modulus continuity, this results we can obtain its via direct theorems. Our current discussion: When we want to compare the results of our paper with the work of previous researchers, we notice that most researchers tried to approximate the restricted functions, while our current work studies the approximation of the unrestricted functions with new conditions and the use of approximation tools within new concepts.

2 Auxiliary Lemmas

Lemma 2.1. Let h be a function in $L_{p,v}(M)$. For every $k \in K, 1 \leq r \leq k-1$ and $\beta \geq 10$ there are polynomials F_r and H_r of grade $\leq k$ sufficient for $x \in [-1,1]$:

$$0 \leq M_r(t) - F_r(t) \leq C_2(\beta)\varrho_r^{\beta}, 0 \leq H_r(t) - M_r(t) \leq C_2(\beta)\varrho_r^{\beta}, \tag{1}$$

where

$$M_r(t) := \{1, \quad if\ t \geq t_r, 0, \quad otherwise\ .\}$$

Proof: For the unusual case $\beta = 18$ polynomials F_r and H_r are, respectively ϑ and Φ_{r+1}.

The following inequalities hold:

$$0 \leq H_r(t) \leq C_2\varrho_r^{18}g_r^{-1} \tag{2}$$

$$\|M_r(t) - F_r(t)\|_{p,v} \leq C_2\varrho_r^{17} \tag{3}$$

$$\int_{-1}^{1} F_r(y)dy \cong 1 - t_m \tag{4}$$

$$\left\|\vartheta_r'(t)\right\|_{p,v} \leq C_2\varrho_r^{19}g_r^{-1}, \tag{5}$$

$$0 \leq M_r(t) - \vartheta_r(t) \leq C_2\varrho_r^{18} \tag{6}$$

$$1 - t_{r-1} < \int_{-1}^{1} \vartheta_r(y)dy < 1 - t_r \tag{7}$$

$$\left\| \Phi_r'(t) \right\|_{p,v} \leq C_2 \varrho_r^{19} g_r^{-1}, \tag{8}$$

$$0 \leq \Phi_r(t) - M_{r-1}(t) \leq C_2 \varrho_r^{18} \tag{9}$$

$$1 - t_{r-1} < \int_{-1}^{1} \Phi_r(y)dy < 1 - t_r \tag{10}$$

Where $t \in S$ and $M_r(t) := M[t_r, 1](t)$.

So,

$$\int_{-1}^{1} F_r(y)dy < 1 - t_r \leftrightarrow \int_{-1}^{1} f_r^9(y)dy < (1 - t_r) \int_{-1}^{1} f_r^9(y)dy$$

$$\leftrightarrow \int_{-1}^{1} (1 - y) f_r^9(y)dy < (1 - t_r) \int_{-1}^{1} f_r^9(y)dy$$

$$\leftrightarrow \prod_{r}^{1} (1, 0, 9) = \int_{-1}^{1} (y - t_r) f_r^9(y)dy > 0,$$

And analogously

$$\int_{-1}^{1} F_r(y)dy > 1 - t_{r-1} \leftrightarrow \prod_{r}^{1} (1, 0, 9) = \int_{-1}^{1} (t_{r-1} - y) f_r^9(y)dy > 0.$$

For any $t \in S$, we have

$$\begin{gathered} 0 \leq F_r'(t) \leq C_2 g_r^{17} f_r^9(t) \\ \leq C_2 \cdot 4^9 \cdot 10^{27} g_r^{17} (|t - t_r| + g_r)^{-18} \\ \leq C_2 \varrho_r^{18} g_r^{-1}, \end{gathered}$$

$$\begin{gathered} \left\| \vartheta_r'(t) \right\|_{p,v} \leq C_2 \varrho_r^{18} |t - t_r| t_r^{10}(t) \\ \leq C_2 \cdot 4^{10} \cdot 10^{30} g_r^{18} (|t - t_r| + g_r)^{-19} \\ \leq C_2 \varrho_r^{19} g_r^{-1}, \end{gathered}$$

and, similarly,

$$\begin{gathered} \left\| \Phi_r'(t) \right\|_{p,v} \leq C_2 \varrho_r^{18} |t_{rr-1} - t| t_r^{10}(t) \\ \leq C_2 \cdot 4^{10} \cdot 10^{30} g_r^{18} (|t - t_r| + g_r)^{-19} \\ \leq C_2 \varrho_r^{19} g_r^{-1}. \end{gathered}$$

Now let us prove the remaining inequalities which are (3) and the right-hand side inequalities in (6) and (9). First, let $t < t_r$. Then with (2), (5), and (8) we have

$$\|M_r(t) - F_r(t)\|_{p,v} = \|F_r(t)\|_{p,v} = \left(\left| \int_{-1}^{t} H'_r(y) v(t) dy \right| \right)^{1/p}$$

$$\leq C_2 g_r^{17}\left(\int_{-\infty}^{t}(|y-t_r|+g_r)^{-18}v(t)dy\right)^{1/p} \leq C_2\varrho_r^{17},$$

$$M_r(t)-\vartheta_r(t) = -\vartheta_r(t) = \left(-\int_{-1}^{t}\vartheta'_r(y)v(t)dy\right)^{1/p}$$

$$\leq C_2\varrho_r^{18}\left(\int_{-\infty}^{t}(|y-t_r|+g_r)^{-19}v(t)dy\right)^{1/p} \leq C_2\varrho_r^{18}$$

and

$$\Phi_r(t)-M_{r-1}(t) = \Phi_r(t) = \left(\int_{-1}^{t}\Phi'_r(y)v(t)dy\right)^{1/p}$$

$$\leq C_2 g_r^{18}\left(\int_{-\infty}^{t}(|y-t_r|+g_r)^{-19}v(t)dy\right)^{1/p} \leq C_2\varrho_r^{18},$$

Respectively.

For $t \geq t_r$, similarly, we have

$$\|M_r(t)-F_r(t)\|_{p,v} = \|1-F_r(t)\|_{p,v} = \left(\left|\int_{t}^{1}F'_r(y)v(t)dy\right|\right)^{1/p}$$

$$\leq C_2 g_r^{17}\left(\int_{t}^{\infty}(|y-t_r|+g_r)^{-18}v(t)dy\right)^{1/p} \leq C_2\varrho_r^{17},$$

$$M_r(t)-\vartheta_r(t) = 1-\vartheta_r(t) = \left(\int_{t}^{1}\vartheta'_r(y)v(t)dy\right)^{1/p}$$

$$\leq C_2 g_r^{18}\left(\int_{t}^{\infty}(|y-t_r|+g_r)^{-19}v(t)dy\right)^{1/p} \leq C_2\varrho_r^{18},$$

and

$$\Phi_r(t)-M_{r-1}(t) = \Phi_r(t)-1+M[t_r,t_{r-1}]$$

$$\leq \left(-\int_{t}^{1}\Phi'_r(y)v(t)dy\right)^{1/p} + C_2\varrho_r^{18}$$

$$\leq C_2 g_r^{18}\left(\int_{t}^{\infty}(|y-t_r|+g_r)^{-19}v(t)dy\right)^{1/p} + C_2\varrho_r^{18} \leq C_2\varrho_r^{18}.$$

This completes the proof of inequalities (3), (6) and (9). Thus the lemma is proved.

Lemma 2.2. Let j be a function in $L_{p,v}(M)$. For any function $h \in L_{p,v}[-1,1]$, $0 < p < \infty$, the following inequality holds:

$$\left(\sum_{r=1}^{k} w(j,g_r,\mu_r)_{\mathbb{T}}^{p,v}\right)^{1/p} \leq C_2 C_0 w_\partial(j,(k+1)^{-1})_{p,v}, \tag{11}$$

Where for every r, $L_r \supset S_r$ is such that $|L_r| \leq C_0|S_r|$, and C_2 depends on p if $0 < p < 1$.

Proof: We need to prove the following

$$S' := \left(\int_{-1}^{1} |L_k(h,t) - \Upsilon_k(h,t)|^p v(t)\, d(t)\right)^{1/p} \leq C_2 \Omega_i^{\varphi}(h, \frac{1}{k})$$

Now,

$$\left(\int_{-1}^{1} |L_k(h,t) - \Upsilon_k(h,t)|^p v(t)\, d(t)\right)^{1/p}$$

$$= \left(\int_{-1}^{1} \left|\sum_{m=1}^{k-1} (\Upsilon_{m+1}(h,t) - \Upsilon_m(h,t)\partial_m(t) - j_m(t)\right|^p v(t)\, d(t)\right)^{1/p}$$

$$\leq \sum_{m=1}^{k-1} \left(\int_{-1}^{1} max \left|(\Upsilon_{m+1}(h,t) - \Upsilon_m(h,t)\partial_m(t) - j_m(t)\right|^p v(t)\, d(t)\right)^{1/p}$$

$$\leq C_2 max \sum_{m=1}^{k-1} \sum_{t \in S_{m+1}} \| (\Upsilon_{m+1}(h,t) - \Upsilon_m(h,t)\|_{p,v}^p$$

$$\times \left(\int_{-1}^{1} \left(1 + \frac{|t - \eta_m|}{\eta_{m+1} - \eta_m}\right)^{(i-1)p} \times |\partial_m(t) - j_m(t)|^p v(t)\, dt\right)^{1/p}$$

$$\leq C_2 max \sum_{m=1}^{k-1} \| (\Upsilon_{m+1}(h,t) - \Upsilon_m(h,t)\|_{p,v}^p$$

$$\times \left(\int_{-1}^{1} \left(1 + \frac{|t - \eta_m|}{\eta_{m+1} - \eta_m}\right)^{ip-jp} v(t)\, dt\right)^{1/p}$$

Where $S_m := [\eta_{m-1}, \eta_m]$.
Now we choose j so that $jp - ip > 2$ and it is readily seen that

$$\left(\int_{-1}^{1} [d_m(t)]^{-2} v(t) dt\right)^{1/p} \leq C_2(\eta_{m-1}, \eta_m), \quad m = 1, \ldots, k-1. \tag{12}$$

Hence by (12) we obtain

$$S' \le C_2 \sum_{m=1}^{k-1} \max_{t\in S_{m+1}} \|(\mathfrak{T}_{m+1}(h,t) - \mathfrak{T}_m(h,t)\|_{p,v}^p \|\eta_{m+1} - \eta_m\|_{p,v}$$

$$\le C_2 \sum_{m=1}^{k-1} \left(\int_{\eta_m}^{\eta_{m+1}} \left|(\mathfrak{T}_{m+1}(h,t) - \mathfrak{T}_m(h,t)\right|^p v(t)\, d(t) \right)^{1/p}$$

$$\le C_2 \sum_{m=1}^{k} \left(\int_{\eta_m}^{\eta_{m+1}} \left|h(t) - \mathfrak{T}_m(h,t)\right|^p v(t)\, d(t) \right)^{1/p}$$

$$\le C_2 \Omega_i^{\varphi} \left(h, \frac{1}{k} \right)_{p,v}^p$$

Lemma 2.3. Let h be an unrestrained function in $L_{p,v}(M)$. Let $k \in K$ be fixed, and let Q_k be a piecewise endless spline with the contract at t_r, $0 \le r \le k$. Then for every interval $[c, d] \subset [-1, 1]$ the following dissimilarity holds:

$$\|Q_k(d) - Q_k(c)\|_{p,v}$$
$$\le C_2 \left(1 + \frac{|d-c|}{\varepsilon_k(c,d)}\right) \varepsilon_k(c,d)^{-1/p} w_\partial\left(Q_k, k^{-1}\right)_{p,v}, \quad 0 < p < \infty. \tag{13}$$

Proof: Let $R := \{r; t_r \in [c, d]\}$. Since for every $r \in R$ the inequality $g_r = |S_r| \ge \varepsilon_k(c, d)$ satisfying, $[c, d]$ have not more than $1 + [|d - c|/\varepsilon_k(c, d)]$ interval S_r. Also, for every $r \in R$ we have

$$w_\partial\left(Q_k, k^{-1}\right)_{p,v}^p = \sup\left(\int_{-1}^{1} \left|\Delta_{g\partial(t)}(Q_k, t)\right|^{p,v} v(t)dt \right)$$
$$\ge C_2 \|Q_k(t_r+) - Q_k(t_r-)\|_{p,v} g_r$$
$$\ge C_2 \|Q_k(t_r+) - Q_k(t_r-)\|_{p,v} \varepsilon_k(c,d).$$

Therefore,

$$\|Q_k(d) - Q_k(c)\|_{p,v} \le \sum\nolimits_{r\in R}^{1} |Q_k(t_r + .) - Q_k(t_r - .)|$$
$$\le C_2 \left(1 + \frac{|d-c|}{\varepsilon_k(c,d)}\right) \varepsilon_k(c,d)^{-1/p} w_\partial\left(Q_k, k^{-1}\right)_{p,v}$$

Lemma 2.4. Let h be an unrestrained function in $L_{p,v}(M)$. For every $y_i \in Y_q = \{y_1, \ldots, y_q\}$ and $\beta \ge 2$, there exists an increasing polynomial $F_k(y_i, t) \in, \Pi_k$ copositive with $F(t - y_i)$ in [−1,1] and such that

$$\|F(t - y_i) - F_k(y_i, t)\|_{p,v} \le C_2 \left(\frac{\varepsilon_k(y_i, t)}{|y_i - x| + \varepsilon_k(y_i, t)} \right)^{\beta} \tag{14}$$

Proof: The dissimilarity was shown in [13] for $\beta = 2$ with $\Delta_k(y_i)$ instead of $\varepsilon_k(y_i, t)$. The proof is similar for any ≥ 2.

By the dissimilarities (see [19], for case)

$$\Delta_k(y)^2 < 4\Delta_k\Big(\|t - y\|_{p,v} + \Delta_k(t)\Big) \tag{15}$$

$$\frac{1}{2}\Big(\|t - y\|_{p,v} + \Delta_k(t)\Big) < \|t - y\|_{p,v} + \Delta_k(y) < 2\Big(\|t - y\|_{p,v} + \Delta_k(t)\Big) \tag{16}$$

for any $t, y \in [-1, 1]$, we have

$$\frac{\Delta_k(y_i)}{|y_i - t| + \Delta_k(y_i)} \leqslant \frac{2\sqrt{\Delta_k(t)(|y_i - t| + \Delta_k(t))}}{\frac{1}{2}(|y_i - t| + \Delta_k(t))} = 4\sqrt{\frac{\Delta_k(t)}{|y_i - t| + \Delta_k(t)}}.$$

Therefore, for $F_k(y_i, t)$ satisfying.
$\|F(t - y_i) - F_k(y_i, t)\|_{p,v} \leq C_2\Big(\frac{\Delta_k(y_i)}{\|y_i - x\|_{p,v} + \Delta_k(y_i)}\Big)^{2\beta}$, we have

$$\|F(t - y_i) - F_k(y_i, t)\|_{p,v} \leq C_2\left(\frac{\varepsilon_k(y_i, t)}{|y_i - t| + \varepsilon_k(y_i, t)}\right)^{\beta}$$

Lemma 2.5. Let h be a positive constant and F_k have at least two b_m in each (y_r, y_{r+1}) for all r. Then there is a piecewise constant spline q_k on F_k such that it is co-positive with f and gratifies

$$\|h - q_k\|_{L_{p,v(R_m)}} \leq C_2\Omega(h, |L_m|,)_{p,v} \tag{17}$$

for each m, where $R_m := \big[b_m, b_{m+1}\big] \subseteq L_m \subseteq \big[b_{m-1}, b_{m+2}\big]$, and C_2 depends on the ratio $\gamma := \frac{(b_{m+2} - b_{m+1})}{b_{m+1} - b_m}$. *If* $0 < p < 1$, C_2 also depends on p. If, in particular, $b_m := t_{k-m}$, $m = 0, \ldots, k$, are used, and k is sufficiently large, then we have

$$\|h - q_k\|_{L_{p,v}} \leq C_2\Omega_\partial(h, (k + 1)^{-1}{}_{p,v}, \tag{18}$$

where C_2 depends on $\varepsilon := min_{0 \leq m \leq q}|y_{m+1} - y_m|$ and also on p in the case of $0 < p < 1$.

Proof. Let $R_m := \big[b_m, b_{m+1}\big]$ and $b_m < y_r \leq b_{m+1}$ for some $y_r \in Y_q$, $1 \leq r \leq q$. Then by supposition, there is closely one y_r in each of the intervals R_{nr}, $r = 1, \ldots, q$, and there is at least one in interval.

R_m between R_{nr} and R_{nr+1} for any $0 \leq r \leq q$.

(Here, for suitability we used the representation $n_0 := -1, n_{q+1} := k$, and $R_{-1} = R_k := \emptyset$.) Note that h does not change sign between R_{nr} and R_{nr+1}. Let c_m be a best $L_{p,v}$, constant approximation of h on R_m, $m = 0, \ldots, k - 1$, then

$$\|h - c_m\|_{L_{p,v(R_m)}} \leq C_2\Omega(h, |R_m|, R_m)_{p,v}. \tag{19}$$

If R_m contain c_m has a similar sign as h. We express

$$q_k := \big\{0, \textit{ for } t \in \big[b_{nr}, b_{nr+1}), 1 \leq r \leq q, c_m, \textit{ for } t \in \big[b_m, b_{m+1})\big\}$$

Since c_{nr-1} and c_{nr+1} have differing signs, we have

$$\|c_{nr-1}\|_{p,v} \le \|c_{nr+1} - c_{nr-1}\|_{p,v} = |L_{nr}|^{-1/p}\|c_{nr+1} - c_{nr-1}\|_{p,v(L_{nr})}$$

$$\le C_2|L_{nr}|^{-1/p}\big(\|h - c_{nr+1}\|_{p,v(L_{nr})} + \|h - c_{nr-1}\|_{p,v(L_{nr})}\big)$$

$$\le C_2|L_{nr}|^{-1/p}\Omega(h, |L_{nr}|, L_{nr})_{p,v},$$

where $L_{nr} := \big[b_{nr-1}, b_{nr+2}\big]$. Here in the previous step, we have used better $L_{p,v}$ polynomial approximation of h on an interval S is also better one on an interval $R \supseteq S$. So

$$\|h - q_k\|_{p,v(R_{nr})} \le C_2\Big(\|h - c_{nr-1}\|_{p,v(R_{nr})} + |c_{nr-1}||R_{nr}|^{1/p}\Big)$$
$$\le C_2\Omega(h, |L_{nr}|, L_{nr})_{p,v}, \tag{20}$$

and this, together with (19), gives (17). From the structure, it is obvious that q_k is co-positive with h.

For $k > K := C_2\varepsilon^{-1}$ such that there are at least two t_m items in each (y_r, y_{r+1}) for all r, inequality (18) immediately follows from (17) and Lemma 2.2.

3 Main Results

Theorem 3.1. If $h \in L_{p,v}[-1, 1]$, $0 < p < \infty$ and $h(t) \ge 0$, $t \in [-1, 1]$, then for every $k \in K_0$

$$E_k^0(h)_{p,v} \le C_2\Omega_\varphi\Big(h, (k+1)_{p,v}^{-1}, \tag{21}$$

Where C_2 is constant in the case $p \in [1, \infty)$ and $C_2 = C_2(p)$ if $0 < p < 1$.

Proof: Throughout this section C_2 denotes absolute constants in the case $1 \le p < \infty$ and constants depending only on p if $0 < p < 1$.

As standard, these quantities are not certainly the same even if they occur in the same line.

First, we approximant h by a piecewise constant function Q:

$$Q(h, t) := q_k + \sum_{r=1}^{k-1}(q_r - q_{r+1})M_r(t),$$

Where q_r is best $L_{p,v}(X)$ constant approximant. to h on the S_r. Since $Q(h, t) = q_r$ on S_r, then $Q(h, t) \ge 0$, $t \in [-1,1]$.

$$\|h - q_r\|_{p(S_r),v} \le C_2 w(h, g_r, S_r)_{p,v}.$$

Therefore, using Lemma 2.2 we have

$$\|h - Q(h)\|_{p,v}^p = \sum_{r=1}^{k} \left(\int_{S_r}^{1} |(h(t) - q_r)v(t)|^p v(t)dt \right)$$

$$\leq C_2^p \sum_{r=1}^{k} w(h, g_r, S_r)_p^p \leq C_2^p w_\vartheta \left(h, (k+1)^{-1} \right)_{p,v}^p . \tag{22}$$

Now we define

$$\Upsilon_k(h,t) \coloneqq q_k + \sum_{r=1}^{k-1} (q_r - q_{r+1}) \left(\frac{F(q_r - q_{r+1}) + 1}{2} H_r(t) + \frac{1 - F(q_r - q_{r+1})}{2} F_r(t) \right).$$

The polynomial $\Upsilon_k(h,t)$is nonnegative since

$$\Upsilon_k(h,t) \geq q_k + \sum_{r=1}^{k-1} (q_r - q_{r+1}) M_r(t) = Q(h,t) \geq 0 .$$

Also, choosing $\beta := 1 + [10/min\{1,p\}]$, by using Lemma 2.1 we obtain

$$\|\Upsilon_k(h) - Q(h)\|_{p,v}^p \leq C_2^p \int_{-1}^{1} \left(\sum_{r=1}^{k-1} |q_r - q_{r+1}| \varrho_r^\beta \right)^p v(t)\, dt$$

$$\leq C_2^p \int_{-1}^{1} \left(\sum_{r=1}^{k-1} g_r^{-\frac{1}{p}} \|q_r - q_{r+1}\|_{L_{p,v}} \varrho_r^\beta \right)^p v(t)\, dt .$$

Now, using the dissimilarity $(\sum \eta_m)^p \leq \sum \eta_m^p$ in the situation $0 < p < 1$ and the well-known Jensen inequality (for the latter the fact that $\sum_{r=1}^{k} \varrho_r^\lambda \leq C_2, \lambda \geq 2$ is needed) we have

$$\|\Upsilon_k(h) - Q(h)\|_{p,v}^p \leq C_2^p \sum_{r=1}^{k-1} g_r^{-1} \|q_r - q_{r+1}\|_{p,v}^p \int_{-1}^{1} \varrho_r^{\beta\{1,p\}} v(t)\, dt$$

$$C_2^p \sum_{r=1}^{k-1} \|q_r - q_{r+1}\|_{p,v}^p ,$$

Since $\int_{-1}^{1} \varrho_r^\lambda dt \leq C_2(\lambda) g_r$ for ≥ 2. Finally, using Minkowski's inequality for $p \geq 1$ and its analog if $0 < p < 1$ and the fact that q_r is a near best constant approximant to f on $S_r \cup S_{r-1}$ (here S_0 is understood as the empty set), together with Lemma 2.2, we obtain

$$\|\Upsilon_k(h) - Q(h)\|_{pv,}^p \le C_2^p \sum_{r=1}^{k} \|h - q_r\|_{p,v(S_r \cup S_{r-1})}^p$$

$$\le C_2^p \sum_{r=1}^{k} \Omega(h, g_r, S_r \cup S_{r-1})_{p,v}^p \le C_2^p \Omega_\partial(h, (k+1)^{-1})_{p,v}^p .$$

The proof of Theorem 3.1 is now complete.

Theorem 3.2. Let $Y_q = \{y_1, \ldots y_q\}$ be given, and let $\varepsilon := min_{0\le m\le q}\|y_{m+1} - y_m\|_{p,v}$. If $h \in L_{p,v}[-1,1] \cap \Delta^0(Y_q)$, $0 < p < \infty$, then for every $k \in K_0$

$$E_k^{(0)}(h, Y_q)_{p,v} \le C_2 \Omega_\varphi\left(h, (k+1)^{-1}\right)_{p,v} \tag{23}$$

where C_2 depends on q, ε and also on p in the case for $0 < p < 1$.

Proof: It is enough to prove Theorem 3.2 for suitably large k, say, $k \ge C_2\varepsilon^{-1}$, since for minor k its claim follows from the fact that

$\|h\|_{p,v} \le C_2\Omega_\varphi(h, 1)_{p,v} \le C_2\Omega_\varphi(h, (k+1)^{-1})_{p,v}$ for $h \in \Delta^0(Y_q)$, $q \ge 1$, and $0 \le k \le C_2\varepsilon^{-1}$.

Here, the first dissimilarity can be proved a similar way as (17), using y_r in place of b_m, and the remark that $\Omega(h, 1)_{p,v} \sim \Omega_\varphi(h, 1)_{p,v}$.

We shall prove Theorem 3.2 by the introduction on q, the number of sign variations.

For $q = 0$ Theorem 3.1 gives the proof. Now we assume that (6) is valid for every function h in $L_{p,v}[-1,1] \cap \Delta^0(Y_{q-1})$ with $Y_{q-1} = \{y_1, \ldots, y_{q-1}\}$. For $h \in L_{p,v}[-1,1] \cap \Delta^0(Y_q)$, it follows from Lemma 2.5 that there exists a piecewise constant spline $Q \in \Delta^0(Y_q)$ with knots $\{t_r\}_{r=0}^k$ satisfying (18). Let $U(t) := Q(t)F(t - y_q)$. Then $U \in L_{p,v}[-1, 1] \cap \Delta^0(Y_{q-1})$, and by the assumption, there exists a polynomial $T_k \in \prod_k \cap \Delta^0(Y_{q-1})$ such that

$$\|U - T_k\|_{p,v} \le C_2\Omega_\varphi\left(U, (k+1)^{-1}\right)_{p,v}. \tag{24}$$

Define $\Upsilon_k(t) := T_k(t)F_k(y_q, t)$, *where* $F_k(y_q, t)$, where $F_k(y_q, t)$ is the polynomial co-positive with $F(t - y_q)$ and given in Lemma 2.4 for $\beta \ge 2 + 4/p$. It is apparent that $\Upsilon_k \in \sum_{2k} \cap \Delta^0(Y_q)$. We are going to estimate $\|Q - \Upsilon_k\|_{p,v}$and then $\|h - \Upsilon_k\|_{p,v}$.

From (22), we have

$$\|Q - T_k\|_{p,v} = \|U(t)F(t - y_q) - T_k(t)F_k(y_q, t)\|_{p,v}$$

$$\le C_2\left\{\|U(t)F(t - y_q) - F_k(y_q, t)\|_{p,v} + \|[U(t) - T_k(t)]F_k(y_q, t)\|_{p,v}\right\}$$

$$\le C_2\left(S + \Omega_\varphi(U, (k+1)^{-1})_{p,v}\right),$$

Where $S := \|U(t)[F(t-y_q) - F_k(y_q,t)]\|_{p,v}$. Here we have used the fact that $\|F_k(y_q,t)\|_{p,v} \leq C_2$. Since $|U(t)| = |Q(t)|$ and $Q(y_q) = 0$, we have

$$S^p = \int_{-1}^{1} |Q(t) - Q(y_q)|^p |F(t-y_q) - F_k(y_q,t)|^p v(t)dt.$$

It follows from Lemmas 2.3 and 2.4 that

$$\begin{aligned} S^p &\leq C_2^p \Omega_\varphi(Q,(k+1)^{-1})_{p,v}^p \int_{-1}^{1} \left(1 + \frac{|y_q - t|}{\varepsilon_k(y_q,t)}\right)^p \\ &\times \varepsilon_k(y_q,t)^{-1} \left(\frac{\varepsilon_k(y_q,t)}{|y_q - t| + \varepsilon_k(y_q,t)}\right)^{\beta p} v(t)dt \\ &:= C_2^p \Omega_\varphi\left(Q,(k+1)^{-1}\right)_{p,v}^p \theta \end{aligned}$$

And we have

$$\theta := \int_{-1}^{1} \left(\frac{\varepsilon_k(y_q,t)}{|y_q - t| + \varepsilon_k(y_q,t)}\right)^{(\beta-1)p} \varepsilon_k(y_q,t)^{-1} v(t)dt \leq C_2.$$

Certainly, it is simple to check the above dissimilarity with $\Delta_k(y_q)$ instead of $\varepsilon_k(y_q,t)$. Then using (15) and (16), we can prove this inequality in terms of $\varepsilon_k(y_q,t)$ as we did in the proof of Lemma 2.4.

$$\|Q - \Upsilon_k\|_{p,v} \leq C_2[\Omega_\varphi(Q,(k+1)^{-1})_{p,v} + \Omega_\varphi(U,(k+1)^{-1})_{p,v}].$$

From (18), we have

$$\Omega_\varphi\left(Q,(k+1)^{-1}\right)_{p,v} \leq C_2 \Omega_\varphi\left(h,(k+1)^{-1}\right)_{p,v,}$$

and

$$\begin{aligned} \|h - \Upsilon_k\|_{p,v} &\leq C_2\left(\|h - Q\|_{p,v} + \|Q - \Upsilon_k\|_{p,v}\right) \\ &\leq C_2\left(\Omega_\varphi(h,(k+1)^{-1})_{p,v,} + \Omega_\varphi(U,(k+1)^{-1})_{p,v,}\right). \end{aligned}$$

Now, we only want to illustration that

$$\Omega_\partial\left(U,(k+1)^{-1}\right)_{p,v} \leq C_2 \Omega_\varphi\left(Q,(k+1)^{-1}\right)_{p,v}.$$

Certainly, using the classification of U(more precisely, the fact that U coincides with $-Q$ on $[-1,y_q]$, $|U(t)| = |Q(t)|$, and U does not change sign on $[y_{q-1},1]$) we conclude that for any numbers $c,d \in [-1,1]$ such that $|d-c|$ is sufficiently small ($\|d-c\|_{p,v} \leq \|y_q - y_{q-1}\|_{p,v}$ will do) the following dissimilarity holds

$$\|U(d) - U(c)\|_{p,v} \leq \|Q(d) - Q(c)\|_{p,v}.$$

This immediately yields

$$\|\Delta_{g\varphi(t)}(U,t,[-1,1])\|_{p,v}^{p}$$

$$= \int_{\{t;t\pm\frac{g\varphi(t)}{2}\in[-1,1]\}}^{1} |U(t+g\varphi(t)/2) - U(t-g\varphi(t)/2|^{p}v(t)dt$$

$$\leq \int_{\{t;t\pm\frac{g\varphi(t)}{2}\in[-1,1]\}}^{1} |Q(t+g\varphi(t)/2) - Q(t-g\varphi(t)/2|^{p}v(t)dt$$

$$= \|\Delta_{g\varphi(t)}(Q,t,[-1,1])\|_{p,v}^{p}.$$

4 Conclusion

Through my paper, it was concluded that in the weighted space, every unbounded function in it can be approximated by an algebraic polynomial in terms Dizain-totic and module of continues direct theorems, and this property also applies to the derivative of functions with derivatives of polynomials.

References

1. Totkov, G.: Converse theorem for the one-sided trigonometrical polynomials. Comptesrendus de l'Académiebulgare des Sciences **32**(7), 875–878 (1979)
2. Andreev, A., Popov, V., Sendov, B.: Jackson-type theorems for best one-sided approximations by trigonometrical polynomials and splines. Math. Notes Acad. Sci. USSR **26**(52), 889–896 (1979)
3. Nurnberger, G.: Unicity in one-sided L1-approximation and quadratureformulae. J. Approx. Theory **45**(3), 271–279 (1985)
4. Petras, K.: One sided L1-approximation and bounds for Peano kernels. NATO ASI Series C **357**, 165–174 (1991)
5. Bebnko, F., Glushko, N.: On the uniqueness of elements of the best approximation and the best one-sided approximation in the space L1. Ukr. Math. J. **46**, 503–513 (1994)
6. Jianli, W., Songping, Z.: Some converse results on one-sided approximation: justifications. Anal. Theory Appl. **19**, 280–288 (2023)
7. Alaa, A., Jumaili, A.: On co-positive approximation of unbounded functions in weighted Spaces. Int. J. Appl. Eng. Res. **12**(21), 11392–11396 (2017)
8. Adnan, A., Hussein, A.: Best simultaneous approximation in weighted space. IOP Conf. Ser. J. Phys. Conf. Ser. **1234**(2019), 01211 (2019)
9. Auad, A., Fayyadh, M.: The direct and converse theorems for best approximation of algebraic polynomial in L_(p, α) (X). J. Phys. Conf. Ser. **1879**(3), 032010 (2021)
10. Auad, A., Klaeif, A.: Best co-proximal and Co-chebyshev of unbounded functions. J. Phys. Conf. Ser. **2322**, 012033 (2022)
11. Han, L.-X., Bai, Y.-M., Feng, Q.: Approximation by multivariate Baskakov-Durrmeyer operators in Orlicz spaces. J. Inequal. Appl. **118**, 2–22 (2023)
12. Auad, A., Hilal, M., Kalaf, N.: Best approximation of unbounded functions by modulus of smoothness. Eur. J. Pure Appl. Math. **16**(2), 944–952 (2023)
13. Auad, A., Al-Sharqi, F.: Identical theorem of approximation unbounded functions by linear operators. J. Appl. Math. Inform. **41**(4), 801–810 (2023)
14. Alaa, A., Mohammed, A.: Some results on approximation in neutrosophic normed space. Int. J. Neutrosophic Sci. (IJNS) **24**(04), 389–396 (2024)



SDN-Based Edge Computing

Fatimah Azeez(✉)

Mustansiriyah University, Baghdad, Iraq
fatimah.azeez@uomustansiriyah.edu.iq

Abstract. The world of IoT is fast changing and, at the same time, it is increasingly difficult for companies to able to handle all data coming from the various devices that are linked together, ensuring that this data can be processed and acted upon in a timely manner is not easy. This paper presents an innovative approach that combines Software-Defined Networking with Mobile Edge Computing to address these challenges while improving IoT application scalability and efficiency. We take advantage of SDN's ability, as a single point, to control the entire network resources— including making optimal decisions on real-time task offloading at the edge. By introducing an integrated task model with management functions at the edge of mobile networks, we aim not only at expediting task completion but also to ensure resource allocation throughout low latency high bandwidth areas; computation offloads should traverse any agile points located near users' wireless access networks. Our system strives to meet these critical needs by directing tasks to edge locations where they can be best handled. The study proposes a new way through which an organization can leverage Software-Defined Networking within Mobile Edge Computing architectures— using it as a means to improve the scalability and efficiency of their IoT applications. The system speeds up task completion by optimizing real-time task offloading decisions and concentrating resource allocation at the mobile edge— which in turn caters to the critical low latency plus high bandwidth needs and makes a significant difference to the systems. The research thus not only highlights the capability of SDN-based edge computing to revolutionize IoT environments but also paves the way for future investigations on more robust network architectures.

Keywords: Mobile Edge Computing · Software-Defined Networking · Offloading Algorithm · Computation Offloading

1 Introduction

The era of 5G has brought about a remarkable surge in mobile subscriptions and data traffic. Ericsson's most recent projection, spanning 2020 to 2026, anticipates a rise in worldwide mobile subscriptions from 7.9 billion to 8.8 billion, while global mobile data traffic is expected to double. The Internet of Things (IoT) is commonly described as billions of interconnected devices that sense and transmit data to a central controlling system. IoT applications are deployed across diverse domains, like smart city networks, disaster management, logistics, intelligent transportation, and health care (Ali et al., 2022).

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 86–95, 2025.
https://doi.org/10.1007/978-3-031-91008-1_8

The IoT is a large network system of billions of inter-connected devices meant to detect and actuate data to a central system alongside transmitting data. The use cases of IoT applications and devices are vast: smart city deployments, retail, disaster control, logistics, intelligent traffic systems, health care, and many others. Although MEC helps lower service latency by reducing the physical distance involved, enhancing system performance for different situations is important, further reducing service latency and energy consumed (Li et al., 2024), (Fan et al., 2024). Mobile Edge Computing (MEC) is an innovative approach that offers cloud-computing features in immediate proximity to mobile devices within 5G networks. Essentially, MEC facilitates mobile devices' ability to delegate tasks to the MEC servers located on the network's edge instead of relying on the servers in the core network. The MEC paradigm can deliver significant advantages in offloading computations, such as high bandwidth, low latency, and computing agility (Haibeh et al., 2022).

To fill this gap, this paper proposes a Task and Management Model for the Mobile edge computing architecture for IoT. The model allocating resources in the mobile edge computing server aims to execute tasks faster and receive tasks from IoT devices to manage the task and the resource inefficiently. The SDN-IoT architecture's three layers are the Infrastructure, the Control, and the Application Layer. The data plane belongs to the Infrastructure Layer, which includes OpenFlow switches at the control plane level and sensor/actuator components at the hardware level. In cases where the OpenFlow switch cannot determine data routing, an SDN controller takes Control, a software-based centralized entity that is responsible for controlling the flow of data within network devices through modification of the flow table with new rules added or old rules deleted— this is what an SDN controller is called (Indrason & Saha, 2024).

1.1 Motivation

The rapid growth of IoT and mobile data traffic necessitates innovative solutions to address the limitations of traditional cloud computing. The reason cloud computing faces scalability problems and is unable to utilize resources efficiently stems from its inability to control massive amounts of data produced by IoT devices, leading to inefficiency in resource management. In the case of many Internet of Things applications, low latency and real-time processing are essential. However, the centralized cloud computing design introduces high latency, making it unacceptable for such applications to use the technology. On the other hand, cloud computing encounters challenges dealing with different types and large quantities (heterogeneous data) that IoT devices can generate and send since they cannot effectively process, store, or manage. Resource Constraints: In cloud computing, the efficient distribution of resources and task management are not simple because of the limited computational capabilities of IoT devices plus edge nodes. The proposed framework aims to tackle these challenges and, in turn, improve system efficiency and meet the essential needs of low latency and high bandwidth in IoT settings. In this work, we leverage software-defined networking at the network's edge to provide a computation offloading framework using MEC that helps determine task offloading.

1.2 Contributions

1. Introducing an innovative framework combining Mobile Edge Computing with Software-Defined Networking has considerably boosted scalability and effectiveness in IoT apps.
2. Optimization in real-time of centralized resource allocation and task offloading decisions at the mobile edge is a strategic approach that addresses the critical low latency and high bandwidth requirements: accelerating task execution.

2 Literature Survey

This section describes a survey of the most common strategies and algorithms for latency, energy, security, resource allocation, and the most recent studies on offloading techniques.

2.1 Latency and Energy Method and Algorithm in MEC with SDN

The paper puts forth a time-slotted approach to reduce the delay for total task processing without the luxury of compromise from any device's energy consumption constraint. This approach entails task offloading and resource allocation for cloud-edge-end cooperative computing networks with task scheduling delay optimization. As a result, they introduce a two-stage distributed algorithm. They also propose an exclusive method for time-slotted task offloading and resource allocation in such network systems (Fan et al., 2024). The authors introduce an approach—based on a resource management technique using multi-objective optimization that ensures fair resource allocation during task execution to achieve two goals: lowering energy usage and minimizing task execution latency in MEC environments. They proposed an enhanced NSGA-II algorithm to address this issue—which is the proper distribution of communication and processing resources for each activity; this is done in such a way as to avoid using excessive computations and through selecting optimal solutions about different—sometimes even conflicting—objectives (Guo et al., 2022). This study focuses on a full offloading policy, which offloads all jobs from the SD to the edge server completely; additionally, a combination of full offloading policy, collaborative offloading strategy, deadline constraints management, and global network view are used in this SDN-powered MEC network through reinforcement learning contributes to enhancing the performance of MEC networks in terms of efficiency, congestion control, and meeting task deadlines (Al-Hammadi et al., 2023).

2.2 Strategies for Resource Allocation

By promoting high availability in servers and virtual machines, the authors of (Saxena et al., 2022) proposed a fault-tolerant elastic resource management (FT-ERM) framework that approaches the issue from a different angle. An online MIMO-ENN failure predictor has been created to predict multiple resource utilization by VMs and evaluate their failure state in real-time. This paper proposes a software-defined networking (SDN) framework for multi-access edge computing systems to improve communication reliability and

latency performance. The proposed strategy can be applied to various industries beyond virtual reality and online gaming (Zhang et al., 2023). This work provides access to a collaborative traffic identification mechanism for SD-IoT. At the access node, iAcceSD employs machine learning (ML)-based traffic identification algorithms to address the diverse and unidentified traffic flows in IoT. The suggested method decreases network latency by processing flows at the edge. An optimization model is built to program the SD-Access nodes considering the heterogeneous and unknowable traffic (Ahmed and Misra, 2022).

2.3 Offloading Techniques and Algorithms

This section contains a survey on the most recent studies of offloading techniques. The authors (Li et al., 2024) considered both task computation and wireless communications constraints in the system modeling; this is necessary because the system operates in a multi-user, multi-class, and multi-layer edge computing environment, and task offloading and computation decisions are made based on the task transmissions, computations, and deadline requirements. Using queuing theory and stochastic geometry (SG), a model of this integrated edge-fog cloud computing system was created, where point processes were used to represent the spatial interactions between nodes. Edge computing and software-defined networking (SDN) collaborate to address the constrained processing capabilities on mobiles while also improving the agility of service offloading: a response due to uncertainties—like network congestion—which threaten performance at the edge node. (Okegbile et al., 2022).

The resource optimization challenge for a MEC system with several users and MEC servers was the subject of the study; this included handling load balancing between various MEC servers, managing user communication, and optimizing CPU resources (Zhang et al., 2022). The development of a stochastic programming problem was proposed as a means to achieve optimal resource utilization. An algorithm based on the Lyapunov approach, which centrally manages energy and delay, was put forth as the first step towards resolving this issue and attaining the system cost optimal under stability restrictions at the battery level— (Chen et al., 2022) examined the task offloading decision-making issue for edge computing in time-sensitive networking (TSN). They suggested the DSDA-MO distributed and sequential decision-making method for multitask offloading to locate the Nash equilibrium.

2.4 Security and Privacy in MEC with SDN

The author of this paper (Xu et al., 2021) used the secure service offloading Method, named SOME method, to enhance the security and efficiency of service offloading in IoV; the SOME method combines SDN-based management, LSH encryption, service selection optimization, and privacy preservation techniques to facilitate secure and efficient service offloading in Internet of Vehicles, ultimately improving the overall quality of experience for drivers and ensuring the sustainability of transportation systems. The research combines deception with decision-making tools, SDN, NFV, SFC, and NS, for resource management in MEC servers. The approach aims at effectively luring attackers while ensuring optimal use of cyber deception strategies. They introduce a cyber

deception strategy utilizing uniform distribution and random selection to divert potential attackers (Kabdjou and Shinomiya, 2024).

3 System Model

The system comprises several critical components: Edge Servers, represented as the set E, where E = E1, E2, E3,… Denotes individual edge servers; IoT Devices, denoted as the set D, where D = D1, D2, D3,… Signifies individual devices, such as smartphones, tablets, sensors, or IoT endpoints; the SDN Controller, symbolized as C, responsible for network management and task offloading decisions; Network Infrastructure, indicated as N, representing the set of networking equipment that constitutes the communication backbone, such as switches and routers (N = N1, N2, N3,…); and the Task Offloading Manager, represented as T, responsible for managing task offloading decisions. The system model is explained in Fig. 1 with all details.

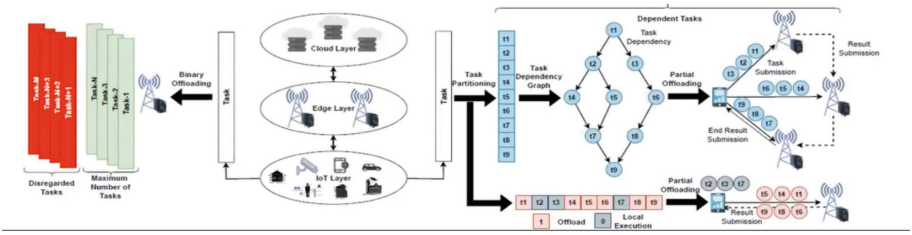


Fig. 1. Full and Partial Offloading Task in SDN-based Edge Computing for IoT Application.

Task Offloading: In the proposed system, task offloading begins with Task Generation, where IoT devices generate tasks denoted as T_i, where i represents the task index. Each task can vary in resource requirements, including computation-intensive tasks (C_i) and data-intensive tasks (D_i). These tasks are generated by devices within the set D. The Task Offloading Manager (T) for each task T_i, decides whether it should be offloaded to another edge server (D) or executed locally ($D_i \in D$). This decision is based on factors like the edge's available resources, the nature of the task, the current network conditions, and the details of Task Offloading in Algorithm 1.

The SDN Controller (C) is pivotal in Task Offloading Decisions. It continuously monitors the network conditions, including the traffic load (L), latency (Δt), and available resources at edge servers (R_e). The information is used by the controller with input from the Task Offloading Manager to decide on task offloading. Two primary strategies are taken into account by the system when it comes to offloading:

A. Partial Offloading: If the task T_i can be divided into two parts, with one part running on the local edge denoted as E_i and the other part running on another edge server is denoted as E_i, the decision is made about how to split the task between these two edges. The decision process may include dividing the task based on its resource needs and any data dependencies that exist within it.

B. Full Offloading: If the job is to be completely sent for execution at another edge server, then the entire T_i is forwarded to an alternate edge server E_i. . This typically happens when tasks have high resource requirements or when network conditions are supportive towards offloading. After the decision to offload is made, Task Execution takes place at the chosen edge server, where the server carries out the offloaded task either partially or fully and returns the results to the IoT device that initiated this task. This ensures that tasks are executed effectively, allowing for optimal resource usage while minimizing latency; a process established through ensuring feedback from these tasks also influences future decisions. Throughout this workflow, the SDN Controller conducts Monitoring and Feedback where it keeps an eye on network conditions like load and latency before providing such information as feedback loops back into our Task Offloading Manager— thereby facilitating dynamic optimization (of) our task offloading decisions based on real-time network performance data observed by him.

Edge Selection: From the perspective of edge node selection, identifying which edge device is most suitable to carry out a specific task holds significant importance— particularly in resource-limited devices for industrial uses. Every task request can be depicted as a tuple (S_k, C), where S_k stands for the input data size of task k in bits (including program data size), and C represents the minimum required CPU cycles in a million instructions per second (MIPS). The specifics of Edge Selection in algorithm 2 are denoted by the CPU cycles needed for task k, which can be calculated through this formula:

$$Ck = Sk \times Di \tag{1}$$

The value of Ck expresses the computational requirement needed by task k. It is figured out through the product of its data volume by the processing intensity (Di), which belongs to that specific edge node. In determining which edge node should handle the task execution, different aspects are taken into account, such as (F_i^c) (which stands for service time availability for delay-sensitive tasks), (F_i^e), (related to current CPU utilization), (F_i^m), (indicating remaining energy) and (F_i^s) (representing RAM availability). A tuple captures the status of an edge device denoted as F_i:

$$F_i = F_i^c, F_i^e, F_i^m, F_i^s \tag{2}$$

All these parameters together give a detailed picture of what each edge device can do, so the selection of the most appropriate edge node for task performance is easy. When looking at these parameters, it would be nice if the selected device had good values for them because this would mean that there is an effective use of resources and that specific needs of tasks (for example, latency and energy efficiency) are met properly. In summary, this model system makes it possible to successfully take off tasks despite the different properties of tasks and conditions in the network— which further contributes to the effectiveness of edge computation.

3.1 Scalable Edge Selection and Task Offloading

This problem aims to maximize the execution of the number of tasks while considering edge node selection and offloading decisions. Let's consider the total number of tasks

executed. Task on the set: task with an indication; end is not executable; we also introduce additional constraints to model the communication energy consumption at the edge nodes where some tasks are offloaded, denoted as Nexecuted

$$\text{Maximize } \mathrm{N}_{\text{executed}} \tag{3}$$

Let X_{ij} be a binary indicator for whether task i is transmitted to edge node j. This binary variable takes on the value of 1 when the task is offloaded to the specific edge node and 0 otherwise; here, i stands for the task index, while j stands for the index of the edge node.

Constraints:
Only one edge node can be assigned to each task

$$X_{ij} < 1 \quad \forall i \tag{4}$$

Due to this restriction, one task should be delegated to no more than one edge node. The number of tasks executed must not be greater than the resources available on each edge node.

$$X_{ij} < \text{Resourcesj} \quad \forall j \tag{5}$$

where resources represent the available resources (CPU, memory, etc.) on edge node j.

Partial Offloading:

$$X_{ij} < Y_{ij} \quad \forall i, j \tag{6}$$

This constraint guarantees that task i can only be partially offloaded to an edge node if it is indeed offloaded at all. Here, the variable Y_{ij} is a binary representation for the scenario when task i is partially offloaded to edge node j; this condition arises from the existence of X_{ij} as a binary variable.

Full Offloading:

$$X_{ij} < Z_{ij} \quad \forall i, j \tag{7}$$

where Z_{ij} is a binary variable indicating whether task i is fully offloaded to edge node j. This constraint ensures that a task can only be fully offloaded to an edge node if it is offloaded at all ($X_{ij} = 1$). Binary Variables: Y_{ij}: Binary variable representing partial offloading of task i to edge node j. Z_{ij}: Binary variable representing full offloading of task i to edge node j.

Algorithm 1 Task Offloading

Input:

Task parameters, $\mathcal{T}_i$

Edge nodes, $\mathcal{E}$

Network conditions

Output:

Offloading decision, X for each task i and edge node j.

for each task i in $\mathcal{T}$ do

Determine task requirements and resource needs.

Evaluate edge node capabilities.

Calculate the offloading score for each edge node.

Select the edge node with the highest score and set $X_{ij} = 1$,

others $X_{ij} = 0$

end for

Algorithm 2 Edge Selection

Input

Set of tasks, $\mathcal{T}_i$

Edge nodes, $\mathcal{E}$

Edge node characteristics F_i

Output

Selection of the best edge node for each task.

for each task i in $\mathcal{T}$ do

Calculate resource requirements of the task

Evaluate edge nodes' capabilities using F_i

Select an edge node with favorable characteristics.

Set selected edge node for task i

end for

4 Conclusion

Mobile Edge Computing integrates Software-Defined Networking; we see a new dawn: an efficient and scalable system for IoT applications. Real-time optimization of task offloading decisions coupled with centralized control capabilities— the proposed system propels task completion speed while ensuring proper resource allocation from the mobile edge. It provides low latency and high bandwidth plus computation agility—an approach significantly able to ensure effective management of large-scale IoT deployments. However, there are many challenges in applying SDN-based computing at the edge of practical situations, which means we have yet to overcome many real-world obstacles and constraints. In future work, practical considerations will be considered to evaluate the framework of SDN-based edge computing in diverse scenarios.

References

Indrason, N., Saha, G.: Exploring Blockchain-driven security in SDN-based IoT networks. J. Netw. Comp. Appl. 103838 (2024)

Kabdjou, J., Shinomiya, N.: Improving quality of service and HTTPS DDoS detection in MEC environment with a cyber deception-based architecture. IEEE Access (2024)

Li, K., et al.: Computation Offloading in Resource-Constrained Multi-Access Edge Computing. IEEE Transactions on Mobile Computing (2024)

Fan, W., et al.: Time-slotted task offloading and resource allocation for cloud-edge-end cooperative computing networks. IEEE Transactions on Mobile Computing (2024)

Sharif, Z., Jung, L.T., Ayaz, M., Yahya, M., Pitafi, S.: Priority-Based Resource Allocation Scheme for Resources Usage in Mobile Edge Computing Platform. Journal of Hunan University Natural Sciences **50**(1) (2023)

Saxena, D., Gupta, I., Singh, A.K., Lee, C.N.: A fault tolerant elastic resource management framework toward high availability of cloud services. IEEE Trans. Netw. Serv. Manage. **19**(3), 3048–3061 (2022)

Zhang, Q., Li, C., Huang, Y., Luo, Y.: Effective multi-controller management and adaptive service deployment strategy in multi-access edge computing environment. Ad Hoc Netw. **138**, 103020 (2023)

Ahmed, N., Misra, S.: Collaborative flow-identification mechanism for software-defined internet of things. IEEE Internet Things J. **9**(5), 3457–3464 (2021)

Okegbile, S.D., Maharaj, B.T., Alfa, A.S.: A multi-user tasks offloading scheme for integrated edge-fog-cloud computing environments. IEEE Trans. Veh. Technol. **71**(7), 7487–7502 (2022)

Haibeh, L.A., Yagoub, M.C., Jarray, A.: A survey on mobile edge computing infrastructure: Design, resource management, and optimization approaches. IEEE Access **10**, 27591–27610 (2022)

Zhang, W., Zhang, G., Mao, S.: Joint parallel offloading and load balancing for cooperative-MEC systems with delay constraints. IEEE Trans. Veh. Technol. **71**(4), 4249–4263 (2022)

Guo, J., Li, C., Luo, Y.: Resource management and switch migration in SDN-based multi-access edge computing environments. J. Supercomput. **78**(13), 15532–15566 (2022)

Chen, J., Pu, C., Wang, P., Huang, X., Zhang, Y., Liu, Y.: Multitask offloading strategy for edge computing in time-sensitive networking. Mob. Inf. Syst. **2022**(1), 1750192 (2022)

Xu, X., et al.: Secure service offloading for internet of vehicles in SDN-enabled mobile edge computing. IEEE Trans. Intell. Transp. Syst. **22**(6), 3720–3729 (2020)

Al-Hammadi, I., Li, M., Islam, S.M.N.: Independent tasks scheduling of collaborative computation offloading for SDN-powered MEC on 6G networks. Soft Computing **27**(14), 9593–9617 (2023)
Ali, O., Ishak, M.K., Bhatti, M.K.L., Khan, I., Kim, K.I.: A comprehensive review of internet of things: technology stack, middlewares, and fog/edge computing interface. Sensors **22**(3), 995 (2022)

Applications of Factor-Based Authentication and Authorization Systems

Mahfuzul Huda[1(✉)] and Abdullah[2]

[1] Faculty of Engineering and Technology, Shubham University, Bhopal, M.P, India
mah.huda@gmail.com
[2] University Institute of Computing and Information Sciences, Chandigarh University, Unnao, India

Abstract. An authentication method used to manage privacy concerns and secure communication channels is called Factor-based authentication. Unauthorized concerns and issues can be reduced and communication can be conducted with greater secrecy when Factor- based authentication is used. Reviewing the salient characteristics of the Factor-based authentication mechanism is the goal of this study. Factor- based authentication is so safe and efficient in terms of security that it helps developers create two-factor authentication programs that lessen internal communication hazards and illegal activity. It is advised that businesses use Factor-based authentication to control security threats and issues related to data breaches. The review and assessment of Factor- based authentication's significance for improving security and safeguarding data was aided by this study. It is discovered that, in order to provide an extra degree of data security in conjunction with password authenticity.

Keywords: Authentication · Factor -based authentication · data breach and two-factor authentication

1 Introduction

This Due to its ability to handle business obstacles and issues as well as create digital systems for business operations, business communities are currently shifting toward digitalization. Employing digital technologies makes it simple for businesses to automate manual processes and carry out several tasks using a single system. Connected business systems are less able to monitor and reduce security risks and threats, making data security one of the most difficult responsibilities for businesses. Businesses may experience data breaches and reduced privacy as a result of security threats and vulnerabilities in their computer networks. Due to their capacity to divulge login credentials and access to private information, over 70% of cybercriminals carry out illicit operations using computer systems and communication channels [1].

An authentication system known as "Factor-based authentication" is created to handle security concerns and illegal activity. A Factor-based authentication system's primary

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 96–103, 2025.
https://doi.org/10.1007/978-3-031-91008-1_9

benefit is that it creates a safe verification procedure that shields web servers and communication channels from cyber-attacks. The purpose of this study is to examine the dangers and security concerns related to computer networks and to assess the significance of Factor-based authentication for data security. To obtain insightful and useful information about factor-based authentication and its effects on web security and secrecy, a survey of the literature will be done.

2 A Review of the Relevant Works

The goal of the review is to manage research gaps by analyzing prior findings to comprehend the significance of Factor-based authentication in data protection and computing network security. According to Zibaei et al. [1], the computing networks and technologies that these organizations employ are not as strong at thwarting cyber- attacks and preventing hacking issues. One of the best ways to secure data is through Factor-based authentication, which can identify unwanted actions taken by hackers on networks and computer systems. By creating a more secure verification process, this kind of online security technology helps businesses to safeguard web servers and communication channels. Malicious software that can transmit undesired signals over computer networks and raise the likelihood of cyber-attacks are the primary creations of cybercriminals (Fig. 1).

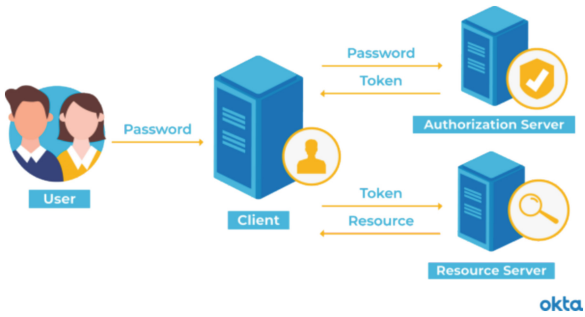


Fig. 1. Factor-Based Authentication and Authorization Systems)

Ensuring the validity of web servers and networks is crucial for businesses, as hackers have the ability to create insider threats and escalate illegal issues. Factor-based authentication is designed to address these issues by concentrating on the secrecy and validity of personal information. In agreement, Belk, et al. [2] said that Factor-based authentication is more appropriate and successful in helping businesses safeguard web servers and communication networks by creating a secure verification program (Fig. 2).

Companies' usage of compromised channels leaves them open to hacker access and compromise the privacy of data being transmitted. Factor-based authentication primarily created encryption software that may provide encrypted codes for communication channels in order to boost privacy. As agreed upon by Wang et al. [3], Factor-based authentication requires obtaining a Factor—a computer-generated code— before allowing users to access the network. Its primary development goal was data protection through

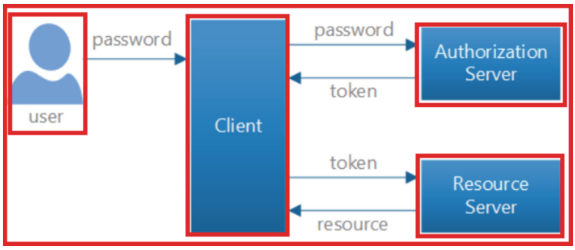


Fig. 2. Operation of Factor-Based Authentication and Authorization Systems

the management of undesired and unauthorized signals. Factor- based authentication is mostly used as an extra layer of data security in conjunction with the authenticity of passwords. In addition to offering two-factor authentication as a way to enhance privacy, it can help businesses manage security risks and vulnerabilities (Fig. 3).

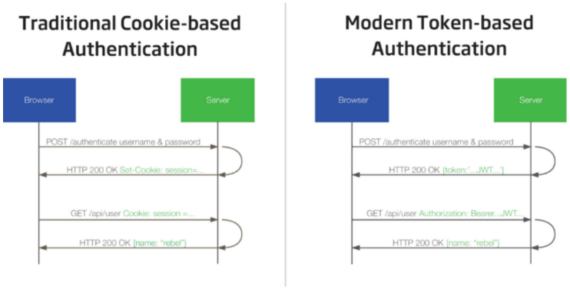


Fig. 3. Factor-based authentication and conventional authentication

For instance, hackers frequently target banking systems in an effort to gain customer account and financial information, including credit and debit card numbers. Banking groups have used Factor-based authentication to address security concerns since it offers two-factor authentication, which increases transaction security. For accessing and completing transactional operations, two-factor authentication is required by more than 70% of businesses and consumers of online banking.

Web servers and networks are vulnerable to a variety of security risks and attacks, including malware, DDoS attacks, brute force attacks, and phishing schemes. One popular cyber-attack used by criminals that can compromise confidentiality and provide hackers access to computer system and network login credentials is malware. Malware threats have the potential to compromise privacy and exacerbate data breach issues for enterprises. Distributed denial of service, or DDoS, is an attack that uses harmful software to target computer networks and web servers used by businesses in order to prevent access and decrease credibility. Plasencia et al. [5] concurred and said that DDoS attacks have the potential to adversely affect web servers' anonymity and privacy, for which.

Factor-based authentication can be implemented.

Brute force and other cyberattacks can be minimized by the use of computer-generated codes and encrypted programs in Factor-based authentication. Using botnets

and security reduction tools, almost 70% of cybercriminals target computer networks in order to carry out illegal activities. To address these issues, security designs should incorporate Factor-based authentication, which would enhance privacy while managing harmful signals and unauthorized activity. Factor-based authentication is frequently more successful than creating encryption-based Factors and giving businesses security precautions.

Companies find it challenging to handle security difficulties and a growth in hacking issues as a result of inadequate security controls and tactics, according to Ratakonda et al. [4]. In contrast to conventional authentication methods such as password-based and biometric systems, Factor-based authentication is more efficient and appropriate for data protection that prioritizes communication channel privacy. Mobile phones can function as additional code generators, providing users with increased protection and preserving the accessibility of sensitive data.

The development of smartphone Factor-based authentication demonstrates that employees of companies can interact with consumers and management in a secure manner while maintaining the privacy of shared data. Factor-based authentication is so safe and efficient in terms of security that it helps developers create two-factor authentication programs that lessen internal communication hazards and illegal activity. Factors are exclusively obtained from computing equipment that offer random codes for data transmission, enabling the development of highly secure systems.

Factor-based authentication requires users to propose encrypted codes and validate their credentials just once, allowing for increased security and privacy in web server accessibility and communication. Users in the current digital generation have access to internet-based communication channels and computer systems, necessitating the development of appropriate security systems and programs. By addressing security threats and challenges, Factor-based authentication can let businesses conduct business operations in a secure manner. Implementing a security policy in a corporation is essential and calls for the right tools and technologies. To address security risks and weaknesses, many businesses have integrated Factor-based authentication into their security policies.

Historically, security measures have been limited to one layer of authentication; nevertheless, hackers can simply compromise privacy and get authenticity. To handle these issues, programmers have developed an authentication system based on encryption, which enables the safe deployment of web servers and communication infrastructure. Factors, when used in the context of Factor-based authentication, are mostly created using encryption software and utilize computer-generated codes that can handle data breaches and ethical issues from companies.

According to Kawamura et al. [6], Factor-based authentication uses JSON web Factors, which are useful for creating security platforms that work for companies. In addition to providing a common method of communication between two parties, JSON web Factors allow encrypted applications, which enhance privacy by converting transmitted data into codes.

The main advantage of Factor-based authentication is that it may help businesses create robust security strategies that will enhance the scalability and privacy of sensitive data. Businesses today gather data from clients and online networks, storing it in

databases that need appropriate security measures. Effective security and authentication systems that can be connected to web servers to safely retrieve data and store it in databases with more authenticity can be built using Factor-based authentication.

Factor-based authentication on web servers can aid in the creation and verification of Factors with accurate data, allowing for the management of malware and undesired signals that hackers may offer. Factor-based authentication offers greater flexibility in terms of security and performance when granting access to web servers and communication networks for businesses. Establishing secure processes and communication infrastructure is crucial for firms to leverage Factor-based authentication. Users cannot share Factor authentication devices between departments and web servers, thus appropriate security protocols and plans must be created, according to Parish et al. [7].

By using Factor-based authentication, business communities can improve the privacy of sent data because it is self-contained and contains all the necessary information for a proper authentication process. Numerous users connect to online servers through computers and mobile devices, making accounts accessible to servers that may compromise the privacy of personal information. Malicious scripts and programs are typically connected to third-party web servers, allowing hackers to steal login credentials and compromise privacy. Factor-based authentication can offer two-factor authentication, which can aid users in maintaining authenticity and enhancing the privacy of their personal information as per Golar et al. [8].

Hackers are able to target databases and get personal details such as login credentials, addresses, account information, financial details, and banking data, according to research presented by Raptis et al. [9]. To enhance privacy and detect undesired or malicious signals, Factor-based authentication can be applied over communication channels used for financial transactions. It is discovered that programs for encoding and decoding data are included in Factor-based authentication, which enables users to send and receive data with greater security as per Addas et al. [15]. The authentication programs send a request to the server with the correct login information first. The authentication server has the ability to provide users with an access Factor that contains encrypted keys, enabling safe communication via networks and web servers. According to Ndako et al. [10], Factor-based authentication enables businesses to create affordable security solutions without requiring more hardware, resources, or devices.

It is safer to use than user IDs and passwords, which enable businesses and users to conduct transactions and access accounts in a secure manner. To improve the privacy of communication channels and data transfer, Factor-based authentication is now integrated into a large number of mobile applications and social media websites. It has an authentication and third-party authority system that may provide digital certificates that increase user trust while shielding data from hackers according to Constantinides et al. [12],

Factor-based authentication is more challenging to administer, nevertheless, due to the increased operating costs associated with the generation of encryption Factors and replacement procedures, which call for more resources and labor. Katsini et al. [13] concurred and pointed out that people using Factor-based authentication may incur greater costs and be required to carry the Factor on a frequent basis, which may provide difficulties.

Factor-based authentication system development calls for certain expertise, which is why more sophisticated training and educational initiatives should be created. Because personnel in firms lack cyber-security experience, insider risks and unauthorized actions can be easily created by hackers. It is crucial that businesses concentrate on these issues and difficulties related to Factor-based authentication in order to successfully reduce internal threats and enhance privacy.

It has been discovered that Factor-based authentication is a useful strategy that companies may use to protect their networks and communication channels against cyberattacks. Insider dangers from computing networks can be reduced by using Factor-based authentication, which is more secure and scalable than standard authentication methods (Fig. 4).

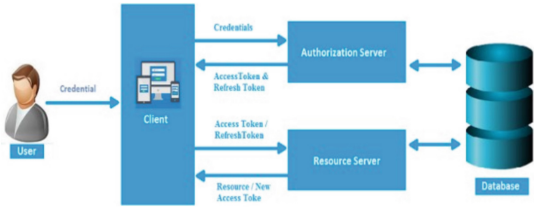


Fig. 4. Factor-Based Authentication and Authorization Systems for web servers The evaluated literature enhanced comprehension of cyber-security and examined the significance of Factor-based authentication in the context of data security. It has been noted that Factor-based authentication can provide businesses with two-factor authentication, which can aid in protecting bank systems and accounts against online fraud [14]. The articles that are included demonstrate that Factor-based authentication has encryption algorithms that may securely transform data into codes employing produced codes for network and system communication.

Users can conduct financial transactions with greater security and effectively reduce internal security risks and concerns with the aid of Factor-based authentication. Businesses are less equipped to fend off cyberattacks and data breaches are more commonplace as a result of inadequate security policies and a lack of awareness. To mitigate the issues arising from Factor-based authentication, it is imperative to establish robust security teams and protocols to minimize future obstacles [12].

Factor-based authentication offers greater flexibility and scalability in terms of.

handling data breaches and hacking issues. It can be integrated with many communication routes. Nevertheless, the created Factors have a single encrypted key that might be compromised by malicious software used by attackers, reducing privacy. Criminals can easily get access to servers and compromise the protection of sensitive data by using generated codes. Building robust and efficient encryption codes for Factor-based authentication is crucial for developers in order to increase privacy and reduce hacking.

Factor-based authentication is a highly recommended feature for security policies and strategies since it can efficiently manage illegal actions and protect data. To minimize the likelihood of hacking, business communities should integrate Factor-based authentication with communication routes that can assist in converting data into codes utilizing encryption software. It is recommended that businesses provide training and

awareness initiatives about authentication and cyber-security to help staff members gain a better understanding and create genuine systems [13].

Companies should also make sure that workers are only visiting legitimate servers, since hackers might create harmful scripts that serve as the basis for third-party servers from which they can gain login credentials. Consequently, communication channels and web servers may be secured against cybercriminals and cyberattacks like malware, DDoS, and brute force can be greatly reduced by utilizing Factor-based authentication.

3 Conclusion

Based on the aforementioned data, it can be said that Factor-based authentication is one of the best strategies for controlling illegal activity and hacking issues. This study contributed to the examination and assessment of Factor-based authentication's significance for improving security and data protection. It is discovered that Factor- based authentication is primarily used to supplement password authenticity with an extra degree of data protection.

It can help businesses manage security threats and weaknesses and suggests two-factor authentication as a way to increase privacy. Developers have developed an encryption- based authentication method to handle such issues and enable the safe construction of web servers and communication infrastructure. Malicious scripts and programs are typically connected to third-party web servers, allowing hackers to steal login credentials and compromise privacy. Factor-based authentication can offer two-factor authentication, which can aid users in maintaining authenticity and enhancing the privacy of their personal information. By completing primary research, subsequent studies will offer a thorough examination of the difficulties and drawbacks of Factor-based authentication.

References

1. Zibaei, S., Salehi-Abari, A., Thorpe, J.: Dissecting nudges in password managers. Proceedings of the Nineteenth USENIX Conference on Usable Privacy and Security. (211–225). https://doi.org/10.5555/3632186.3632198
2. Constantinides, A., et al.: Security and Usability of a Personalized User Authentication Paradigm: Insights from a Longitudinal Study with Three Healthcare Organizations. ACM Transactions on Computing for Healthcare. **4**(1), 1–40 (2023). Online publication date: 31 Jan 2023. https://doi.org/10.1145/3564610
3. Wang, S., Salehi-Abari, A., Thorpe, J.: PiXi: Password Inspiration by Exploring Information. Information and Communications Security, 249–266 (2023). https://doi.org/10.1007/978-981-99-7356-9_15
4. Ratakonda, D., Mehrpouyan, H., Fails, J.: Pictures are easier to remember than spellings!. International Journal of Child-Computer Interaction **33**(C) (2022). Online publication date: 1 Sep 2022. https://doi.org/10.1016/j.ijcci.2022.100515
5. Zibaei, S., Malapaya, D., Mercier, B., Salehi-Abari, A., Thorpe, J.: Do password managers nudge secure (random) passwords?. Proceedings of the Eighteenth USENIX Conference on Usable Privacy and Security. 581–597. https://doi.org/10.5555/3563609.3563640

6. Suárez-Plasencia, L., Herrera-Macías, J., Legón-Pérez, C., Sosa-Gómez, G., Rojas, O.: Detection of DIAG and LINE Patterns in PassPoints Graphical Passwords Based on the Maximum Angles of Their Delaunay Triangles. Sensors **22**(5), 1987 (2022). https://doi.org/10.3390/s22051987
7. Kawamura, T., Ebihara, T., Wakatsuki, N., Zempo, K.: EYEDi: Graphical Authentication Scheme of Estimating Your Encodable Distorted Images to Prevent Screenshot Attacks. IEEE Access **10**, 2256–2268. https://doi.org/10.1109/ACCESS.2021.3138093. https://ieeexplore.ieee.org/document/9662374/
8. Parish, Z., Salehi-Abari, A., Thorpe, J.: A study on priming methods for graphical passwords. Journal of Information Security and Applications **62**(C) (2021). Online publication date: 1 Nov 2021. https://doi.org/10.1016/j.jisa.2021.102913
9. Golar, P., Khandelwal, B.: Graphical-Based Authentication System and Its Applications. Design, Applications, and Maintenance of Cyber-Physical Systems, 63–91 (2021). https://doi.org/10.4018/978-1-7998-6721-0.ch004
10. Raptis, G., Katsini, C., Cen, A., Arachchilage, N., Nacke, L.: Better, Funner, Stronger: A Gameful Approach to Nudge People into Making Less Predictable Graphical Password Choices. Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems. 1–17. https://doi.org/10.1145/3411764.3445658
11. Ndako Adama, V., Oyebisi Oyefolahan, I., Ndunagu, J.: Pure recall-based graphical user authentication schemes: perspectives from a closer look. 3rd African Human-Computer Interaction Conference: Inclusiveness and Empowerment. 141–145. https://doi.org/10.1145/3448696.3448721
12. Golar, P., Khandelwal, B.: Study of Usability Parameter for Graphical Based Authentication System 2020 9th International Conference System Modeling and Advancement in Research Trends (SMART), 23–26 (2020). https://doi.org/10.1109/SMART50582.2020.9337116. 978-1-7281-8908-6
13. Constantinides, A., Belk, M., Fidas, C., Pitsillides, A.: An eye gaze-driven metric for estimating the strength of graphical passwords based on image hotspots. Proceedings of the 25th International Conference on Intelligent User Interfaces. pp. 33–37. https://doi.org/10.1145/3377325.3377537
14. Katsini, C., Avouris, N., Fidas, C.: CogniPGA: Longitudinal Evaluation of Picture Gesture Authentication with Cognition-Based Intervention. i-com **18**(3), 237–257 (2020). https://doi.org/10.1515/icom-2019-0011. Online publication date: 18 Nov 2019, Online publication date: 1 Dec 2019
15. Addas, A., Salehi-Abari, A., Thorpe, J.: Geographical Security Questions for Fallback Authentication 2019 17th International Conference on Privacy, Security and Trust (PST), pp. 1–6 (2019). https://doi.org/10.1109/PST47121.2019.8949063. 978-1-7281-3265-5



The Hybrid STR-ENN Model: A Study with Application

Maryam Luqman Othman and Nihad Shreef Khalaf Aljboori(✉)

Mathematics, College of Education for Women, Tikrit University, Tikrit, Iraq
Mariam.loqman964@st.tu.edu.iq, nihad.shreef16@tu.edu.iq

Abstract. This paper presents a new hybrid model that combines the seasonal trend model (STR) and the Elman neural network (ENN) to forecast seasonal time series with high accuracy and to provide accurate forecasts of seasonal time series. The model is based on dividing the time series into three components: trend, seasonality, and residual components. The STR model first divides the time series into these three components, and then the ENN is trained on each component separately to predict each part. The final results are then combined to obtain the overall forecast of the time series. The model was tested on monthly carbon dioxide emissions data from January 1995 to April 2020. The results showed that the hybrid model performed better than the individual models, achieving a mean absolute error (MAE) of 0.0099 and a mean square error (MSE) of 3.42769×10^{-4}. These results reflect the model's ability to forecast seasonal time series with high accuracy, making it suitable for use in long-term forecasting applications.

Keywords: STR using regression · Elman neural network · STR-ENN hybrid · Decomposition models · and Seasonal change

1 Introduction

Nineteenth-century economics proposed dividing time series into unobservable components [1, 2]. During that period, a lot of studies were conducted to identify "cycles" that allowed economic crises to be predicted and explained, such as in 2015 Dokumentov and Rob introduced new general methods for analyzing seasonal data: STR (performing seasonal trend analysis based on regression) and STR immunity. In some ways, STR is similar to Ridge Regression and the immunity of STR can be related to LASSO [3], An Elman neural network is a recurrent neural network (RNN) designed to capture and store contextual information in a hidden layer. It was first introduced by Jeff Elman in 1990 to process data sequences [4].

Many hybrid models have been presented that combine part of a time series in their structure while the other part represents a neural network. Examples include: In 2020, a study was proposed to predict the number of passengers in the metro based on the STL-LSTM model by [5]. In 2022, Guo et al. presented the state-of-health (SOH) estimation of a lithium-ion battery (LIB) based on the Elman neural network [6]. In the same year This study was presented by He et al. This study presents a hybrid approach

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 104–117, 2025.
https://doi.org/10.1007/978-3-031-91008-1_10

integrating seasonal trend analysis and machine learning (called STL-ML) to predict rainfall time series one step ahead based on historical rainfall and other meteorological (e.g. temperature, humidity, etc.) data [7], and in 2023, Sultana and Nihad presented a study creating a hybrid STL-FFNN structure that combines the STL decomposition model and feed-forward neural networks [8], and Aljboori followed it up with a survey of another hybrid model, STDR-MNN [9].

The main objective of the research is to develop a new hybrid model that combines the seasonal trend model (STR) and the Elman neural network (ENN) to improve the forecasting accuracy of seasonal time series. The goal is to reduce the forecast errors by taking advantage of the advantages of both the seasonal analysis model and the artificial neural networks, allowing the model to generalize better to new data and make more effective and accurate predictions.

The study included five sections, where the first section contained the Decompose Trend and Seasonality using regression (STR) model with a comprehensive diagram of the model's working structure, while the second section included the Elman neural network model, while the third section contained the algorithm for working the proposed hybrid model, while the The fourth represents conducting a comprehensive analysis of real data based on the proposed model, starting from the data entry stage through segmentation of the series, which concluded with a set of figures, tables, and explanations that explain the stages of analysis, along with developing an evaluation group to predict the model to determine the extent of its efficiency. Then, finally, the most important conclusions reached were presented the study.

2 Decompose Trend and Seasonality Using Regression (STR)

The first and simplest STR model describes a time series y_t consisting of three parts:

$$y_t = TC_t + S_t + I_t \tag{1}$$

$$y_t = TC_t \times S_t \times I_t \tag{2}$$

where TC_t is the trend, S_t is the additional seasonal component, I_t is the residual component while $t \in \{1, 2, \ldots, n\}$ and we have k seasons. We assume that $s_n(t) \in \{1, \ldots, k\}$, which converts time t to the corresponding season $s_n(t)$.

We assume that the seasonal component S_t has a constant recurring pattern. At time t we observe (indirectly, through Eqs. (1) or (2)) only one component of the seasonal pattern. The other components of this pattern at that particular moment in time. In other words, we propose to define, together with S_t, Other "unseen" components are responsible for seasonality other than $s_n(t)$. In this way, we treat the seasonal model as a two-dimensional, $\{S_{i,t}\}_{i=1}^{k}$, and assume that $S_t = S_{s_n(t),t}$ where S with one index represents a vector of seasons and S with two indexes represents a matrix of seasonal shapes in Eq. (1). Thus Eq. (2) can be rewritten as follows:

$$y_t = TC_t + S_{s_n(t),t} + I_t \tag{3}$$

where $S = [S_{s,t}]$ is a matrix of dimension k × n, where k represents the number of seasons and n represents the length of the time series.

This representation allows simple constraints to be imposed on the seasonal patterns represented by the matrix $S = [S_{s,t}]$. The entire model can be described as follows:

- I_t represents the residuals, which have a symmetric and independent normal distribution with zero mean and constant variance, i.e. $I_t \sim$ iid $N(0, \sigma_I^2)$
- TC_t represents the smooth trend according to the conditions $\Delta^2 TC_t = TC_{t+1} - 2TC_t + TC_{t-1}$ such that $TC_t \sim$ iid $N(0, \sigma_{TC}^2)$.
- The sum of the seasonal coefficients must be zero, such that it has the property $\sum_s S_{s,t} = 0$ for any time t.
- Each seasonal term varies with a smooth transition over time, such that all time periods ∀t have the vectors $\{\Delta_t^2 S_{s,t}\}_{s=1}^k = \{S_{s,t+1} - 2S_{s,t} + S_{s,t-1}\}_{s=1}^k$ which $S_{s,t} \sim$ iid $N(0, \sigma_S^2 \Sigma_S)$, ∀t is inside the vectors, so that Σ_S represents a matrix of dimension k × k which can be considered as the covariance matrix of k random variables $\xi_s = \lambda_s + \frac{1}{k}\sum_{r=1}^{k} \lambda_s$ obtained from $\lambda_1, \ldots, \lambda_k \sim$ iid N(0, 1) of random variables.
- The model parameters are given by σ_I^2, σ_{TC}^2, TC_0, TC_1, $S_{s,0}$, $S_{s,1}$, or $\{S_{s,n}\}_{s=1}^k$.
- It should be noted that in this simpler form of STR, the seasonal component is presented as a two-dimensional matrix only to ensure that the seasonal components add to zero for any t.
- In another case, we assume that our time series y_t can be further decomposed as follows:

$$y_t = TC_t + \sum_{i=1}^{I} S_t^i + \sum_{p=1}^{P} \alpha_{p,t} z_{p,t} + I_t \tag{4}$$

where TC_t and S_t^i represent the smooth variable direction (the fact that the function is smooth means that its second derivatives are small because, otherwise, large values of the second derivatives would lead to a high curvature of the function, making it oscillatory), and the variable seasonal components smooth with complex topology respectively, while $z_{p,t}$ represents covariates with coefficients $\alpha_{p,t}$ that may be time-varying and even seasonal, I_t represents the remainder [10].

The modeling process of the STR model roughly includes three stages which are as follows: model preparation, parameter estimation in the model, and model evaluation. The process of preparing the electronic model includes determining the lags of the regression part, nonlinearity testing, and pattern identification. The evaluation phase of the model includes goodness-of-fit testing and goodness-of-fit testing. The modeling steps for STR model domains are as follows [3]:

3 Elman Neural Network

Abbreviated as ENN, is considered one of the types of recursive neural networks. An Elman network is referred to as a simple recurrent network, and it is a special case of artificial recursion. It differs from traditional two-layer networks in that the first

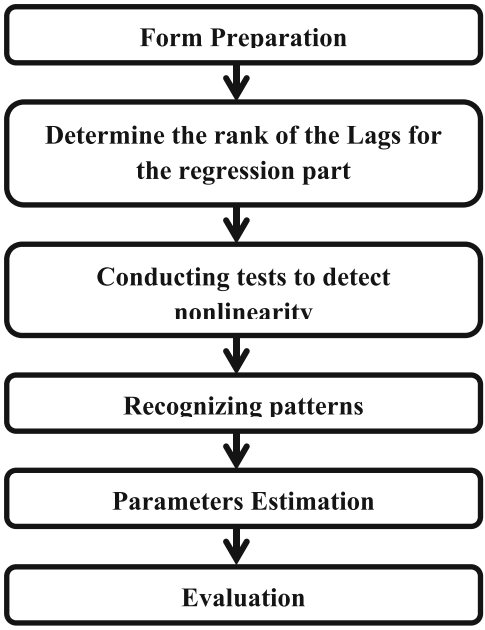


Fig. 1. STR model modeling process diagram [3]

layer contains recurrent communication. That is, it is a simple artificial neural network consisting of three layers and has a back loop from the hidden layer to the input layer, called the context layer, and the outputs of the context layer are inputs to the hidden layer, it contains a memory that allows it to detect and generate temporal variables patterns, and it usually contains sigmoid artificial neurons in the hidden layer, and linear artificial neurons in the output layer. With this combination of artificial neurons, the transfer functions can approximate any function with arbitrary accuracy if only there are enough artificial neurons in the hidden layer. The Iman network is similar to the Jordan network, except that the only difference is that the context units are fed from the output layer instead of the hidden layer [11].

4 The STR-ENN Hybrid Model

The hybrid model is based on the assumption that the STR model is responsible for dividing the data series into three components, which are a seasonal component, a trend component, and a residual component. Perhaps it is restrictive to confirm that the rest of the time series is processed using regression, after which all components are delivered to the ENN network to train and test the data. Received from the seasonal model. Below are the steps for making the proposed model:

1. Entering the studied data series.
2. Check the stability of the series before creating the model. A preprocessing process such as the difference transformation procedure transforms the data into a stable time series.

3. Using Eq. (4), the series is divided into three components, where the trend component describes the basic smooth mean of the data (after accounting for seasonality). The remaining component (which is assumed to be uncorrelated) contains only noise and characteristic patterns in the data.
4. Estimating the regression coefficients in the residual component is the last step in the steps of making the seasonal model.
5. Divide the data for each component obtained in step (3) into two groups: a test group and a training group.
6. Training the three obtained sequences using the ENN neural network, in order to predict the test sets for each component separately.
7. Combine the prediction results of the three components using Eq. (2.8) again to obtain a prediction for the original series.
8. Calculate the mean absolute error (MAE) and mean square error (MSE), as well as calculate the relative error value R. Through the equations:

$$MAE = \frac{1}{T}\sum_{k=0}^{T}|\hat{y}_k - y_k| \tag{5}$$

$$MSE = \frac{1}{T}\sum_{k=0}^{T}(\hat{y}_k - y_k)^2 \tag{6}$$

$$R^2 = 1 - \sum_{j}\left(\overline{y}_k - y_k\right)^2 / \sum_{j}(\hat{y}_k - y_k)^2 \tag{7}$$

where y_k represents the original observation value at time k, while $\hat{y}_k$ represents its prediction value, T represents the length of the data series, and $\overline{y}_k$ represents the values of the average observations.

9. The model with the best predictive indicators in the test set represents the best model that can be used to predict the data series.

5 Data Analysis Using a Hybrid STR-ENN Model

On the practical level, and for the purpose of knowing the efficiency of the proposed model, we should have touched on a practical aspect that was conducted by modeling that simulates the structure that was mentioned previously.

The data used in this application was the monthly emission rates of carbon dioxide (CO2) into the Earth's atmosphere, and the amount of carbon dioxide is measured in parts per million (ppm), i.e. (mg/l). For the period from (01-01-1995 to 04-30-2020), 304 views, obtained from the website https://www.kaggle.com/datasets.

The data was divided into two parts, the first part consisting of 296 observations that were relied upon to build the structure of the model, while the second part consisted of the last 8 observations that were developed as a test set for the efficiency of the proposed model.

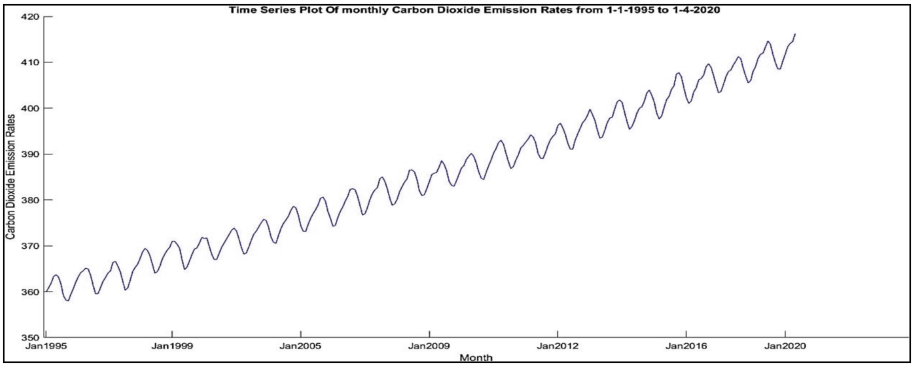


Fig. 2. Monthly CO2 emission rates in the Earth's atmosphere

First Stage: As we mentioned previously, in order for the analysis to be complete, the first stage must be the description stage. Here, the data series is drawn and its stability is known. Figure 1 represents a plot of the data series representing monthly rates of carbon dioxide emissions from the Earth's atmosphere, measured in units of mg/l.

The previous figure shows a noticeable increase in the time series, with seasonal fluctuations in its components.

Figure 3 shows a plot of ACF and PACF for 20 Lags, to complete the description stage of the studied series.

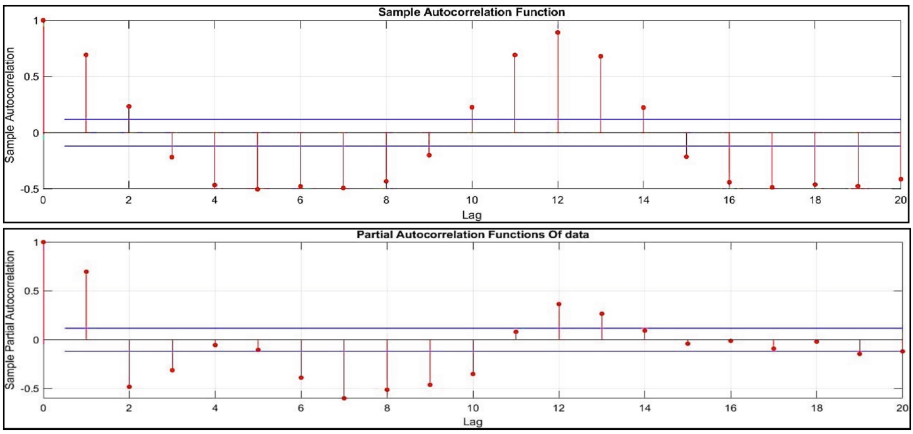


Fig. 3. Plot of ACF and PACF

The time differences in Lags shown in Fig. 2 illustrate the extent of the instability of the time series, as ACF and PACF showed instability, through all the Lags in the ACF outside the confines of the confidence interval, while in the PACF there are 11 Lags outside those limits. Known as the relationship $\frac{\pm 1.96}{\sqrt{n}}$, where n is the length of the time series [12, 13].

Second stage: This stage is called the modeling stage (capturing the random structure of time series by specifying the appropriate model), but before starting this stage, a pre-processing process must be carried out to give stability to the data series, and at this stage, the logarithm transformation of the series is used. Figure 4 shows the data series after performing a logarithm transformation.

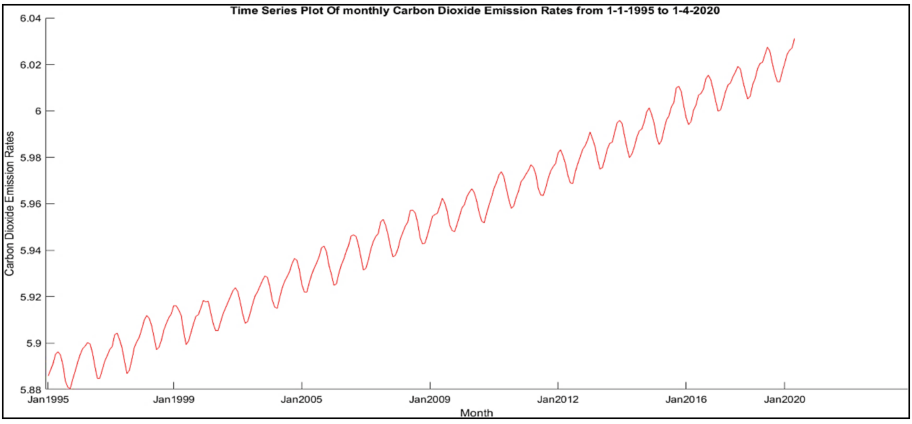


Fig. 4. Logarithm of the data series

Third Stage: After giving the time series numerical stability, the seasonal STR model is used to divide the time series into three sub-parts (seasonal, trend, and reminded). Figure 5 represents the sub-parts of the time series, while Tables 1, 2 and 3 represent the values of the trend series, the seasonal series, and the residual series, respectively.

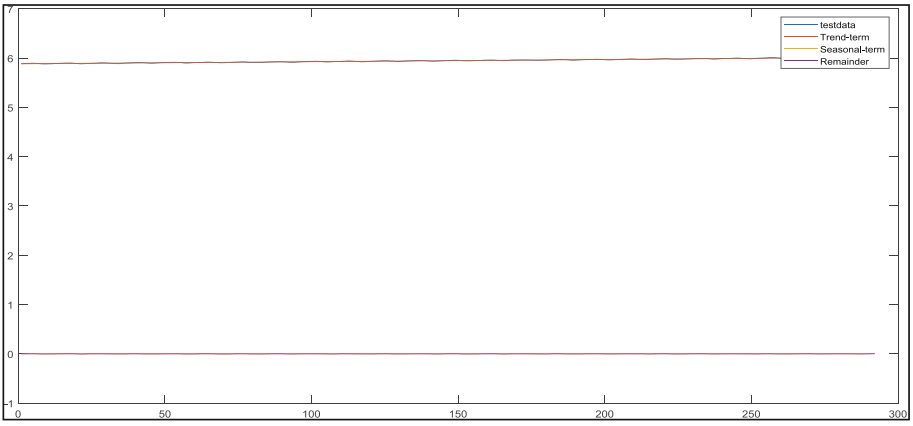


Fig. 5. Sub-parts of the time series

From Fig. 4, we notice that the data series has high trend values, and as we mentioned previously, values of the residual series close to zero indicate that the seasonal components and trend are accurate in describing the time series, meaning that there is little noise in the time series after analysis.

Fourth Stage: Now that the segmentation stage of the original series has been completed, and before moving to the stage of operating the neural network, the regression parameters of the residual series are estimated to prepare the series as a final step to deliver them to the neural network.

Each sub-series of the three series is divided into two groups, a test group with 80%, and a training group with 20%, and 10 hidden layers with a stopping time of 1000. The average values are also calculated, which represents the value 5.9519 used in calculating the relative error defined in Eq. 6. Figure 6 represents the neural network diagram.

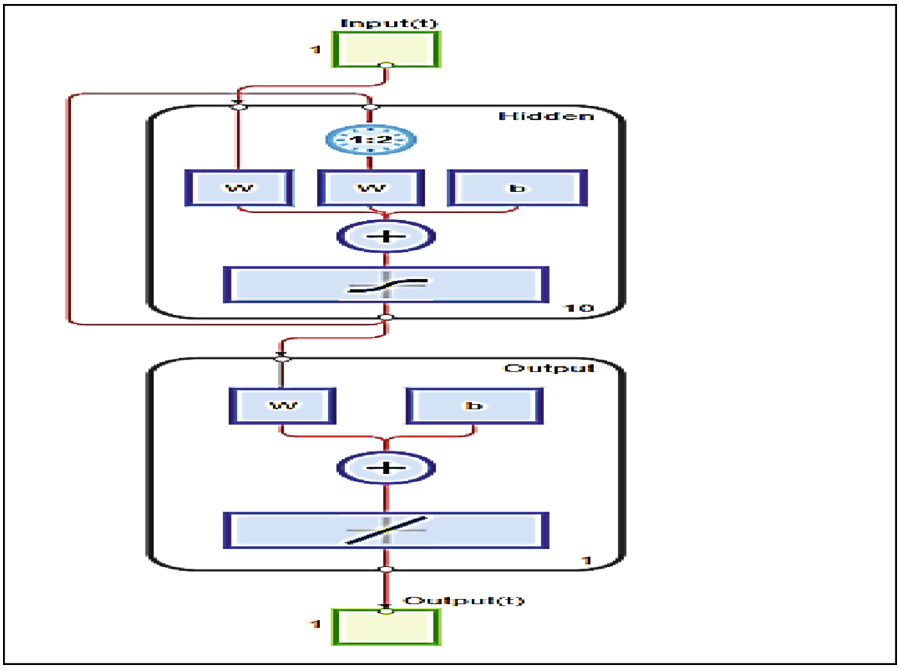


Fig. 6. Neural network diagram

Where Table 4 represents the values of the training set.

Using ten hidden layers with a stopping time of 1000 and to prevent overfitting, several measures are taken, namely early stopping: training is stopped when the performance on the validation set starts to deteriorate while it continues to improve on the training set. This helps to avoid the model learning patterns that are specific to the training set only. Validation Data: A portion of the data is used to validate the performance during different stages of training. This monitors generalization and prevents the model from overfitting.

Table 1. The values of the training set.

Units	Initial Value	Stopped Value	Target Value
Epoch	0	211	1000
Elapsed Time	-	00:06:04	-
Performance	3.35e-05	1.13e-05	0
Gradient	0.000202	3.51e-05	1e-05
Validation Checks	0	6	6

As follows, Fig. 7 shows the training and validation set values for best validity, while Fig. 8 represents the training case.

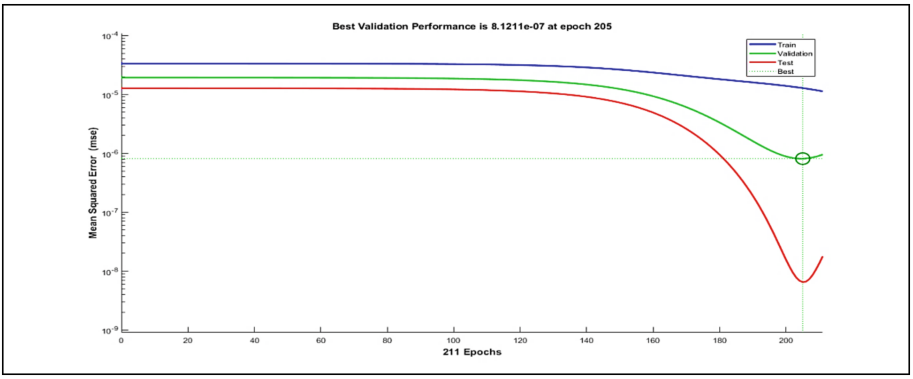


Fig. 7. Shows the training and validation set values for the best validity

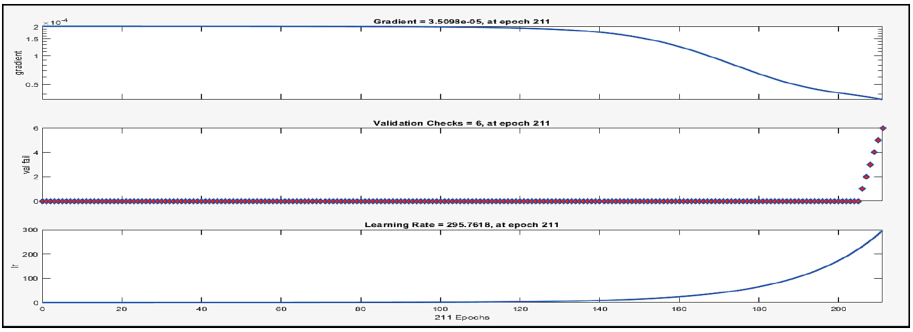


Fig. 8. Represents the training case.

As shown in the figure above, the regression values are equal to $3.5098e^{-05}$, while the validation checks value is equal to 6, and finally, the learning rate value is equal to 295.7818 at cycle 211.

The error values in the graph with 20 bins can be observed in Fig. 9 as follows:

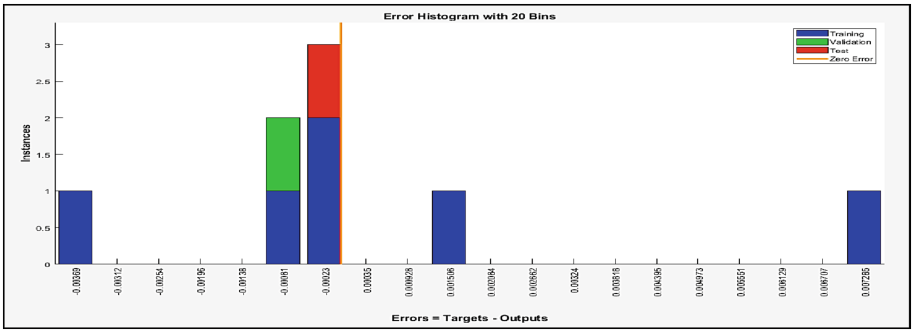


Fig. 9. Error values for a histogram with 20 boxes

The error histogram is a graph of the errors between the target values and the expected values after training the feedforward neural network (ENN). Since these error values indicate how much the expected values differ from the target values, they can be negative, or the boxes are the number of vertical bars you notice on the chart. The total error range is divided into 20 smaller bins here. The y − axis represents the number of samples from the dataset of the series that fall into a particular bin. For example, in the middle of the series plot, the bin corresponding to the error has 0.00029 and the height of that bin for the training dataset is below but near 3 and the validation and testing dataset is between 2.5 and 3. This means that many sample samples from different sequence data sets have errors lying in this next range. The zero error line corresponds to the zero error value on the error axis, i.e. the x − axis. In this case, the zero error point is located at the bottom of the box at center 0.00029.

Therefore, Fig. 10 shows the regression of training the ENN neural network at the end of cycle 211, as it plots the linear regression of the goals in relation to the outputs.

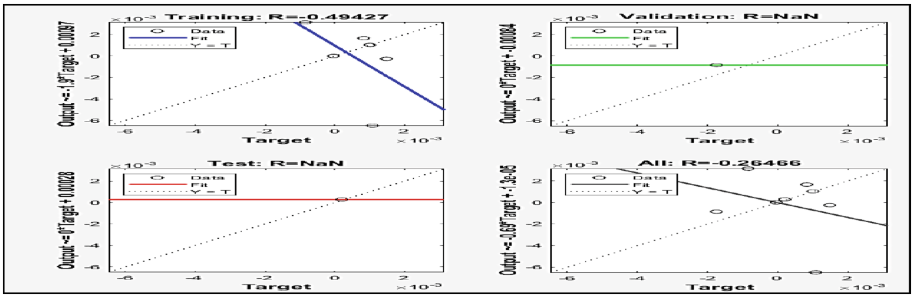


Fig. 10. ENN training regression

The response of output element-1 to time series-1 is shown as follows (Fig. 11):

The response of output element-1 to time series-1 means that the time series is target t (i.e., the target of the time series) and the output time series is y (i.e., the output of the

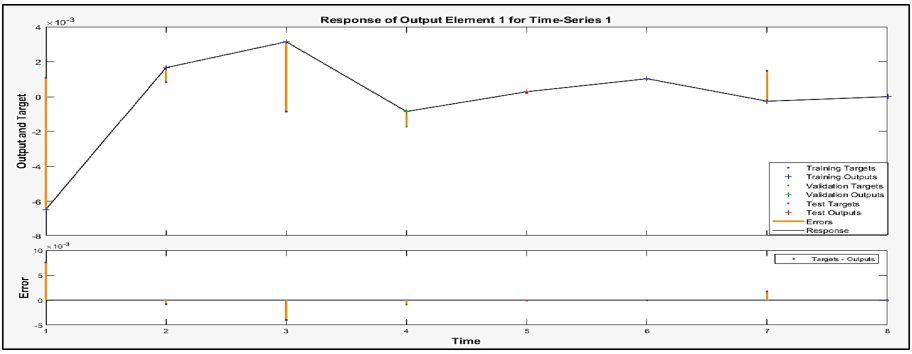


Fig. 11. Response of output component-1 to time series-1

time series), and plots them on the same axis, explaining the errors between them (i.e., consider the multi-input-output time series problem using Deep learning tools in ENN. As for drawing the autocorrelation function for errors in the neural network, it is 8 Lags. It is shown in Fig. 12 as follows:

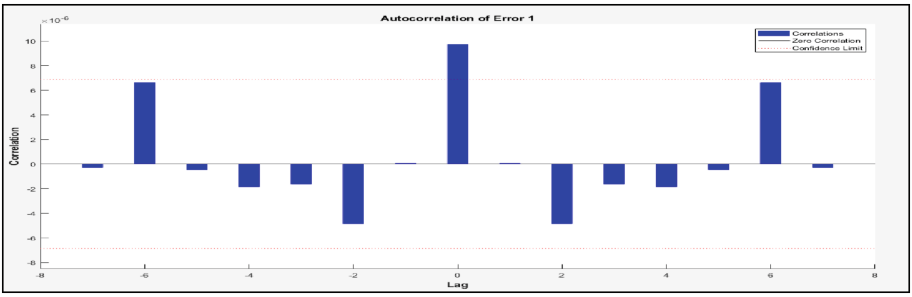


Fig. 12. Autocorrelation of ENN errors

The previous figure represents the presence of only one value outside the confidence interval. Figure 13 represents the correlations between the input and output errors of the ENN neural network.

In the above correlation framework, the biggest driver of output is the input that has the largest absolute correlation value. Such that the correlation lies in the range [-1,1], and: A negative correlation ($\rho < 0$) indicates that input and output move in opposite directions that is, as input increases, output decreases (and vice versa), while a zero correlation ($\rho = 0$) indicates that the two variables are completely unrelated. A positive correlation ($\rho > 0$) indicates that input and output move in the same direction—that is, as input increases, output increases (and vice versa). In the figure above, it appears that the inputs have a negative and positive correlation. This means that there are correlations between the inputs that move in the same direction as the outputs, and there is also the opposite.

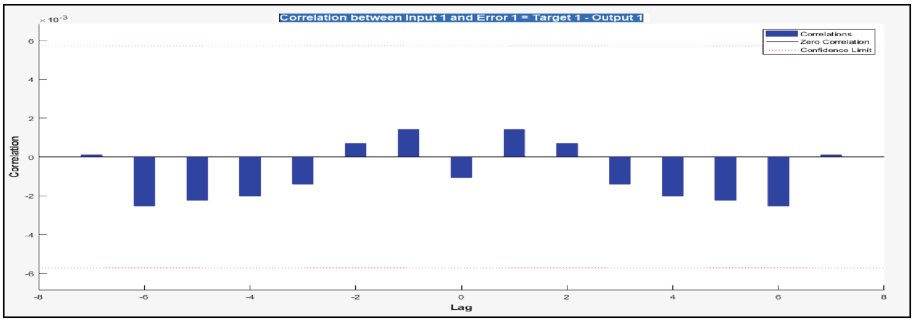


Fig. 13. Correlation between the input and output errors of the ENN neural network

Fifth Stage: Finally, the outputs of each sub-series (seasonal, trend, remainder) are obtained for the ENN. As we mentioned previously in the algorithm or scheme of the proposed model, the outputs of each sub-series are collected using Eq. 6 to obtain predictions for the proposed STR-ENN model, while Fig. 14 shows the values of the evaluation group of the data series (the last 8 observations of the original series) with the predictions for the hybrid model.

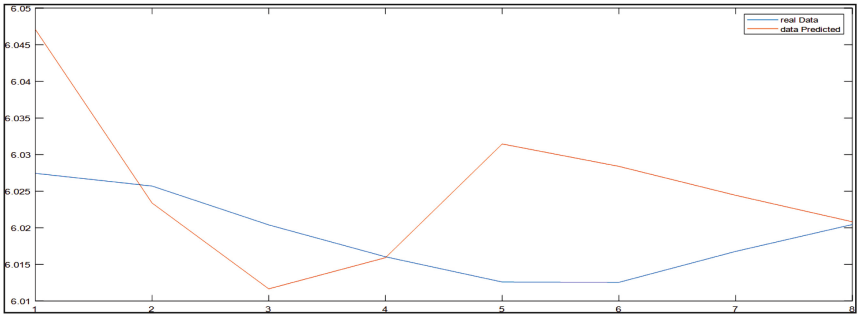


Fig. 14. Orthographic ensemble values for the data series with predictions for the hybrid model

Finally, the following table shows the forecast values of the STR-ENN, ENN, and STR models with the evaluation group, in addition to the forecast accuracy sampling criteria MAE and MSE [14].

Looking at the results of Table 5, we find that the predictive values using the Elman Neural Network (ENN) show convergence with the actual data but are not completely accurate. For example, the first predicted value using the ENN is 6.0706 compared to the actual value of 6.0274, which means that there is a relative error between the two values. The predictive values using the Seasonal Trend Model (STR) differ significantly from the actual data, as the values are presented in the range of 12.03 to 12.04, which is very far from the actual values, indicating that this model is not suitable for prediction alone without combining with other techniques. While the predicted values using the hybrid STR-ENN model are closer to the actual values compared to the other models.

Table 2. Prediction values for the hybrid model in addition to the values of the original observations for the evaluation group, with MAE and MSE

	Real Data	Forecasting by STR-ENN	Forecasting by STR	Forecasting by ENN
1	6.0274	**6.0471**	12.0384	6.0706
2	6.0257	**6.0234**	12.0479	6.0293
3	6.0204	**6.0117**	12.0345	5.9699
4	6.0160	**6.0159**	12.0491	6.0000
5	6.0126	**6.0314**	12.0389	6.0253
6	6.0125	**6.0284**	12.0483	6.0228
7	6.0168	**6.0244**	12.0349	6.0205
8	6.0204	**6.0208**	12.0414	6.0075
MAE		**0.0099**	6.0198	0.0198
MSE		$\mathbf{3.42769 \times 10^{-4}}$	6.0222	6.639175×10^{-4}

For example, the first predicted value is 6.0471 while the actual value is 6.0274, which means that the difference is very small, which is an indication of the accuracy of the model. This convergence appears in almost all values, as the predicted values using the hybrid model are very close to the actual values, indicating the efficiency of this model in prediction.

6 Conclusions

The results showed that the hybrid model combining the seasonal trend model (STR) and the Elman neural network (ENN) had high accuracy in forecasting seasonal time series. The mean absolute error (MAE) was 0.0099, and the mean square error (MSE) was 3.42769×10^{-4}. These results indicate the model's efficiency in dealing with unseen data and achieving accurate forecasts. The hybrid model also excelled in its ability to divide the time series into three main components: trend, seasonality, and residuals. The analysis showed that the trend accounted for the bulk of the data, while seasonality and residuals had little effect, which enhanced the model's accuracy in describing the time series. Compared to the individual models (STR and ENN), the hybrid model showed superior performance in forecasting time series. For example, the predicted values using the hybrid model were much closer to the actual values than the predicted values using the individual models, confirming the hybrid model's efficiency in improving forecasting. Despite the high prediction accuracy, the model consumed a relatively large computation time of 00:06:04, which is considered long compared to the individual models. This indicates the need to improve the computation efficiency of hybrid models to achieve a balance between accuracy and speed.

References

1. Sen, R., Das, S.: Computational Finance with R. Springer Nature (2023). https://doi.org/10.1007/978-981-19-2008-0
2. Buys-Ballot, C.H.D.: Les changements périodiques de température, dépendants de la nature du soleil et de la lune, mis en rapport avec le pronostic du temps, déduits d'observations néerlandaises de 1729 à 1846. Kemink (1847)
3. Dokumentov, A., Hyndman, R.J.: STR: A seasonal-trend decomposition procedure based on regression. Monash Econometrics and Business Statistics Working Papers **13**(15), 2015–13 (2015). https://EconPapers.repec.org/RePEc:msh:ebswps:2015-13
4. Elman, J.L.: Finding structure in time. Cogn. Sci. **14**(2), 179–211 (1990). https://doi.org/10.1207/s15516709cog1402_1
5. Chen, D., Zhang, J., Jiang, S.: Forecasting the short-term metro ridership with seasonal and trend decomposition using loess and LSTM neural networks. IEEE Access **8**, 91181–91187 (2020). https://doi.org/10.1109/ACCESS.2020.2995044
6. Guo, Y., Yang, D., Zhang, Y., Wang, L., Wang, K.: Online estimation of SOH for lithium-ion battery based on SSA-Elman neural network. Protection and Control of Modern Power Systems **7**(3), 1–17 (2022). https://doi.org/10.1186/s41601-022-00261-y
7. He, R., Zhang, L., Chew, A.W.Z.: Modeling and predicting rainfall time series using seasonal-trend decomposition and machine learning. Knowl.-Based Syst. **251**, 109125 (2022). https://doi.org/10.1016/j.knosys.2022.109125
8. Sultana, Z.A., Aljbooria, N.S.K.: Seasonal Decomposition and Trend using Hybrid STL-FNN with Application. Advances in the Theory of Nonlinear Analysis and Its Application **7**(4), 35–46 (2024). https://doi.org/10.17762/atnaa.v.i.280
9. Aljboori, N.S.K.: Structural structure of the STDR-MNN Hybrid Model with Application. Advances in the Theory of Nonlinear Analysis and its Application **7**(4), 89–98 (2023). https://doi.org/10.17762/atnaa.v7.i4.285
10. Dokumentov, A., Hyndman, R.J.: STR: Seasonal-trend decomposition using regression. INFORMS Journal on Data Science **1**(1), 50–62 (2022). https://doi.org/10.1287/ijds.2021.0004
11. Krenker, A., Bešter, J., Kos, A.: Introduction to the artificial neural networks. Artificial Neural Networks: Methodological Advances and Biomedical Applications. InTech, 1–18 (2011). https://doi.org/10.5772/15751
12. Noori, N.A., Mohammad, AA.: Dynamical approach in studying GJR-GARCH (Q, P) models with application. Tik. J. of Pure Sci. **26**(2), 145–156 (2021). https://doi.org/10.25130/tjps.26.2021.040
13. Khalaf, N.S., Abdullah, H.H., Noori, N.A.: The Impact of Overall Intervention Model on Price of Wheat. Iraqi Journal of Science, 853–862 (2024). https://doi.org/10.24996/ijs.2024.65.2.22
14. Abdullah, H., khalaf, N.S., Noori, N.A.: Comparison of non-linear time series models (Beta-t-EGARCH and NARMAX models) with Radial Basis Function Neural Network using Real Data. Iraqi J. Comp. Sci. Math. **5**(3) 26–44 (2024). https://doi.org/10.52866/ijcsm.2024.05.03.003

Optimizing HMIM Logic Gates Using Hybrid Plasmonic Waveguides to Reduce Ohmic Losses

Wissam Hussien Hadi[1(✉)], Faris Mohammed Ali[1], and Raad Abrahem Khleed[2]

[1] Engineering Technical College, Al-Furat Al-Awsat Technical University, Najaf, Iraq
wessamhh.82@gmail.com, faris@atu.edu.iq

[2] Department of Medical Instruments, Engineering Techniques, Al-Farahidi University, Baghdad, Iraq
raed.khalid@alfarahidiuc.edu.iq

Abstract. Optical circuits have been introduced as an alternative to electronic circuits as a means of transmitting signals. Both types, optical and electronic, are subject to the phenomenon of signal dispersion especially at light curves when the wavelength is smaller than 0.5 of the wavelength. To achieve this, two hybrid plasmonic routers are used. The first type - abbreviated as (HMIM) - is designed with an insulating core sandwiched between semiconductor layers on both sides and then covered with two layers made of metal. The second hybrid plasmonic router (HIMI) has a metal core sandwiched between semiconductor layers on both sides topped with two more insulating layers. These hybrid routers have been used in five logic gates, namely XNOR, XOR, AND, NOR, OR, and OR. Two wavelengths have also been adopted to ensure that the hybrid routers perform their assigned tasks efficiently. The two wavelengths are 1550 nm and 820 nm. In order to measure the efficiency of each logic gate in the presented waveguides, the contrast ratio was determined to achieve the highest contrast ratio at XOR in the HIMI architecture of 33 dB. As for the issue of logic gate size, the solution was to design logic gates ranging from 1000 nm^2 to 8000 nm^2, which is much smaller compared to the sizes of existing logic gates.

1 Introduction

1960 witnesses one of the pivotal technical innovations, that is, the invention of Laser-Light Amplification by Stimulated Emission of Radiation. The existence of Laser greatly aids in producing and advancing light beams that are phase-structured. They also vitally contribute to the production and development of frequencies that are homogenous along. During the 1980s, communications that are fiber-optic based were on the verge of breaking out, yet another milestone in science and technology. At this juncture, the capacity of transmitting data through the optical fibers was entirely realized. In the current state, optical fibers were developed to transfer optical signals over long distances. This technology involves focusing light beams based on the refractive properties of any transparent material, such as glass or plastic. What is essential in this technology is that, unlike all its predecessors, optical fibers allow data transmission at very high speeds over large distances without losing a clear signal, noticeably degrading it at least. The seminal study [1] has established the significance of the fiber-optic based communications.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 118–129, 2025.
https://doi.org/10.1007/978-3-031-91008-1_11

After the eighties of the last century, the limits to optical technologies were tested coupled with the emergence of astonishing ground-breaking technological advancements on nanoscale levels [2]. Such advancements impacted the filed of photonics starting what is known as the 3rd breakout of photonics namely, nano-photonics. To put it differently, this breakout led to investigate how light and matter interact on a nano level [3]. Therefore, nano-plasmonics was born because of the remarkable optical properties that metal at the nanoscale had brought forth according to which nano-plasmonics could be leveraged to guide and boost the process in which light and matter interact on a nano scale level. As a field of exploration, nano-plasmonics is promising due to potential applications across disciplines including sensor development, laser production, energy storage as well as transmission. In general, future potentials are likely to lie in the areas of optimization of optical devices, development of photonic chips, and techniques for improved optical performance. Perhaps one of the future challenges that will make a significant change in the field of photonics is light direction and guidance at the level of nanometers. Developments in the field of nanophononics and related fields have continued since then. The technology to create nanodevices has indeed advanced, and the techniques for sensing and analysis have evolved to the nanoscale. There is a wide range of uses for nano-photonics, from improving the features of medical devices to sensor technology to enhancing efficiency in optical devices [4, 5]. The structure of a MIM plasmonic waveguide is somewhat different from that of an IMI waveguide. It is composed of a dielectric film, the thickness of which is denoted as 'd', having a dielectric constant of ϵd. Cladding and substrate wrapping over the dielectric layer are further included onto the metal, having complex-valued permittivities ϵc and ϵs, respectively. The schematic diagram of the MIM waveguide structure can be depicted in Fig. 9. To understand the plasmonic mode that is guided within the MIM waveguide structure, the characteristic mode [7, 8].

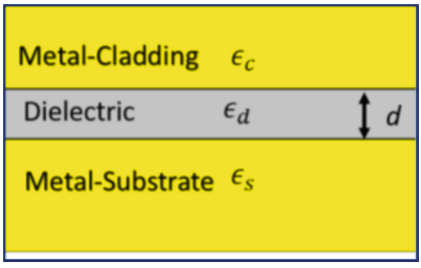


Fig. 1. Structure of the MIM plasmonic waveguide

The plus sign expressed in the model associates with the LRS-MIM standing for the (Long Range Symmetrical Multi-Mode). Moreover, it resembles the fundamental MT (transverse magnetic) mode which as highlighted above. The model with a negative sign belongs to the short-range antisymmetrical Multi-Mode (SRA-MIM). Owing to their relatively low propagation loss, it is only the LRS-MIM modes that will be considered for this discussion [9–11].

2 The Proposed System

Logic gates that are high-speed are indispensable for applications necessary of chip-level optical computing including data encryption, binary combination, tag switching, switching, header recognition, pair checking, among other applications. At present, all reported logic gates have either been electrically or entirely optically operated. Traditional electronic gates exhibit a number of limitations, including delays, race conditions, heat loss, and vibrations. Such limitations could be eliminated by means of devising all-optical logic gates (AOLGs) that are linear interferometry dependent. After that, each gate in the cascade circuit can be induced synchronously with a reduced state delay, different from electronic logic gates.

The gates of AOLGs are disadvantageous due to the poor contrast ratio between the '1' and '0' logic states caused by the lack of interference effect. Furthermore, it is also difficult to control the difference in phase between the two data input arms. Though this can be minimized by miniaturizing the device, this miniaturization is not possible with conventional optical logic gates as they are limited below the wavelength range by refraction. On the other hand, logic gates depend on surface plasmons at a nanometer scale, but they have giant ohmic losses and hence cannot be practically realized.

AOLGs that depend on hybrid plasmon indices (HPWGs) offer a promising resolution as they combine the advantages of both conventional photonic and pure plasmonic techniques. This work introduces the design of logic gates for HMIM (hybrid metal insulator) PWG AOLGs operating at two operation wavelengths of 820 nm and 1.55 nm for the first time: AND, NOR, OR, XNOR, XOR. Such design yield strong confining capability, lower propagation losses, improvements in Ohmic and transmission efficiencies. Add to that, the theoretical underpinnings according to which the linear interference is utilized to design logic gates. Consequently, the HMIM PWG-based logic gates are featured as superior to other logic gates.

This work adopts the theoretical underpinnings of linear interference, implemented using a Y-splitter. The Y-splitter based on plasmonic HIMI and HMIM was studied at 1.55 wavelengths, followed by designing logic gates utilizing optimized parameters. The suggested splitter is supposed to be more efficient than those reported in the literature. Large-scale integration with multilayer-directed constituents including loop flexors, turns, splitters, logic gates, among other components, can make excellent use of this study.

Each simulation was carried out employing the Comsol Multiphysics 6.0 software. This software aids in designing and analyzing comprehensive electro magneticity, and it applies a numerical finite element method for surface division. HMIM PWG was applied to power dividers and logic gates' designs. A similar guide is shown in Fig. 1, wherein silicon has been taken as a base layer reinforced by two thin layers of silica. In contrast, metal coverage on both sides of silica provides the combination strength. The properties of the process materials: silicon, silica, and silver, have made it plausible to formulate high insulators, low insulators, and metals. Material properties are kept as they are. Here, silica is a base coat, and air is a sheathing layer. The conventions for guide width, metal thickness, distance thickness, and high insulator thickness are denoted as W, tm, ts, and th in Fig. 1. These can be feasibly implemented.

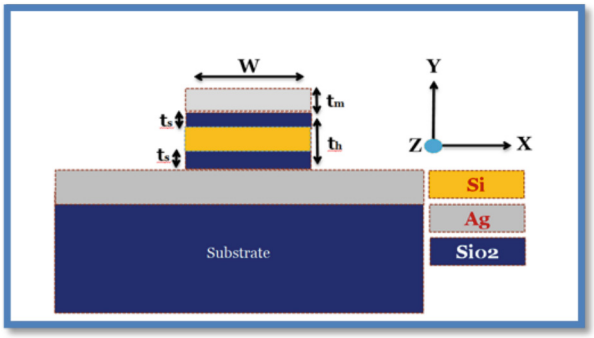


Fig. 2. Transversal view of the HMIM plasmonic waveguide

The effects of the logic gates AND, NOR, XNOR, OR and XOR are inputted to be calculated for each instance separately. Both of the S-parameter (in dB) and ohmic loss are employed to measure the Intensity-Contrast-Ratio exhibited by individual gates.

3 Results and Discussion

The HMIM plasmonic waveguide differs from a standard one when light transmits across an interface that is insulator-metal-dielectric. Within the HMIM plasmonic waveguide, plasmonic modes are supported at the Ag-SiO interface, and the silicon strip supports the usual dielectric mode—the two modes couple in a SiO2 thin film to result in combined plasmonic modes. The HMIM plasmonic waveguide is formed with varying materials from the conventional guide; therefore, the parameters are optimized to create efficient propagation of the principal mode, using quite a few modifications. This was satisfied in the excellent scheme of the primary working mode, between the diffusion length and confinement. This happens when the two modes: plasmonic and average dielectric stay under the same conditions.

The HMIM-XOR gate is a logical gate that works logically according to XOR operations. The XOR gate equates two signals that are considered input. And it provides a signal as an output that has the value 1 when the two signals are disparate; otherwise, a 0 output is provided. For the purpose of designing a logic gate of the XOR type and for achieving its maximum performance, the complementary arms are utilized to realize maximum optical interference efficiency, which results in rising loss due to radiation. In addition, the gate would endure deterioration in its optical efficiency with regard to interference. An enhanced performance was realized via employing unique dimensions for designing the gate, for which tm = 5 nm, ts = 5 nm, th = 5 nm, w = 20 nm, and L = 410 nm. It's worth mentioning here that the performance was already satisfying. It has to be noted that the threshold limit is −4 dB. Moreover, any value that is greater than −4 dB was treated as a non-activated "0" logic state.

The achieved values highlighted in Table 1 are the ones for the XOR gate configuration when a wavelength of 1550 nm was used with HMIM, as shown in Fig. 2. Therefore, we realize that this HMIM-XOR gate yields a correct output result '1' in case the two

input signals happen to have dissimilar values: (0,1) or (1,0); and if there are two signals that are similar, '1', '1' or '0', '0', then the answer will be '0'. The given values for S-parameter (dB) and ohmic losses are preferable to obtain the desired performance. The intensity contrast ratio for the indicator is 21; from Table 1, this means that the gate can commendably differentiate between the states that are either high and low. The results, in general, depict that the HMIM-XOR gate, invoking the HIMI photoelectric waveguide, carries out the logical XOR operation with high accuracy and efficiency (Fig. 3).

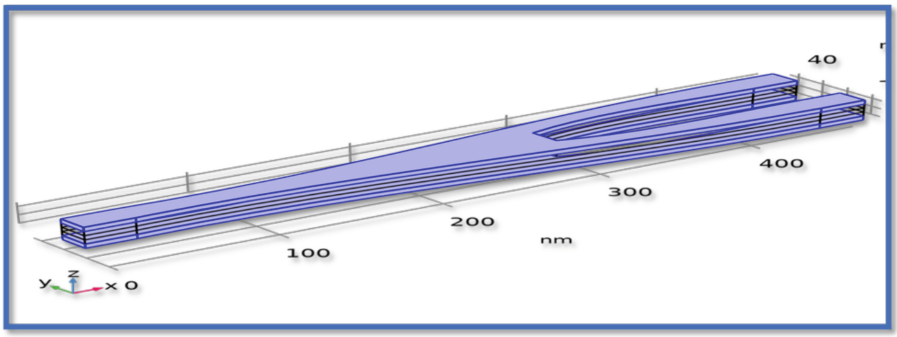


Fig. 3. Logic gate of the XOR – HMIM type

Best case: (1, 0) from Table 1. In this instance, it is established that the gate of HMIM-XOR type delivers the proper output result (1) for both the different input signals with the value of (0, 1). The ohmic losses here were found to be low, having the value 0.1213, and slightly affect the gate's performance. Another S-parameter (dB) having a value of −1.88 was also meager compared with the threshold limit (−30 dB) as a reference to the coefficient; thus, the value was not attainable due to its low value.

Table 1. Values achieved by the logic gate of the XOR-HMIM type at a wavelength of 1550 nm

Input1	Input 2	output	ohmic -loss	S. parameter (Mag)	S. parameter(dB)
0	0	0	1.7333	0.17777	−15.001
1	0	1	0.1222	0.80555	−1.888
0	1	1	0.70444	0.49444	−6.111
1	1	0	2.6444	0.070888	−22.999
INTENSITY CONTRAST RATIO – C.R					21

4 The Logic Gate of the HMIM-OR Type - 1550 nm

This logic gate performs specific logic operation, namely OR. The logic gate of the OR type equates two signals that represent the input, and it produces an output signal accordingly. The output signal will have the value of 1 if either of input signals equals

1 and 0. In the case that both of the input signals are the same, then the value will be inverted to the function of XOR.

An OR gate with two input signals is designed with a footprint of 10*800 nm square at a wavelength of 1.55 nm. An OR gate is a device that allows one signal as the output based on two signals.

A dimension was chosen that would best perform for the purpose of designing the gate at hand, with tm = 5 nm, ts = 5 nm, and th = 5 nm; w = 20 nm, L = 410 nm. It is shown that this dimension was reached when using these dimensions because the gate's performance is already satisfactory, as illustrated in Fig. 4.

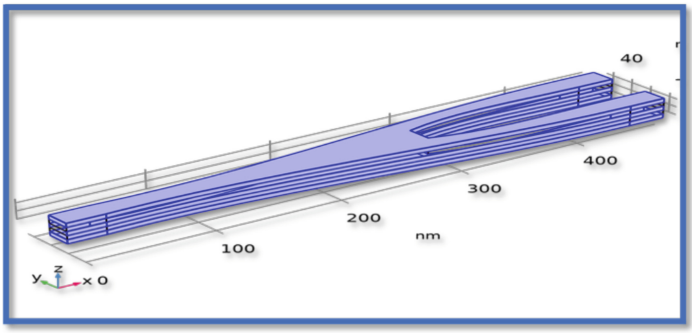


Fig. 4. The logic gate of the OR – HMI type

The HMIM-OR gate is a logic gate of the OR type. It performs the logic function, OR. The OR gate contrasts two signals from the input for generating signals as output. The output signal will have the value 1 in case that one of the inputs equals 1. However, the output signal will have the value 0 in the case that the two input signals are equal, forming the inverse value of the logic function XOR.

Obtained Results:

1. **Case number one:**
   - o S-parameter (dB): −13.7
   - o S-parameter (Mag) value: 0.20666
   - o Ohmic losses: 1.5777

   In accordance, it could be noted that, in the two sets of input signals, the HMIM-OR gate provides a desired output (1) for the set when either 1, 0 or 0, 1 is applied. The negative value of S-parameter (dB) gives a signal boosting to a greater extent, whereby the logical result comes true.

2. **Second case:**
   - o S-parameter (dB): −0.4888
   - o S-parameter (Mag) value: 0.94555
   - o Ohmic loss: value is not there (absent value)

In such instance, a missing value ought to be obtained for the ohmic losses exhibiting impracticality for making a full evaluation on performance.

3. **Third case:**
   - o S-parameter (dB): −4.2666
   - o S-parameter (Mag) value: 0.61222
   - o Ohmic losses: 0.49999

In such instance, it could be noted that the logic gate of the HMIM-OR type delivers a valid output (1) when either of the two input signals equals 1 (1, 0) or (0, 1). The ohmic losses, accordingly, are considered moderate. To put it differently, they have no affect on how the gate functions.

4. **Fourth Case:**
   - o S-parameter (dB): −1.566
   - o S-parameter (Mag) value: 0.82666
   - o Ohmic loss: 0.1999

In this instance, the HMIM-OR gate delivers an accurate output '1' for either of the two input signals being 1, that is (1, 0) or (0, 1). These are very pertinent values for the S-parameter (dB) and ohmic losses to produce this logical behavior.

The value of the intensity contrast ratio is 15; hence, this value implies that the gate contrasts the high and low well. The performance has been achieved by implementing an HMIM-OR gate that carries out the functions of logical OR with a high level of accuracy and efficiency using the photoelectric waveguide HIMI as the Table 2.

Table 2. Values of the logic gate of the OR-HMIM type operating at the 1550 nm wavelength

Input 1	Input 2	Out put	ohmic loss	S. parameter (Db)	S. parameter (Mag)
0	0	0	1.5777	−13.7	0.20666
1	0	1	-	−0.4888	0.94555
0	1	1	0.49111	−4.2666	0.61222
1	1	1	0.1999	−1.566	0.82666
INTENSITY CONTRAST RATIO–C.R					13

4.1 HMIM-NOR Gate - 1550 nm

This is a logic gate that is based on the technology of plasmonic waveguide, namely the HMIM. This type of logic gate is essential in conducting logic functions of the NOR nature.

Such logic gate heavily utilizes the process of interaction between two specific types of waves: plasmonic and photoelectric. The interaction occurs within the waveguide, and it is indispensable for harnessing forms of waves that are plasmonic as well as photoelectric constituting the signals of the input. Inside the waveguide, both forms of waves are initiated once the input is exerted on the logic gate of the HMIM-NOR type.

- **All signals are off (0, 0):** Either form of waves, plasmonic and photoelectric, are activated inside the waveguide. In such instance, the result will be in a plasmonic mode culminating in signal that the value 0.
- **One signal is off (0), and the other signal is on (1):** in such case, a signal with value 0 is produced due to the interference of both waves, plasmonic and photoelectric, constituting a situation of a photoelectric nature inside the guide.
- **Both signals on (1, 1):** in this case, the plasmonic and photoelectric forms of waves interacting creating a photoelectric situation inside the wave guide. As a result, a signal with value of 1 is obtained.

To summarize, an interaction ought to occur between two types of waves, plasmonic and photoelectric, for the purpose of generating modes of both plasmonic and photoelectric nature. To that end, the interaction has to happen inside the wave guide and the type of input signal paly indispensable role. Correspondingly, for obtaining the optimal performance, the logic gate at hand has been designed employing unique set of dimensions. They are: tm = 5 nm, ts = 5 nm, th = 5 nm, w = 20 nm, and L = 600 nm. This logic gate could perform efficiently by applying the aforementioned dimensions. Figure 5 illustrates the details explained above.

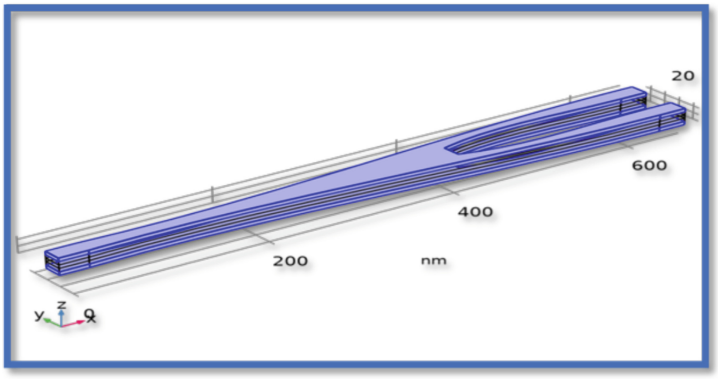


Fig. 5. Logic gate of the NOR-HMIM type

The first instance stands for efficient performance in which the S-parameter (dB) is −7.68, and the ohmic loss has the value of 0.88517. Drawing on the results shown in Table 3 below, this logic gate exhibits an efficient performance in which the contrast ratio has the value of 15 dB. Such value is considered preferable in comparison to the performance of existing logic gates of the same type. It is worth noting that such logic gate is essential to numerous applications that require a contrast ratio that is high in light, brightness, and signal intensity.

4.2 HMIM XNOR – 1550

The logic gate of the HMIM-XNOR type is designed and optimized employing various techniques for attaining efficient performance. Opposite arms are adopted for enhancing

Table 3. Performance values of the logic gate of the NOR-HMIM type when adopting a wavelength of a 1550 nm

Input 1	Input 2	Out put	ohmic loss	S. parameter (Mag)	S. parameter (dB)
0	0	1	0.88555	0.41222	−7.6888
1	0	0	-	0.23777	−12.4777
0	1(180)	0	1.4333	0.23888	−12.4666
1	1	0	2.6666	0.069777	−23.111
INTENSITY CONTRAST RATIO – C.R					15

optical interferometric efficiency. However, this could lead to increased loss due to radiation. For acquiring optimal performance, distinct dimensions have been selected in designing this logic gate. These are the dimensions: tm = 5 nm, ts = 5 nm, th = 5 nm, w = 20 nm, and L = 600 nm. It should be pointed out that a threshold with a specific decibel level is introduced, and a value that is not abide by the threshold level would be considered a 0-logic status which could not be enabled.

Figure 6 highlights the design of the logic gate of the HMIM-XNOR type adopting a wavelength of 1550 nm value.

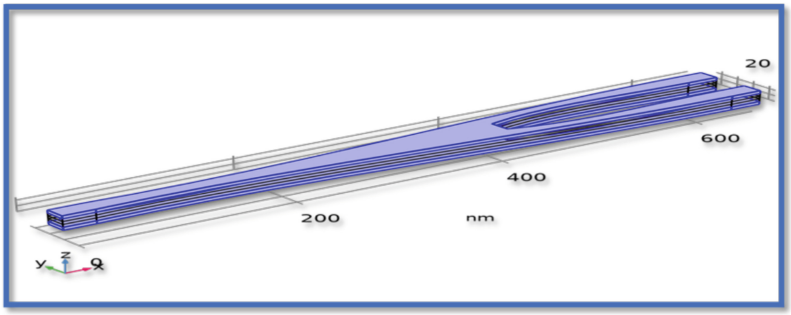


Fig. 6. The logic gate of the XNOR-HMIM type

The operation of the XNOR gate is as follows:

- **Matching signals (0, 0 or 1, 1):** XNOR logic gate generates a signal as an output that stands for the logic status of 1.
- **Different signals (0, 1 or 1, 0):** In contrast to the previous case, XNOR logic gate generates a signal as an output that stands for the logic status of 0.

In this paper, simulations and experiments have been conducted to substantiate the role of the waves of the photoelectric type within the suggested wave guides. Accordingly, the results confirm that the waves of the photoelectric type improve the contrast ratio of the XNOR logic gate. In general, the results of both simulations and experiments confirm that there is an improvement upon how the logic gate performs and how it can

interact with signals of high contrast. Moreover, the Ohmic losses have also been evaluated with regard to values of both input as well as output. In addition, the S-parameter analysis has also been adopted to equate the Ohmic losses. The results indicate that the Ohmic losses exhibit negative impact on the performance of the gate. In either case, the results confirm considerable enhancement when employing the photoelectric type of waves. Table 5 below highlights the values for the details explained above as the Table 4.

Table 4. Effect of the wavelength of 1550 nm on the NOR-HMIM logic gate

Input 1	Input 2	Out put	ohmic loss	S. parameter (Mag)	S. parameter (dB)
0	0	1	0.88555	0.41222	−7.6888
1	0	0	-	0.23777	−12.4777
0	1	0	1.4333	0.23888	−12.4666
1	1	1	0.012211	1.0101	0.0101-
INTENSITY CONTRAST RATIO - C.R					5

5 The Logic Gate of the HMIM-AND Type - 1550 nm

This logic gate utilizes both of the dielectric waves as well as the plasmonic waves in a plasmonic waveguide of the HMIM type for the purpose of conducing logic functions of the AND type. This logic gate utilizes the outcomes of the interaction between the magnetic waves and the interfaces of the materials that constitute the waveguide. Such interaction generates dielectric and plasmonic types of waves at the same time. On a general basis, the logic gate of the AND type requires two signals for generating one signal as an output.

For the purpose of enhancing the logic gate at hand, the researcher leveraged the technique of the opposite arms. Such technique is vital in increasing the efficiency of optical interferometry; nonetheless, the technique could boost losses due to radiation. It has to noted that the researcher selected unique dimensions in designing the logic gate at hand. These dimensions are tm = 5 nm, ts = 5 nm, th = 5 nm, w = 20 nm, and L = 410 nm. Consequently, the ohmic losses have been minimized which could aid in increasing the efficiency of the logic gate and lowering losses of power when the logic gate operates. S-parameter values are close to zero which indicates that the logic gate is stable, and it can resist changes in signal (Fig. 7).

The results, as shown in Table 5, indicate excellent performance with minor ohmic losses. The results also indicate that the S-parameter coefficient is near zero. This substantiate that there is an enhancement in the efficiency and stability of the logic gate. In other words, the logic gate could be ideal for digital and electronic circuit applications. The logic gate at hand shows relatively relabel performance when implementing logic functions of the AND type, with the HMIM plasmonic waveguide aiding in the improvement of the logic gate performance with reference to the S-parameter values and acceptable ohmic losses.

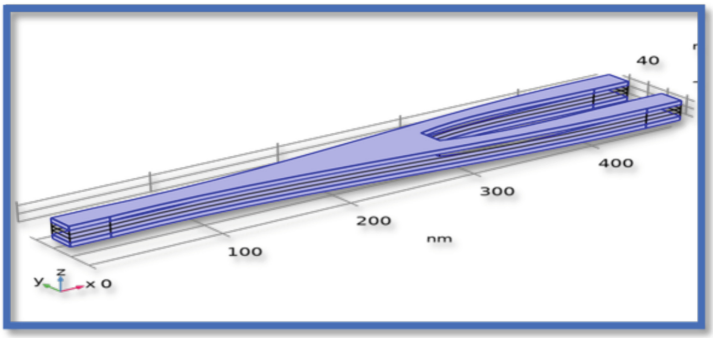


Fig. 7. A logic gate of the AND-HMIM type

Table 5. Performance Values of the logic gate of the AND-HMIM type employing a wavelength of 1550 nm

Input 1	Input 2	Out put	ohmic loss	S. parameter (dB)	S. parameter (Mag)
0	0	0	1.6444	−14.2626	0.193535
1	0	0	-	−17.8080	0.128787
0	1	0	2.0507	−17.8181	0.12882
1	1	1	0.82137	−7.1331	0.43921
INTENSITY CONTRAST RATIO –C. R					10

6 Conclusion

In this research, four novel designs of plasmonic waveguides have been introduced. The HMIM design has been among the introduced waveguides. It has been employed in the logic gate of the HIMI-XOR type, and its performance has been the optimal in comparison the other waveguide especially with regard to the significant reduction of the Ohmic losses. Based on the findings, the following conclusions can be drawn:

1. The lowest value of ohmic losses recorded was 0.49101 when using wavelengths of 1550 nm and 820 nm in the proposed structure. Such significant reduction of losses substantiates that the system performs highly effectively.
2. A disparity has been recorded with reference to the values of the contrast ratio as well as S-parameter. The disparity is highly likely due to minimizing the dimensions in HMIM design. The lowest value of the reflected signal has been observed within the logic gate of the XOR type, and it has been 33.9 dB.
3. The findings of this paper aid in overcoming most of the challenging issues identified in previous studies. In particular, the findings provide a solution for the issue of signal dispersion occurring at the curve of the arm. At which, the wavelength of a signal has to be lesser than half the value of the waveguide.

References

1. Kim, I., et al.: Nanophotonics for light detection and ranging technology. Nat. Nanotechnol. **16**(5), 508–524 (2021)
2. Ramakrishnan, M., Rajan, G., Semenova, Y., Farrell, G.: Overview of fiber optic sensor technologies for strain/temperature sensing applications in composite materials. Sensors **16**(1), 99 (2016)
3. McCray, W.P.: Will small be beautiful? Making policies for our nanotech future. Hist. Technol. **21**(2), 177–203 (2005)
4. Bursi, L., Calzolari, A., Corni, S., Molinari, E.: Light-induced field enhancement in nanoscale systems from first-principles: The case of polyacenes. ACS Photonics **1**(10), 1049–1058 (2014)
5. Makarov, S.V., et al.: Light-induced tuning and reconfiguration of nanophotonic structures. Laser Photonics Rev. **11**(5), 1700108 (2017)
6. Wang, L., Zeng, Y.P., Wang, Z.Y., Xia, X.P., Liang, Q.Q.: A refractive index sensor based on an analogy T shaped metal–insulator–metal waveguide. Optik **172**, 1199–1204 (2018)
7. Zhou, Z., Bai, B., Liu, L.: Silicon on-chip PDM and WDM technologies via plasmonics and subwavelength grating. IEEE J. Sel. Top. Quantum Electron. **25**(3), 1–13 (2018)
8. Kocabaş, ŞE., Veronis, G., Miller, D.A., Fan, S.: Modal analysis and coupling in metal-insulator-metal waveguides. Phys. Rev. B **79**(3), 035120 (2009)
9. Butt, M.A.: Metal-insulator-metal waveguide-based plasmonic sensors: Fantasy or truth—A critical review. Applied Research **2**(4), e202200099 (2023)
10. Akhavan, A., Ghafoorifard, H., Abdolhosseini, S., Habibiyan, H.: Metal–insulator–metal waveguide-coupled asymmetric resonators for sensing and slow light applications. IET Optoelectron. **12**(5), 220–227 (2018)
11. Ali, F.M., Abdullah, A.K., AbdulNabi, M.A.: Design and Simulation of Optical Logic Gates Based on (MIM) Plasmonic Waveguides and slot cavity resonator for Optical Communications. In: Journal of Physics: Conference Series, Vol. 1963, No. 1, p. 012152. IOP Publishing (2021)



Assessing the Effectiveness of Machine Learning Models in IoT Systems

Mahfuzul Huda[1(✉)] and Abdullah[2]

[1] Faculty of Engineering and Technology, Shubham University, Bhopal, M.P., India
mah.huda@gmail.com

[2] University Institute of Computing and Information Sciences, Chandigarh University, Unnao, India

Abstract. The term "Internet of things" (IoT) refers to a network of disparate devices. With the use of this technology, network devices can offer higher-quality services in the form of smart homes, cities, factories, etc. A subfield of computer science known as "machine learning" deals with a system's capacity to draw lessons from its past and use those lessons to predict future events. This study also includes a comparison of two machine learning methods for user authentication and prediction. By applying two different machine learning algorithms on a single dataset, the intended method was demonstrated. Using the Movie Star dataset, Convolutional Neural Networks (CNN) and Conv2D were implemented and evaluated. The application of various algorithms to enhance or assess the precision and speed of new or existing models will be the main focus of the research.

Keywords: IoT · CNN · Conv2D · Password-Based Authentication and GWN

1 Introduction

Since everything in the world will be controlled by the internet, internet-based services are available everywhere. This is the fundamental technology used to link several computers and gadgets. In a similar vein, the internet of things is currently a highly popular field in which it is applied. Through the networking of devices and non-IP components like televisions, fans, refrigerators, health care providers, and other network companies, this industry expands the use of the internet. Because of cyberattacks, web application security has grown increasingly complicated over time. It has been observed that IOT offers all societal segments and commercial business sectors a common degree of services as per Birhane et al.

As a result, information technology and electronic goods develop a solid partnership. In a similar vein, all electrical gadgets may now connect to the internet and interact thanks to processors. According to a survey, by 2020 there will be over 20 billion connected IoT devices, and a significant portion of the budget will go for hardware alone. Consequently, IoT serves as the foundation for both smart secure cities and smart homes. IoT devices are less secure from online threats as per Singh et al.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 130–136, 2025.
https://doi.org/10.1007/978-3-031-91008-1_12

The conventional notion of IoT networks today is linked to vast quantities of sensors and other networking devices, which provide a number of fundamental issues. The two primary concerns with the overall IoT architecture are privacy and access control. With three fundamental requirements—confidentiality, integrity, and availability—security and privacy are the most crucial aspects of the Internet of Things. IoT must comply with all of these security regulations. Another crucial difference between networking operations and the IOT working environment is the need for tighter security detection measures for these kinds of devices according to Ding et al.

As per the designs of IoT networks, authentication plays a crucial role in enabling communication and data sharing across all components. However, if no filter is used, network assaults can readily steal users' passwords according to the Otoom et al.

In order to authenticate users using an iris biometric, the research will employ machine learning. The system administrator and the system itself must be able to readily identify users and authenticate the permitted ones in order for this research to achieve the expectations utilizing machine learning models. In the example below, user authentication allows Gate Way Node (GWN) authentication in addition to sending a message across sensors. The three phases of identification, authorization, and authentication are maintained by IoT authentication systems, where sensors must register on the network and authenticate as per Javaid et al.

It is essential to comprehend the authentication procedure in order to concentrate on these concerns. Occasionally, nevertheless, users are unavailable to GWN for the purpose of transmitting authentication data. Consequently, sensor nodes are deployed remotely to authenticate the IoT network in order to tackle this issue. As per the designs of IoT networks, authentication plays a crucial role in enabling communication and data sharing across all components. If a filter isn't used, though, users' credentials could be easily obtained by network attacks and used against them according to the Jung et al.

This study will yield a thorough understanding of IoT authentication and its accessories. A defined taxonomy of assaults and their classification using appropriate technical methodologies will be presented. This study will also address IOT authentication techniques that are useful in reducing a variety of dangers. This article will conclude with an authentication technique, outstanding issues, and a proposal for future research.

2 IoT Methodologies for Authentication

In order to grant the appropriate access to the appropriate entity, authentication is the process of identifying and validating the identities of individuals or devices. Passwords are a widely used authentication method used at nearly all access points. It needed a special combination of characters, numbers, or words entered by the user or device. When a user tries to enter the system, the system verifies the input they provide with the data that is kept in its database, which contains their ID and username. A closer look at the IoT authentication techniques is provided in the following figure, which was provided by Sapkal et al. (Fig. 1)

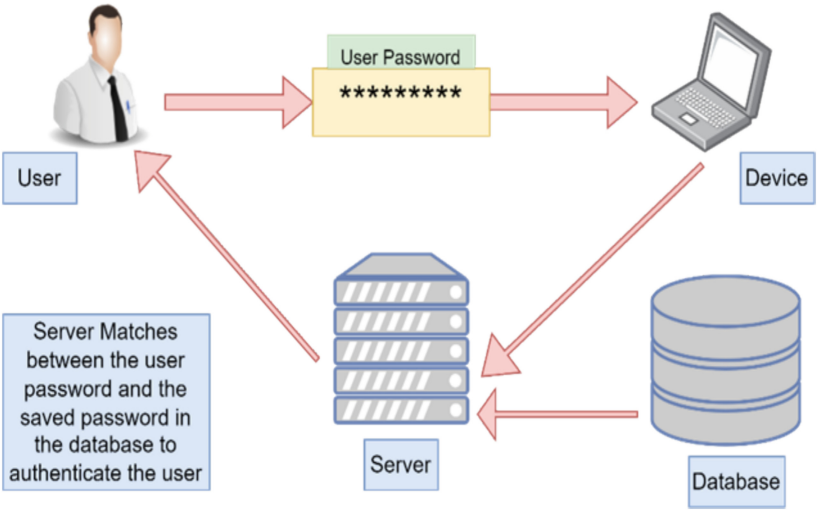


Fig. 1. Password Authentication process.

3 Factors Based Authentication

Declared that there are two types of factor-based authentication: soft and hard. Soft factor-based authentication works by having the communication media ask a server for a communication channel. The server then generates an OTP (one-time password) and delivers it to the communication media. In order to approve or reject access to an entity, a server eventually compares an OTP input from a user with the one it originally requested. Conversely, hard factor-based authentication refers to the process of identifying individuals via a small device or card. Additionally, the system combines the information on the card with data saved on the server in order to employ this strategy correctly. A soft factor-based authentication system is depicted in the figure below (Fig. 2).

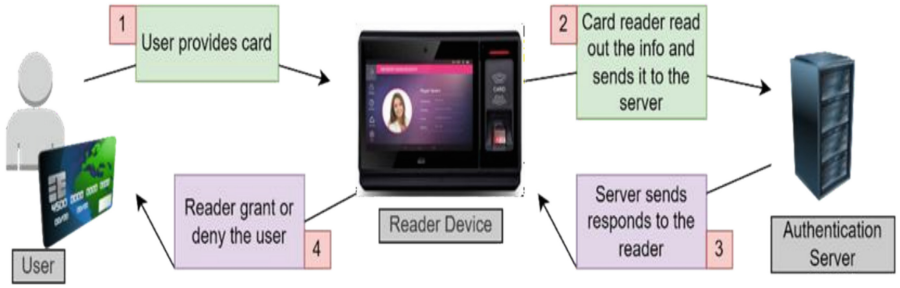


Fig. 2. The authentication process of a smart card

4 Biometric-Oriented Verification

Using a person's fingerprint, face, iris, or other biometric, biometric authentication is possible. The particular biometric scanner obtains individual biological data from the user and compares it with recorded data obtained during the registration procedure. For instance, Iris authentication techniques identify persons based on mathematical patterns proposed by the Ramallo et al. (Fig. 3)

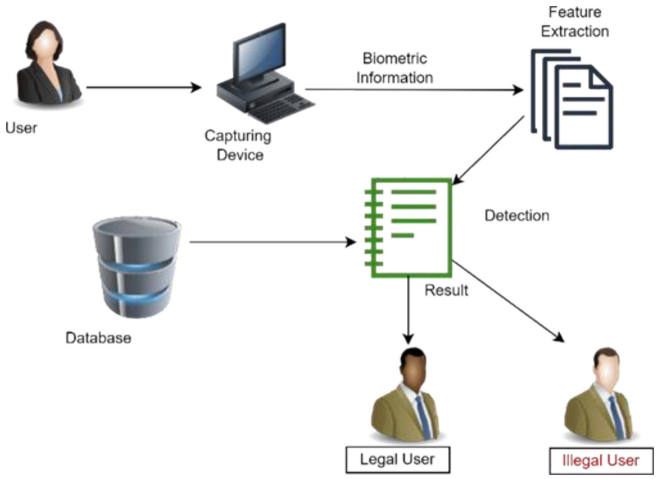


Fig. 3. Authentication Process of Biometric Mechanism

5 Verification Using Cryptography

Cryptographic authentication, or key-based authentication, is the act of establishing one's identity through a challenge-response handshake using cryptographic keys. Here's an illustration of what you own. Every organizational setting already makes extensive use of key-based authentication. For secure shell key management and authentication in protocols like TLS, SSH, and remote desktop (RDP), cryptographic keys are employed by Bhatia et al

6 Multi-Factor Authentication (MFA)

An application, an online account, or a VPN can only be accessed with the use of two or more verification factors, or MFA, as an authentication mechanism. Multifactor authentication is a requirement of a robust identity and access management (IAM) policy (MFA). In addition to a login and password, MFA requires one or more additional verification criteria, which lowers the likelihood of a successful cyberattack by Singh et al.

7 Convolutional Neural Network (CNN)

Convolutional neural networks, or CNNs for short, are a type of artificial neural network used for object and picture classification and recognition. Deep Learning identifies objects in an image by using a CNN. CNNs are utilized for many different tasks and applications, such as speech recognition in natural language processing, video analysis, obstacle detection in self-driving cars, image processing, and computer vision tasks like segmentation and localization. CNNs are especially well- liked in the Deep Learning space because of their significant contribution to these quickly developing and expanding domains as per Khan et al. Given that it does not take into account all input nodes to influence all output nodes, CNN was selected with the idea that it would work well with this kind of dataset.

8 Conv2D

2D convolution's class Conv2D layer (e.g. spatial convolution over pictures). By convolving the layer input with a convolution kernel, this layer produces a tensor of outputs. Unlike a densely connected network, where models learn each pattern repeatedly, the CNN uses Conv2D units to recognize and process the pixels of the image by recognizing the spatial patterns in the pictures. These patterns can then be relocated in any part of the same image or other images without the CNN model having to make an effort to recognize and learn those patterns again. For high accuracy in image recognition applications, the Conv2D is used (Olaofe, Z). Conv2D's effective image recognition is one of the main justifications for its use in this investigation by Alhasan et al. authentication.

9 Implementation

This study will present the test that was created with several different algorithms. It will show the output of each algorithm. Determining the correctness of each model and comparing the outcomes is what contributes most in this case. This study will use the faces of movie stars to investigate human facial recognition. The purpose of this exam is to determine how models work efficiently to produce results that are more accurate. In this test, two algorithms are used: Conv2D and Convolutional Neural Network (CNN).

9.1 Result Measurements

This section contains a discussion of the experiment results. A range of criteria were used to evaluate the effectiveness and accuracy of machine learning in classifying data sets. In this study, 20% were utilized for testing and 80% were used for training the model. Four measurements will be made during the examination, as seen below.

Precision	= TP /(TP + FP)
Recall	= TP /(TP + FN)
Accuracy	= (TP + TN)/(TP + FP + TN + FN)
F1 Score	= (2 * (Precision * Recall))/((Precision + Recall))

9.1.1 Precision

The precision of a machine learning model refers to the degree of accuracy in its positive predictions. Precision is defined as the number of true positives plus the number of false positives, divided by the total number of positive predictions.

9.1.2 Recall

In machine learning, a recall is a model's capacity to find every pertinent case in a set of data. The number of accurate positive predictions produced out of all potential positive predictions is called the recall. Recall highlights the instances in which positive predictions were overlooked, as contrast to accuracy, which only addresses the accurate positive predictions among all positive predictions.

9.1.3 Accuracy

Based on the input, or training data, a statistic that shows which model is more adept at detecting correlations and trends between variables in a dataset. A model's capacity to provide forecasts and ideas increases with its ability to generalize to previously unidentified data, hence increasing its market worth.

9.1.4 F1 Score

One of the most important evaluation metrics in machine learning is the FI-score. It combines precision and recall, two previously incompatible measures, to elegantly summarize a model's predictive efficacy.

10 Conclusion

Internet-based services are accessible everywhere since the internet will control everything in the planet. This is the most basic way to connect many computers and gadgets to one another. In other areas as well, the internet of things is growing in popularity. Through networking devices and non-IP components such televisions, fans, refrigerators, health, and other network enterprises, this industry increases the usage of the internet. Web application security has grown more difficult over time as a result of cyberattacks. It has been noted that IOT offers all facets of industry and society a uniform level of service. Consequently, information technology and electronic devices are closely related. In a similar vein, processors enable all electrical devices to connect to the internet and communicate.

By using this technique, network devices can provide higher-quality services, such as those found in smart homes, smart cities, or smart industries. In computer science, machine learning is the study of a system's capacity to draw lessons from its past and use those lessons to forecast future occurrences. A person wishing to authenticate himself in order to access a facility or system can utilize a range of machine learning algorithms. Machine learning algorithms are able to recognize systems or users that are at risk of being accessed without authorization. A comparison of two machine learning

techniques for user prediction and authentication is also included in this paper. Conv2D and Convolutional Neural Networks (CNNs) were employed in this study's experiment.

Google Colab were used for the examination. It appears from experiments that the method can increase the accuracy of recognition. The application of various algorithms to improve or assess the precision and speed of the new model or the current ones is the research's next focus. To get a more accurate result, the experiment conducted on the machine learning classifier mentioned above might be expanded to another.

References

1. Birhane, M., et al.: COVID-19 Vaccine Breakthrough Infections Reported to CDC—United States. Morb. Mortal. Wkly. Rep. **70**, 792–793 (2021). [Google Scholar]
2. Singh, R.P., Javaid, M., Haleem, A., Suman, R.: Internet of things (IoT) applications to fight against COVID-19 pandemic. Diabetes Metab. Syndr. Clin. Res. Rev. **14**, 521–524 (2020). [Google Scholar] [CrossRef]
3. Ding, W., Levine, R., Lin, C., Xie, W.: Corporate immunity to the COVID-19 pandemic. J. Financ. Econ. **141**, 802–830 (2021). [Google Scholar] [CrossRef]
4. He, W., Zhang, Z.J., Li, W.: Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic. Int. J. Inf. Manag. **57**, 102287 (2021). [Google Scholar] [CrossRef] [PubMed]
5. Otoom, M., Otoum, N., Alzubaidi, M.A., Etoom, Y., Banihani, R.: An IoT-based framework for early identification and monitoring of COVID-19 cases. Biomed. Signal Process. Control **62**, 102149 (2020). [Google Scholar] [CrossRef] [PubMed]
6. Javaid, M., Khan, I.H.: Internet of Things (IoT) enabled healthcare helps to take the challenges of COVID-19 Pandemic. J. Oral Biol. Craniofac. Res. **11**, 209–214 (2021). [Google Scholar] [CrossRef] [PubMed]
7. Jung, Y., Agulto, R.: A public platform for virtual IoT-based monitoring and tracking of COVID-19. Electronics **10**, 12 (2021). [Google Scholar] [CrossRef]
8. Mukherjee, R., et al.: IoT-cloud based healthcare model for COVID-19 detection: An enhanced k-Nearest Neighbour classifier based approach. Computing, 1–21 (2021). [Google Scholar] [CrossRef]
9. Sapkal, G., et al.: Neutralization of Delta variant with sera of Covishield vaccinees and COVID-19 recovered vaccinated individuals. bioRxiv (2021). [Google Scholar] [CrossRef]
10. Ramallo-González, A.P., González-Vidal, A., Skarmeta, A.F.: CIoTVID: Towards an Open IoT-Platform for Infective Pandemic Diseases such as COVID-19. Sensors **21**, 484 (2021)
11. Bhatia, M., Kaur, S., Sood, S.K.: IoT-inspired smart toilet system for home-based urine infection prediction. ACM Trans. Comput. Healthc. **1**, 1–25 (2020). [Google Scholar] [CrossRef]
12. Singh, V., et al.: IoT-Q-Band: A low cost internet of things based wearable band to detect and track absconding COVID-19 quarantine subjects. EAI Endorsed Trans. Internet Things, 6 (2020). [Google Scholar] [CrossRef] [Green Version]
13. Khan, P.I., Razzak, I., Dengel, A., Ahmed, S.: Understanding information spreading mechanisms during COVID-19 pandemic by analyzing the impact of tweet text and user 14. Features for Retweet Prediction (2021). arXiv:2106.07344. [Google Scholar]
14. Qayyum, A., Razzak, I., Tanveer, M., Kumar, A.: Depth-wise dense neural network for automatic COVID19 infection detection and diagnosis. Ann. Oper. Res. 1–21 (2021)
15. Alhasan, A., et al.: A case- study to examine doctors' intentions to use IoT healthcare devices in Iraq during COVID-19 pandemic. Int. J. Pervasive Comput. Commun. (2020)

Blockchain-Assisted Dynamic Attack Detection Method Based Secure Data Management in Industrial 4.0

D. Padmapriya[1], J. Kamalakumari[2], Ahmed J. Obaid[3], P. Tamilarasi[4], D. Balaganesh[5(✉)], and K. Madhumathi[6]

[1] Department of Computer Science, Saveetha College of Liberal Arts and Sciences, Saveetha Institute of Medical and Technical Sciences, Chennai, India
padmapriyad.sclas@saveetha.com

[2] Department of Computer Application, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India
kamalakj@srmist.edu.in

[3] Faculty of Computer Science and Mathematics, University of Kufa, Najaf 54001, Kufa, Iraq
ahmedj.aljanaby@uokufa.edu.iq

[4] Department of Computer Applications, Bharathiar University, Coimbatore, India

[5] Berlin School of Business and Innovation GmbH, Karl-Marx-Straße 97-99, 12043 Berlin, Germany
duraisamy.balaganesh@berlinsbi.com

[6] Department of Computer Science, Anna Adarsh College for Women Annanagar, Chennai 600 040, India

Abstract. Internet of Things (IoT) edge sensors and the data they collect are crucial to modern business systems. Such cloud systems achieve the optimal execution of dynamic tasks by integrating remote resources. The money and lives of industry owners are at stake when hackers compromise data or forge source devices after introducing advanced persistent threats (APT). Many problems exist, such as advanced persistent threats (APTs) that inject malicious code into susceptible edge devices, unsafe data transfer, inconsistent trust across stakeholders, non-compliant data storage methods, etc. Hence, this paper proposes the **Blockchain-assisted Dynamic Attack Detection Method (BCDADM)** for administering inbound and outbound security in data acquisition and dissemination. Integrating end-to-end authentication using blockchain data on reputation and sequence discrimination is a security mechanism for outbound communication. The blockchain paradigm governs data collection and dissemination via processing terminal and industry-wide integrity verification and categorization. The suggested method is to apply the key aspects of the deep transfer learning (DTL) algorithm to the ResNet model. After the APT filtering at the edge is successful, the data is sent to the DHT that is linked with it. The registration, authentication, and validation of IoT sensors are guaranteed by the Consortium Blockchain (CBC) network. Data and APT detection transactions are recorded on the immutable ledger. According to the findings of the experiments, the suggested design outperforms the conventional one in terms of privacy and security.

Keywords: Blockchain · Cloud · IoT · deep transfer learning (DTL)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 137–148, 2025.
https://doi.org/10.1007/978-3-031-91008-1_13

1 Introduction

An emerging trend in manufacturing, the Industrial Internet of Things (IIoT) integrates ICT into processing industries to improve production reliability. The smart industries have embraced automation and self-sufficient processing and computing capabilities with the assistance of the IoT and intelligent computing [1]. In the traditional model of industrial processing, various operations supporting production and customer replies are carried out by the field layer up to the management layer [2]. To meet the increasing needs of users and the increasing requirement for productivity, industries must work faster and more efficiently [3]. The ubiquitous cloud environment makes delivering infrastructure and applications as services possible. Many intelligent systems and communication forms allow such a diversified platform to improve customer service [4, 5]. Sharing information digitally across several terminals and customers is essential to smart businesses [6]. Applications used in industry transmit large amounts of data at every stage of their design, necessitating stringent safety protocols. Data quantity and quality are reduced when inbound and outgoing threats from the smart industrial environment and the IoT platform are considered [8]. Different levels of the architecture have to be responsible for administering security in IIoT, in contrast to traditional authentication methods. On top of using trust models and end-to-end authentication, security is managed in a distributed and scalable way.

To conduct mining and linking operations, distributed systems need a protocol called a "blockchain," which consists of a network of verified and unchangeable links. Various systems receive environmental information in blocks and then share it for distributed access and sharing. Regarding the smart industry and IoT platforms, the calculable aspects that govern device behaviour are authentication, trust, and reputation. Blockchain technology makes tracking and saving this data for later use possible. Smart and deep transfer learning techniques are joining blockchain technology in analyzing the behaviour and condition of connecting devices. For blockchain to work, the results of analyses conducted using AI and ML techniques to identify the types of interacting devices are crucial. This technology is integrated into any application that uses cloud-based data exchange.

The main contribution of this paper:

- Designing the proposed BCDADM for managing data acquisition and dissemination security, including incoming and outgoing.
- The proposed method ensures the safety of outbound communication by using end-to-end authentication and blockchain data on reputation and sequence discrimination.
- The numerical results have been performed, and the proposed method achieves high data security and management compared to other methods.

2 Related Works

Data suggested for use after blockchain verification is the Blockchain and Digital Twin-Based Heuristic Multi-Cooperation Scheduling Framework (BC-DT-HM-CSF) [11]. Hence, the procedure only transmits result reports to prevent the frequent transfer of sensitive data. According to the simulation findings, the suggested authentication method

is faster than the traditional protocol. Furthermore, BC-DT-HM-CSF utilizes the PDQN DRL model, which exhibits superior precision, stability, and dependability.

An ideal answer to the problem of massive data integrity may be found in the trusted consortium blockchain (TCB) architecture, which employs the hyperledger fabric modular (HFM) for security and integrity verification [12]. To ensure high transaction throughput and low latency of HFM contents, the TCB uses trustworthiness in heterogeneous IIoT networks regulating end-point peers to accomplish robust data integrity.

Protecting Industrial IoT against assaults of all kinds using a deep learning-based intrusion detection system (DL-IDA) [13].To improve the IDS's detection effectiveness, the suggested mode applied the feature engineering approach known as singular value decomposition (SVD). For an unbalanced dataset, we used the synthetic minority over-sampling (SMOTE) technique to avoid over-fitting and under-fitting, two potential sources of biased classification.

An ideal RMC-CNN model for energy efficiency and security in industrial IoT based on deep learning (DLEFO-RMC-CNN) [14]. The key generation process uses a dynamic honeypot encryption algorithm to encrypt the data. Data is safely sent and kept in the IoT cloud, which may be decrypted at user request.

A blockchain-based interactive method (BC-IA) for systems integration in manufacturing [15]. Blockchain technology offers a solution for data interchange that might alleviate strain on business cloud services. Implementing a blockchain-based system may greatly enhance the efficiency of data interactions via a discreet organizational structure. The healthcare industry has provided a clear description of the data security that is associated with blockchain technology. We were also able to prepare this article with the assistance of the research papers [17–20] that were presented in the previous proceedings.

3 Proposed Methodology

Therefore, the BCDADM is suggested as a means of controlling data capture and dissemination security both incoming and outgoing in this study. An approach to safeguarding outbound communication is the integration of end-to-end authentication using blockchain data on reputation and sequence discrimination. When it comes to processing terminal data gathering, distribution, and integrity verification and classification across industries, the blockchain paradigm is in charge. One approach is to optimize the ResNet model using the essential features of the deep transfer learning (DTL) technique. Successful completion of APT filtering at the edge triggers data transmission to the associated DHT. To ensure that Internet of Things (IoT) sensors are legitimate, the Consortium Blockchain (CBC) system verifies and authenticates them. An immutable ledger records data and transactions related to APT detection.

Figure 1 shows the proposed IIoT data management system's design. It consists of four primary parts: a platform for exchanging metadata based on blockchain technology, data storage via IPFS, a supplier of IIoT data, and a consumer of IIoT data. The Industrial Internet of Things (IIoT) devices and applicable data handling units are known as data providers in the production system. Information infrastructure as a service (IIoT) devices provide their raw data to a linked handling unit, which could be a regular computer, a local

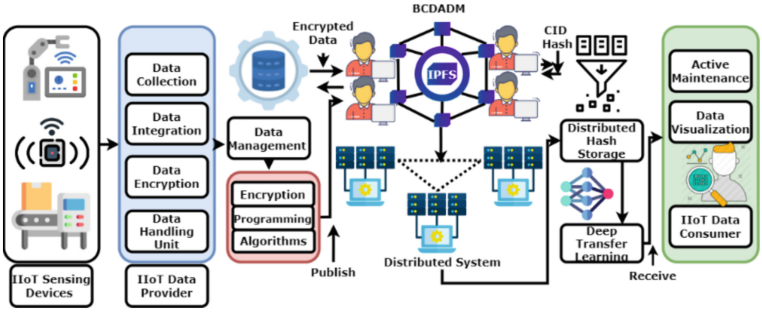


Fig. 1. Proposed Work

server, or even a single-board computer. Before bulk uploading to IPFS, the handling units gather and combine the raw data. It is possible to encrypt data before uploading it, depending on privacy by design. A cryptographic hash is created as the Content Identifier (CID) when the material is saved in the IPFS network; this hash may be used to retrieve the submitted data. The CID is encoded and encrypted by the handling unit, together with additional metadata, once it has been received. This creates a transaction, which is then communicated to the data-sharing platform. This solution's primary selling point addresses the two biggest problems with earlier blockchains—its inability to scale and high transaction costs. Any interested party may search or be suggested transactions listed on the Tangle. The degree to which a transaction's contents are protected by encryption may vary. Only recipients in possession of verified decryption keys will be able to access encrypted information.

Here is a three-step process for the suggested protection program. The first stage is deploying a deep transfer learning model within the edge server. The model is settled in the edge server after training on two merged and preprocessed datasets. Upon receiving a request from the edge server, it verifies the data for advanced persistent threats. Secondly, the associated DHT receives data from the sensors and a history of detections. It must verify that no advanced persistent threats (APTs) were introduced during data transmission across the network before storing the data. Here, a blockchain consortium oversees the procedure to ensure that no untrusted devices transmit data. Finally, blockchain smart contracts save data to DHT storage and record transactions into the shared ledger. Each of them is briefly shown in the captions. The content of the transaction is decoded and, if necessary, decrypted by IIoT data consumers. They may access the IPFS data by following the CID in the content. Based on the privacy setting, further decryption may be necessary.

Figure 2 deliberates the deep transfer learning-based knowledge transfer. By storing and transferring information learned from addressing one issue to another, deep transfer learning (DTL) converges; the proposed BCDADM model trained to identify intrusions might benefit from knowledge learned to detect malware. To make a decision prediction in tandem with another model doing a separate job, as shown in Fig. 2, the BCDADM model shares or reuses its information. Terms like "domains" and "tasks" describe deep transfer learning (DTL). Assume that $X = \{y_1, ..., y_m\} \in X$ and that $Q(y)$ is a conditional probability distribution. Then, the domain C is composed of these two elements. A job

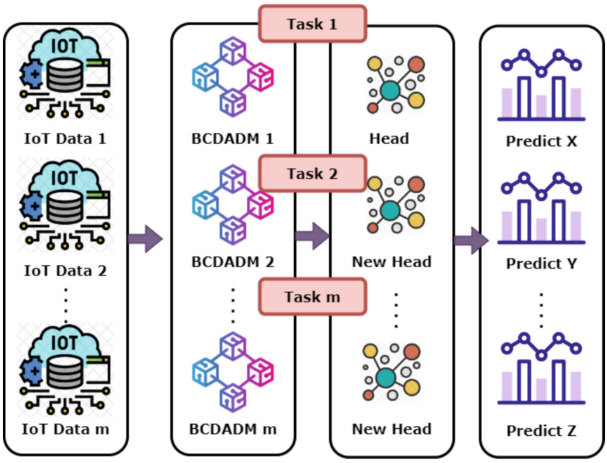


Fig. 2. Deep Transfer Learning-based Knowledge Transfer

with two items is represented by the domain $C = \{X, P(X)\}$. There is a label space X and an objective predictive function $e : X \rightarrow Y$. The function predicts the label $e(y)$ for an instance y in the label space. This task, represent ed by $s = \{x, e(y)\}$, from the training dataset, which contains pairs $\{x_j, y_j\}$, where y_j is an element of y and x_j is an element of X. If $C_t \neq C_s$ OR $\urcorner_t \neq \urcorner_s$ then the input domain C_t and the training task $\urcorner_t$ are equivalent, and the output domain C_s is defined. Utilizing the information in $\urcorner_s$ and C_s, DTL enhances the learning process of the target prediction function $e_s(.)$ in DT. Storage of data from edge sensors also necessitates visual representations.

Figure 3 demonstrates the detection of DTL-based APT. The proposed BCDADM-based model for APT Detection consists mainly of two components, as shown in Fig. 3: the first is the portion that trains the model, and the final is the part that detects intrusions. Following the network data preparation, we have included it in our suggested model. Afterwards, we will conduct empirical trials to find the most important model parameters. The best intrusion detection model for diverse Internet of Things (IoT) applications will be chosen based on its best forecasting performance on the training set. The trained DTL model used a randomly chosen training dataset and verified it using a validation dataset about the intrusion detection portion. Using discrete-type parameters, we compare the models' detection ability. The final detection model was chosen for heterogeneous Internet of Things applications based on best performance. Conv1D, a one-dimensional Fully Convolutional Neural Network (FCN), is the network architecture we've chosen for the DTL technique. The suggested DTL model's design in Fig. 3. The network's input has the same form. The first, second, and third layers use the one-dimensional convolution layer. Layer one consists of 128 filters with an 8-layer kernel, layer two of 256 filters with a 5-layer kernel, and layer three of 128 filters with a 3-layer kernel. The third one-dimensional convolution layer uses the Rectified Linear-Unit (ReLU) activation function. A BatchNormalization() operation follows each one-dimensional convolution layer. The stride of the sum of these three convolution layers is 1. To ensure the best performance, the method repeats twice for block two and block-3, respectively. To create

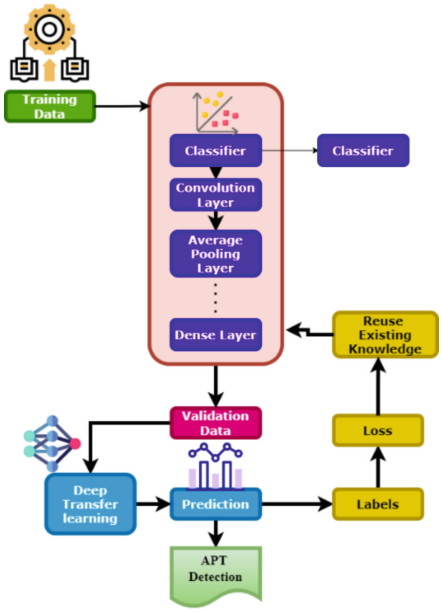


Fig. 3. DTL based APT Detection

a multivariate series with dimensions determined by the number of filters in each layer, each block takes the outputs of the preceding block as input and applies certain non-linearities to them. Taking the third block's input and averaging each series, the fourth layer combines a GlobalAveragePooling1D() process. This method drastically reduces the number of parameters needed for a deep model by using a class activation map to interpret the learned features. The output of the gap layer is then passed to softmax classification layers whose number of neurons equals the total number of classes in the dataset. The purpose of excluding other hyper-parameters and data correlation is to keep the study brief. This made our ability to determine the impact of deep transfer learning on APT detection possible. However, when APT detection is done at the edge server, it's encrypted so it can be sent via the consortium (CBC) blockchain during data transmission. Assume that $\urcorner_t$ represents a detection status and $\urcorner_s$ stands for a data transaction. All of this will be documented in the BCL, or blockchain ledger. The CBC functions as key generating and distributing (KGD) to facilitate communication between edge devices and blockchain peers. Algorithm 1 discusses secure data transmission and store.

Algorithm 1: Secure Data Transmission and Store

Input: S_y represents IIoT data Transactions
K examines the access control lists
δ deliberates the signature of the S_y
ID_i explores the ith number of IIoT devices identities
X express the system parameters
PK express the private key

Output: U_{j_c}, U_{t_y}, t set & return verification sorting flag true

Create:(ID, K, δ, S_y)
Sign(S_y, PK)
Cast (S_y, δ)
For $S_y \leftarrow S_{y_j}$
do
$U_1 \leftarrow verification\ (ID, L, X)$
$U_2 \leftarrow verification\ (ID, L, X)$

if $(U_1 \| U_2)$then
$t \leftarrow store\ DHT(S_y, ID)$
end
end

Over the BC network, the OSN's Gossip protocol disseminates ledger updates. Accordingly, the pointer is committed to memory in the ledger, but the data address is safely kept in the offline or online DHT data repository on IPFS or HL CouchDB. In this case, the signature method may be shown as a series of three or four quadruple-tuples of probabilistic polynomial-time algorithms, where H stands for generation, T for signing, U for verification, K for key distribution, F for encryption, and C for decryption. In addition to the identities IDj, the devices in this case need the Access Control List (ACL) before creating and signing Transaction S_y. . The creation of the ACl list (k), production of signatures (δ), and publication of transactions S_y are entirely responsible for the industry 4.0 devices and the Edge Gateway. Nevertheless, to access data later, the same K will be necessary. As seen in algorithm 1, upon successful execution, it sets three distinct flags (U_1, U_2, T). U_1 : *is true* if the identities are associated with the generated public keys, and U_2 : *is true* if the certificate-less signature satisfies the earlier-mentioned criteria.

The peers on the Blockchain respond to the receipt by verifying the transaction S_y. . In the event of data access, the interchangeable verification method is effective. Similarly, the third flag is set to true (t) once data is written to the DHT. Finally, the S_y Pointer S_q The rest of the ledger is updated whenever a new block is added to the blockchain.

4 Results and Discussion

This research recommends that the BCDADM regulate data collection and dissemination security during transmission and reception. One way to secure outbound communication is to integrate end-to-end authentication with blockchain data on popularity and sequence discrimination. Data processing, dissemination, integrity verification, and categorization at the processing terminal are all areas where the blockchain paradigm leads the way. One strategy is improving the ResNet model by incorporating key aspects of the deep transfer learning (DTL) method. Data transfer to the corresponding DHT is initiated after APT filtering at the edge. The Consortium Blockchain (CBC) technology certifies and validates IoT sensors to ensure they are genuine. Information and transactions about APT detection are recorded in an immutable ledger. This study uses the public Kaggle dataset: https://www.kaggle.com/datasets/munaalhawawreh/xiiotid-iiot-intrusion-dataset [16].

4.1 Response Rate (%)

In the industrial setting, the response rate is determined by dividing the total number of transactions $(mor(m-n))$ by the total number of transactions (m). If S_n is true, then $f_s \rightarrow 0$, according to the deep transfer learning analysis using B and E_s therefore the answer is always an integer between $1 and m$, reaching a maximum level. On the other hand, because of data forging from the field sensors, the X solutions in (4b) and (4b) coexist. Finding $(m-n) \in m$ is the main issue if the answers are categorized as x. To find $(m-n)$ devices in the $B = 1$ and S_n categories, the recurrent analysis conditions are adjusted as $\neg d_q(m-n)d_q$ by watching a decrease in t.

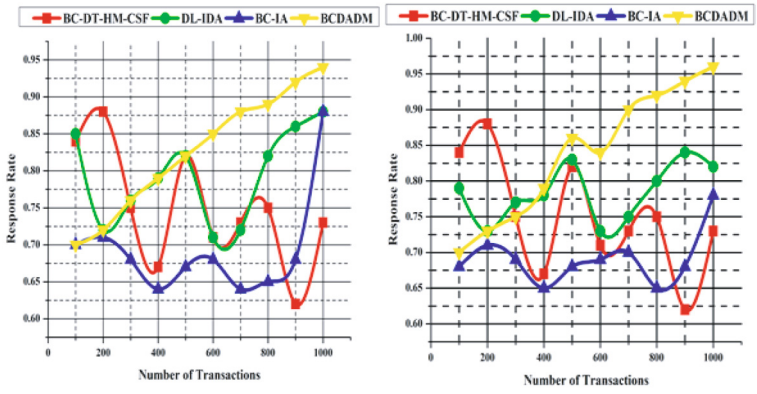


Fig. 4. Response Rate

Figure 4a and b deliberate response rate. The new sequence δ is given to the recognized sensors, which is then confirmed at the receiving end and shared with the industry blockchain. The receiving sequence and dispersed transactions may be checked for

equality by exchanging information. Using O_s and other recurrent analyses, the suggested model can retrieve $(m - n)$ instances from the adversary/forged sequences. The procedure can reply to the greatest number of requests, which helps ensure its effective delivery. Figure 4a shows the results of a comparison study for several transactions with a failure rate of 0.05 and 0.07. Similarly, Fig. 4b shows the response rate for different process ratios and variables. The results show that the suggested model is trustworthy for the processes and transactions.

4.2 Latency Ratio (%)

The smart industry's transmission times $S + S_s$ where S_s how the suggested model calculates the time latency. This time is spent following the classification in (4a) and the subsequent distributions in (4b). The class uses concurrent analysis and transmissions therefore the feasible latency is $\frac{S+S_s}{t \in M}$. On the other hand, the actual time delay experienced is $\frac{S+S_s}{t \in M} + \frac{S+S_s}{(m-n)}$ since the number of spreading sequences, T *and* δ, are different. For sensor instances of s and not S, specifically the constraint $\neg d_q(m - n)$, the metric S is calculated. Only cases where $\neg d_q$ satisfies S are taken into consideration for collection and distribution.

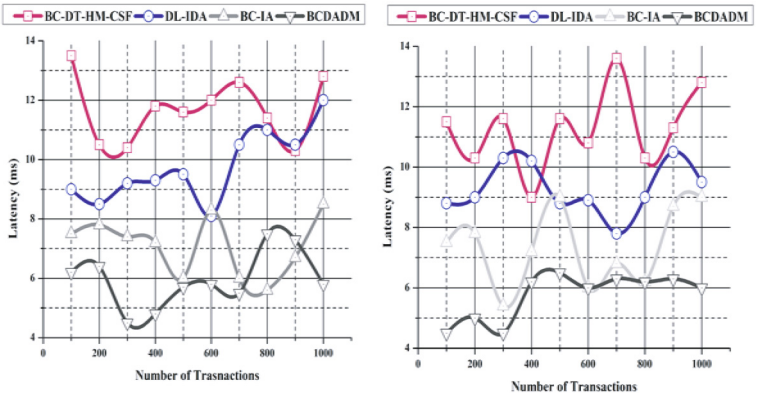


Fig. 5. Latency

Figure 5a and b shows a comparison of the latencies experienced by different types of transactions when FAP is present. When $S = 0$, a minor increase in latency is noted, as in transactions = 400, 600, and 900, but in other circumstances, some occurrences follow S and $(m - n)$ is unnecessary. Furthermore, unlike other approaches, the transactions are not re-initiated due to lost, inaccurate, or fabricated data answers. Therefore, this suggested approach limits the time for retransmission or extended gathering sessions. The comparison shows that the suggested model achieves a 3.12% decrease in FAP (with a response rate of 0.95), a 6.63% increase in response rate (with a failure rate of 0.06), and an 11.91% decrease in delay (with a False alarm progression (FAP) % of 2).

4.3 Computation Time (%)

Optimizing blockchain-based secure data management systems for Industry 4.0 may reduce computation time while improving efficiency and security. By doing away with energy-intensive mining and simplifying validation, efficient consensus mechanisms such as Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) drastically decrease computational overhead when compared to traditional Proof of Work (PoW). Off-chain solutions like state channels and sidechains conduct transactions and computational duties outside to reduce the main blockchain's burden further. This speeds up processing times and ensures data integrity via smart contracts and periodical anchoring. Another way to improve performance is by using batch processing methods. These approaches aggregate many transactions into one batch and minimize the frequency of blockchain visits.

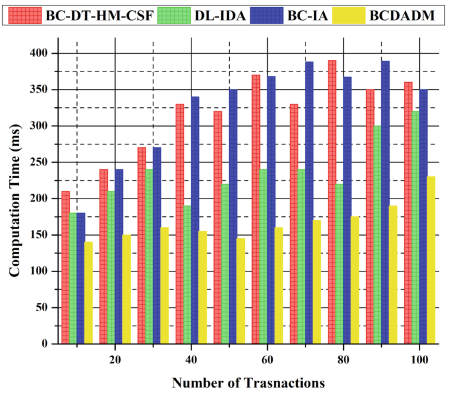


Fig. 6. Computation Time

Figure 6 shows the computation time. Further data management optimisation may be achieved via caching, index storage, and data compression. These techniques expedite data retrieval and transmission while maintaining security, allowing for the effective processing of massive data volumes. Symmetric encryption is popular because it quickly encrypts and decrypts data without sacrificing speed, thanks to its high computational efficiency. By dividing the computational burden and processing data closer to its source, distributed and parallel processing techniques like edge computing and parallel processing among several nodes increase processing rates and decrease latency. Finally, security risks may be quickly and effectively discovered without a large computational strain using lightweight machine-learning models for real-time monitoring and anomaly detection. These solutions, when combined, provide a strong foundation for the safe and efficient management of industrial data in a blockchain setting, allowing us to fulfil the demanding requirements of Industry 4.0 without exposing ourselves to unnecessary risks.

5 Conclusion and Future Work

Effective APT detection at the network's periphery and transparent recording of detection history in an immutable blockchain ledger are some of the features discussed in these papers. This model is responsible for managing the security of data capture and dissemination, both incoming and outgoing. The incoming data is first categorized using recurrent learning to identify harmful data dissemination patterns. The end-to-end authentication uses sequence distinction and blockchain reputation data for the outgoing security measure. By eliminating the need for certificates, the certificates data transfer method increases confidence between partners and guarantees a cost-effective and long-term solution. The experimental results show that the proposed method achieves a high response rate of 0.96, a latency of 6ms, and a computation time of 230s compared to other methods.

References

1. Khan, S.I., et al.: Implementation of cloud based IoT technology in manufacturing industry for smart control of manufacturing process. Int. J. Interactive Design and Manufact. (IJIDeM), 1–13 (2023)
2. Caiazzo, B., Murino, T., Petrillo, A., Piccirillo, G., Santini, S.: An IoT-based and cloud-assisted AI-driven monitoring platform for smart manufacturing: design architecture and experimental validation. J. Manuf. Technol. Manag. **34**(4), 507–534 (2023)
3. Atieh, A.M., Cooke, K.O., Osiyevskyy, O.: The role of intelligent manufacturing systems in the implementation of Industry 4.0 by small and medium enterprises in developing countries. Engineering Reports **5**(3), e12578 (2023)
4. Li, K., Zhang, Y., Huang, Y., Tian, Z., Sang, Z.: Framework and capability of industrial IoT infrastructure for smart manufacturing. Standards **3**(1), 1–18 (2023)
5. Ryalat, M., ElMoaqet, H., AlFaouri, M.: Design of a smart factory based on cyber-physical systems and Internet of Things towards Industry 4.0. Applied Sciences **13**(4), 2156 (2023)
6. Pandey, N.K., Kumar, K., Saini, G., Mishra, A.K.: Security issues and challenges in cloud of things-based applications for industrial automation. Annals of Operations Research, 1–20 (2023)
7. Gunasekaran, K., Kumar, V.V., Kaladevi, A.C., Mahesh, T.R., Bhat, C.R., Venkatesan, K.: Smart decision-making and communication strategy in industrial internet of things. IEEE Access **11**, 28222–28235 (2023)
8. Sasikumar, A., et al.: Blockchain-based trust mechanism for digital twin empowered Industrial Internet of Things. Futur. Gener. Comput. Syst. **141**, 16–27 (2023)
9. Ryalat, M., ElMoaqet, H., AlFaouri, M.: Design of a smart factory based on cyber-physical systems and 9Internet of Things towards Industry 4.0. Applied Sciences **13**(4), 2156 (2023)
10. De Giacomo, G., Favorito, M., Leotta, F., Mecella, M., Silo, L.: Digital twins composition in smart manufacturing via Markov decision processes. Comput. Ind. **149**, 103916 (2023)
11. Chen, H., Jeremiah, S.R., Lee, C., Park, J.H.: A digital twin-based heuristic multi-cooperation scheduling framework for smart manufacturing in iiot environment. Appl. Sci. **13**(3), 1440 (2023)
12. Juma, M., Alattar, F., Touqan, B.: Securing big data integrity for industrial IoT in smart manufacturing based on the trusted consortium blockchain (TCB). IoT **4**(1), 27–55 (2023)
13. Soliman, S., Oudah, W., Aljuhani, A.: Deep learning-based intrusion detection approach for securing industrial Internet of Things. Alex. Eng. J. **81**, 371–383 (2023)

14. Sankaran, K.S., Kim, B.H.: Deep learning based energy efficient optimal RMC-CNN model for secured data transmission and anomaly detection in industrial IOT. Sustainable Energy Technol. Assess. **56**, 102983 (2023)
15. Liu, S., Lu, Y., Li, J., Shen, X., Sun, X., Bao, J.: A blockchain-based interactive approach between digital twin-based manufacturing systems. Comput. Ind. Eng. **175**, 108827 (2023)
16. https://www.kaggle.com/datasets/munaalhawawreh/xiiotid-iiot-intrusion-dataset
17. Peng, S.-L., Jhanjhi, N. Z., Pal, S., Amsaad, F., (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
18. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
19. Pal, S., Díaz, V.G., Le, D.-N. (eds.): IoT: Security and Privacy Paradigm, 1st ed. CRC Press (2020). https://doi.org/10.1201/9780429289057
20. Mukhopadhyay, K., et al.: Recent advancement of block chain in health care. In: AIP Conference Proceedings, Vol. 2845, No. 1. AIP Publishing (2023). https://doi.org/10.1063/5.0156992

Mental Disorder Classification Using Ensemble Machine Learning

K. Dheenathayalan(✉) and K. K. Savitha

PG Extension and Research Centre, Bharathiar University, Erode, India
prof.dheena@gmail.com

Abstract. Psychological health is a crucial part of people's lives and society. Poor mental health affects our well-being, our ability to work, and our connotations with friends, family, and community. There are many different types of mental illness, sometimes referred to as mental disorders with different causes, symptoms, and treatments. Early detection of mental health problems allows specialists to treat them more effectively and it improves patient's quality of life. Mental disorders are diagnosed and classified based on the symptoms and behavioural changes of the person. A few previous studies assessed machine learning techniques to detect mental health issues using several accuracy criteria. This study evaluated machine learning models logistic regression, random forest, naïve bayes, decision tree, k-nearest neighbor, neural network and ensemble machine learning to classify whether the persons working in tech industry suffered from mental illness or not, and compared their efficacy using accuracy, precision, recall and F1 score metrics. This study tested these machine learning models for classifying mental disorder data and found that ensemble learning classifier achieved best accuracy of 84.5%, precision of 0.80, recall of 0.91 and f1-score of 0.85.

Keywords: Mental disorder · Machine learning · Neural network · Accuracy · Ensemble learning

1 Introduction

Mental health conditions are not uncommon. Hundreds of millions suffer from them yearly, and many more do over their lifetimes. It's estimated that 1 in 3 women and 1 in 5 men will experience major depression in their lives. Mental health is a lot more than the absence of illness: it is an intrinsic part of our individual and collective health and well-being. we need to transform our attitudes, actions and approaches to promote and protect mental health, and to provide and care for those in need. To fight mental disorders, appropriate and timely assessment is essential to diagnose and classify one from the other.

Machine learning plays an important role in artificial intelligence. Machine learning is a subset of artificial intelligence, while neural networks are a subset of machine learning. Machine learning models are made up of algorithms that are capable of recognizing patterns within data. Machine learning begins with training data or input data.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 149–159, 2025.
https://doi.org/10.1007/978-3-031-91008-1_14

By analysing this information, machine learning models can identify patterns and trends in the data to make accurate predictions for the future based on the past data. Machine learning algorithms typically fall into one of three categories: supervised learning, unsupervised learning, or reinforcement learning. Neural networks are a specific type or subset of machine learning in which the model has interconnected nodes that function similarly to those of a human brain. This allows the model to learn and identify the relationships found between input and output data. Common types of neural networks include convolutional neural networks (CNN), feedforward neural networks (FNN), modular neural networks (MNN), and recurrent neural networks (RNN).

Machine learning deals with three problems: classification, regression, and clustering. It employs data and algorithms to imitate how people learn while gradually improving accuracy in various tasks. Machine learning has been applied to areas of mental treatment to detect and classify mental health conditions and analogous health outcomes. Typically, these algorithms require significant data to learn patterns and perform classification tasks. One of the most widely applied machine learning methods in the prediction of mental disorders is supervised learning.

1.1 Objective of the Work

The main objective of this work is to detect mental disorder of persons working in tech industry using ensemble machine learning algorithm. The proposed ensemble learning algorithm combines logistic regression, random forest and naïve bayes classifiers. The grid search technique has been used to increase the performance of the proposed algorithm by tuning the hyperparameters.

1.2 Supervised Machine Learning

Supervised learning, also known as supervised machine learning, is a subcategory of machine learning and artificial intelligence. It is defined by its use of labelled data sets to train algorithms that to classify data or predict outcomes accurately. As input data is fed into the model, it adjusts its weights until the model has been fitted appropriately, which occurs as part of the cross-validation process. Supervised learning uses a training set to teach models to yield the desired output. This training dataset includes inputs and correct outputs, which allow the model to learn over time. The algorithm measures its accuracy through the loss function, adjusting until the error has been sufficiently minimized. Supervised learning can be separated into two types of problems classification and regression [1, 2].

Classification uses an algorithm to accurately assign test data into specific categories. It recognizes specific entities within the dataset and attempts to draw some conclusions on how those entities should be labelled or defined. Common classification algorithms are linear classifiers, support vector machines (SVM), decision trees, k-nearest neighbour, and random forest. Regression is used to understand the relationship between dependent and independent variables. It is commonly used to make projections. Linear regression, logistical regression, and polynomial regression are popular regression algorithms [3, 5].

Neural Networks: Primarily leveraged for deep learning algorithms, neural networks process training data by mimicking the interconnectivity of the human brain through layers of nodes. Each node is made up of inputs, weights, a bias (or threshold), and an output. If that output value exceeds a given threshold, it activates the node, passing data to the next layer in the network. Neural networks learn this mapping function through supervised learning, adjusting based on the loss function through the process of gradient descent. When the cost function is at or near zero, we can be confident in the model's accuracy to yield the correct answer [10].

Naive Bayes: Naive Bayes is classification approach that adopts the principle of class conditional independence from the Bayes Theorem. This means that the presence of one feature does not impact the presence of another in the probability of a given outcome, and each predictor has an equal effect on that result. There are three types of Naïve Bayes classifiers: Multinomial Naïve Bayes, Bernoulli Naïve Bayes, and Gaussian Naïve Bayes. This technique is primarily used in text classification, spam identification, and recommendation systems [6, 11].

Support Vector Machines (SVM): A support vector machine is a popular supervised learning model used for both data classification and regression. That said, it is typically leveraged for classification problems, constructing a hyperplane where the distance between two classes of data points is at its maximum. This hyperplane is known as the decision boundary, separating the classes of data points on either side of the plane [7].

K-Nearest Neighbour: K-nearest neighbour, also known as the KNN algorithm, is a non-parametric algorithm that classifies data points based on their proximity and association to other available data. This algorithm assumes that similar data points can be found near each other. As a result, it seeks to calculate the distance between data points, usually through Euclidean distance, and then it assigns a category based on the most frequent category or average. Its ease of use and low calculation time make it a preferred algorithm by data scientists, but as the test dataset grows, the processing time lengthens, making it less appealing for classification tasks. KNN is typically used for recommendation engines and image recognition [4, 15].

Random Forest: Random forest is another flexible supervised machine learning algorithm used for both classification and regression purposes. The "forest" references a collection of uncorrelated decision trees, which are then merged together to reduce variance and create more accurate data predictions [12, 14].

Decision Tree: Decision Tree algorithms are a type of probability tree-like structural model that continuously separates data in order to categorize or make predictions depending on the results of the previous set of questions. The model analyses the data and provides responses to the questions in order to assist you in making more informed choices [8, 9].

1.3 Mental Disorders

Mental disorders can negatively affect a person's mood, behaviour, and thinking ability. These abnormalities can impact personal and professional relationships, sometimes creating an unhealthy environment for both the person and the people in their lives.

Types of Mental Disorders
Mental health disorders are characterized by issues regarding mood, thoughts, and behaviour. They may also be referred to as psychological disorders, mental illnesses, and mental health conditions. The types are, Major depressive disorder (MDD), Autism spectrum disorder (ASD), Loneliness, Bipolar disorder, Anxiety disorder, Post-traumatic stress disorder (PTSD), Sleeping disorder, psychotic depression, Obsessive-compulsive disorder (OCD), Pervasive developmental disorder (PDD), Attention-deficit/hyperactivity disorder (ADHD), Eating disorder (ED)

Mental health professionals diagnose mental health conditions using a list of symptoms such as, feeling nervous, Panic, breathing rapidly, Trouble in concentration, having trouble in sleeping, Hopelessness, Hallucinations, feeling negative, avoids people or activities, having nightmares, Social media addiction, Feeling tired, Suicidal thought.

The Mental Disorder Dataset
The mental disorder dataset used in this study is a survey of mental health in tech workplace created by Open Sourcing Mental Illness (OSMI) organization. The organization promotes mental health in tech industry through online resources, handbooks, research, and speaking at tech conferences. That includes various attributes like age, gender, self-employed, work interfere, leave and so on. The dataset includes 27 columns in which first column is timestamp and others are attributes of each patient. There are 1259 entries in the dataset, each row represents characteristics of each patient. Initially the dataset contains range values and categorical data. Some of the irrelevant columns are dropped from dataset, hence the dataset contains 24 columns. Then the cell values are encoded as numeric values and checked if there is any missing data. The target column is treatment column which decides whether the person needs treatment or not.

2 Algorithms Used

K-Nearest Neighbor
The K-nearest neighbors algorithm is a supervised classification algorithm. It classifies objects dependant on nearest neighbor. It is a type of instance-based learning. The calculation of distance of an attribute from its neighbors is measured using Euclidean distance.

Naïve Byes
Naïve Bayes classifier is a supervised algorithm. It is a simple classification technique using Bayes theorem. It assumes strong (Naive) independence among attributes. Bayes theorem is a mathematical concept to get the probability. The predictors are neither related to each other nor have correlation to one another. All the attributes independently con tribute to the probability to maximize it. It is able to work with Naïve Bayes model and does not use Bayesian methods. Many complex real-world situations use Naive Bayes classifier.

Decision Tree
Decision tree is a classification algorithm that works on categorical as well as numerical data. Decision tree is used for creating tree-like structures. Decision tree is simple and widely used to handle medical dataset. It is easy to implement and analyse the data in tree-shaped graph. The decision tree model makes analysis based on three nodes: root node, interior node and leaf node.

Random Forest
Algorithm Random forest algorithm is a supervised classification algorithmic technique. In this algorithm, several trees create a forest. Each individual tree in random forest lets out a class expectation and the class with most votes turns into a model's forecast. In the random forest classifier, the greater number of trees give higher accuracy.

Neural Network
MLP (Multi-Layer Perceptron) is a type of neural network with an architecture consisting of input, hidden, and output layers of interconnected neurons. It is capable of learning complex patterns and performing tasks such as classification and regression by adjusting its parameters through training.

Ensemble Learning: The term ensemble means 'collection of things', in machine learning terminology it means an approach to combine multiple machine learning models to achieve better accuracy and robustness compared to individual model. Ensemble learning combines predictions from multiple models to obtain better predictive accuracy [13]. In this work we proposed an ensemble technique which combines logistic regression, random forest and naïve bayes. We used voting classifier machine learning model to combine the above said three classifiers. The performance of the proposed model is increased by tuning the hyperparameters such as n_estimators and random_state using Grid Search technique.

3 Results and Discussion

3.1 Feature importance

The important features from the dataset are identified using extra-tree classifier. The Extra Tree Classifier is an ensemble algorithm that seeds multiple tree models constructed randomly from the training dataset and sorts out the features that have been most voted for. The Figs. 1 shows the importance of features in descending order, that means the

very first feature *Age* is the most important feature and *gender* is the second most important feature and so on. Based on the importance, the top eight features are selected for prediction of mental illness.

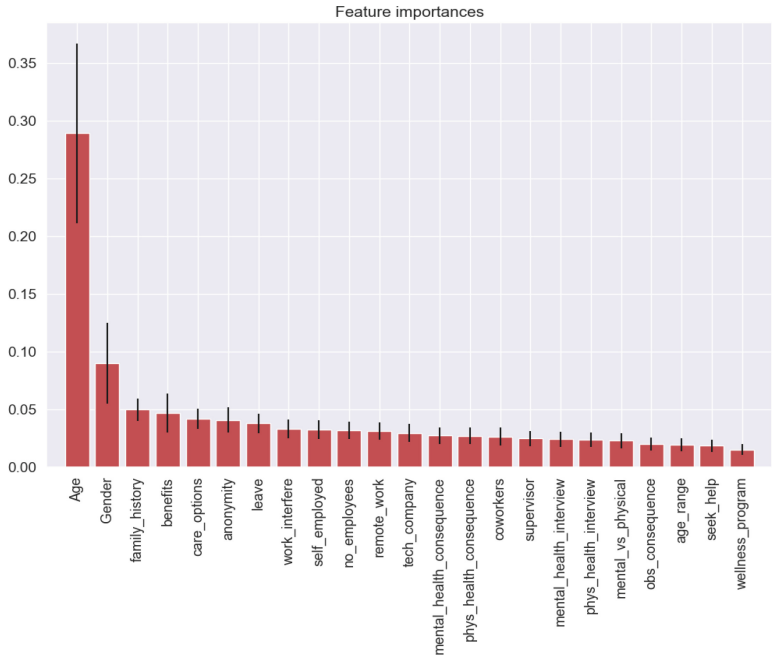


Fig. 1. Feature importance

3.2 Classification of Mental Disorders

A confusion matrix is a matrix that summarizes the performance of a machine learning model on a set of test data. It is a means of displaying the number of accurate and inaccurate instances based on the model's predictions. It is often used to measure the performance of classification models, which aim to predict a categorical label for each input instance. While assessing a classification model's performance, a confusion matrix is essential. It offers a thorough analysis of true positive, true negative, false positive, and false negative predictions, facilitating a more profound comprehension of a model's recall, accuracy**,** precision**,** and overall effectiveness in class distinction. When there is an uneven class distribution in a dataset, this matrix is especially helpful in evaluating a model's performance beyond basic accuracy metrics.

The confusion matrices of machine learning models are given in Figs. 4, 7, 10, 13 and 16. The Receiver Operating Characteristics (ROC) Curve is the graphical representation of the effectiveness of the binary classification model. It plots the true positive rate (TPR) vs the false positive rate (FPR) at different classification thresholds. The ROC curves of all models are shown in Figs. 3, 6, 9, 12 and 15. Prediction of probability is used to find the probability distribution and histogram of probability prediction of all models is given in Figs. 2, 5, 8, 11 and 14. Figure 17 displays comparison accuracy of individual models.

3.3 Decision Tree Classifier

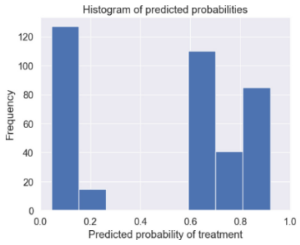


Fig. 2. DT-prediction probability

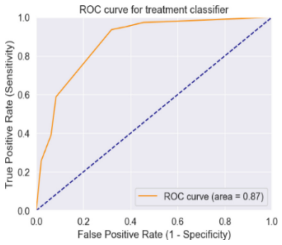


Fig. 3. DT – ROC curve

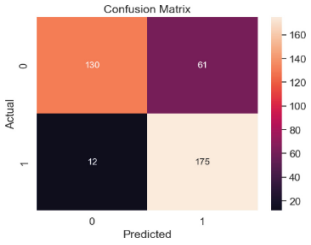


Fig. 4. DT – confusion matrix

3.4 Random Forest Classifier

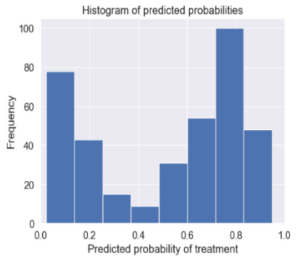


Fig. 5. RF-prediction probability

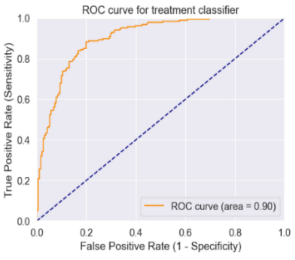


Fig. 6. RF – ROC curve

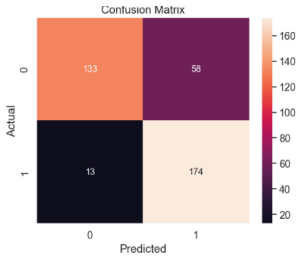


Fig. 7. RF – confusion matrix

3.5 Logistic Regression

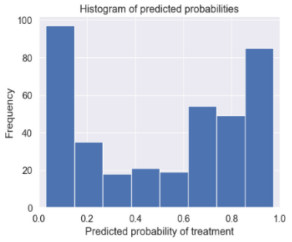


Fig. 8. LR-prediction pro bability

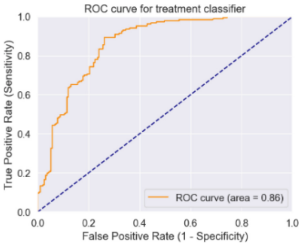


Fig. 9. LR – ROC curve

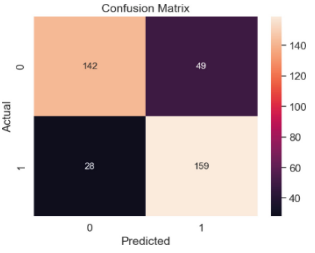


Fig. 10. LR – confusion matrix

3.6 Proposed Ensemble Technique

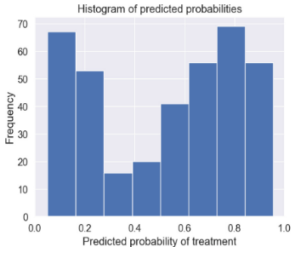


Fig. 11. Prediction probability

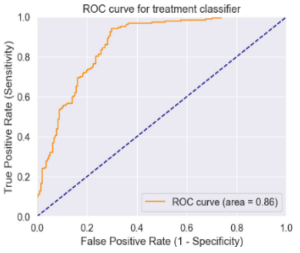


Fig. 12. ROC curve

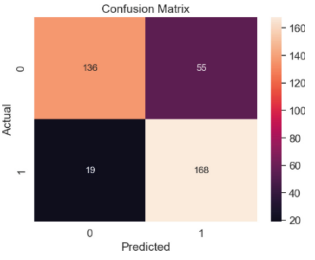


Fig. 13. Confusion matrix

3.7 Performance Improved Using Grid Search

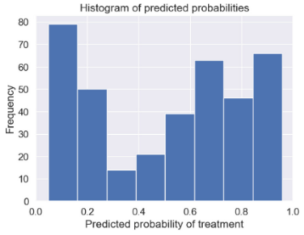


Fig. 14. Prediction probability

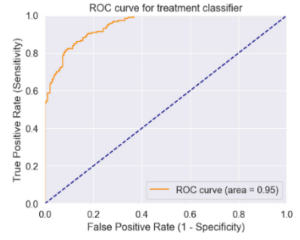


Fig. 15. ROC curve

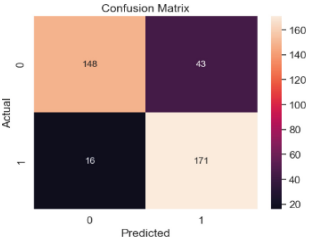


Fig. 16. Confusion matrix

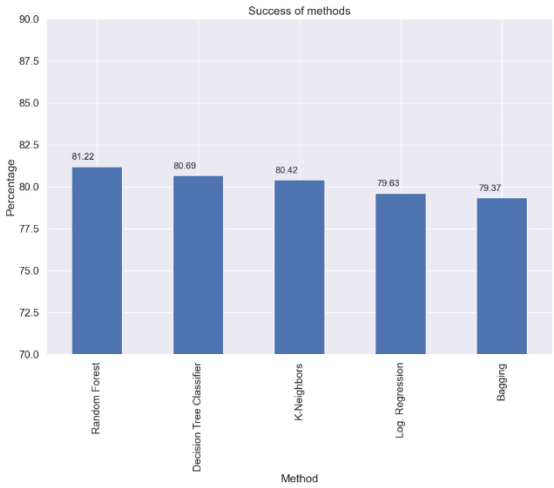


Fig. 17. Comparison of model accuracy

The values of the quality metrics of different classifiers are shown in Table 1. It clearly understandable that the ensemble classifier with grid search tuning outperformed other classifiers in aspect of accuracy, precision and f1-score.

Table 1. Performance metrics of classification models

Technique	Accuracy	Precision	Recall	F1-Score
Ensemble with Grid Search Tuning	**84.3%**	**0.80**	0.91	**0.85**
Ensemble	81.4%	0.75	0.89	0.81
RFC	81.2%	0.75	**0.93**	0.83
DTC	80.6%	0.74	**0.93**	0.82
KNN	80.42%	0.78	0.84	0.81
LRC	79.63%	0.76	0.85	0.80
Bagging	79.37%	0.74	0.82	0.78

4 Conclusion

This study assessed and compared different supervised machine learning models for classifying mental disorder dataset. This dataset initially contained 1259 entries, 27 attributes and one target variable. After pre-processing and encoding the number of columns were reduced to 24. The dataset is transformed to a data frame then divided into training set (80%) and testing set (20%). All machine learning models are trained using this training data and then tested on testing set. The efficacy of models is compared

by using performance metrics accuracy, precision, recall, f1-score, confusion matrix and ROC curve. Based on the comparison it is found that proposed ensemble model achieved 81.4% and the performance of this model is improved with Grid Search technique and outperformed other models with accuracy of 84.3%, precision of 0.80 and f1-score of 0.85. The same classifiers can be tested on other datasets to evaluate their performance. Performance evaluation of machine learning models must include metrics other than above said in future to find the appropriate classification model. Machine learning algorithms are trained to make classifications based on the input data. Over time, the system can be trained and improved the way it functions based on the data it's already processed. Bias in the data or in the algorithm may lead to inaccurate predictions, hence the data and algorithm must be chosen wisely.

References

1. Chung, J., Teo, J.: Mental health prediction using machine learning: taxonomy, applications, and challenges. Appl. Computat. Intel. Soft Comp. **2022**, 1–19 (2022). https://doi.org/10.1155/2022/9970363
2. Arif, M.B., et al.: Classification of anxiety disorders using machine learning methods: a literature review. Insights of Biomedical Research **4**, 95–110 (2020). https://doi.org/10.36959/584/455
3. Rahman, A.U., et al.: Enhancing heart disease prediction using a self-attention-based transformer model. Scientific Reports 14 (2024)
4. Bhatt, C.M., Patel, P., Ghetia, T., Mazzeo, P.L.: Effective heart disease prediction using machine learning techniques. Algorithms **16**(2), 88 (2023). https://doi.org/10.3390/a16020088
5. Md Mamun, A., et al.: Heart disease prediction using supervised machine learning algorithms: Performance analysis and comparison. Computers in Biology and Medicine **136**, 104672 (2021). ISSN 0010-4825, https://doi.org/10.1016/j.compbiomed.2021.104672
6. Shah, D., Patel, S., Bharti, S.K.: Heart disease prediction using machine learning techniques. SN COMPUT. SCI. **1**, 345 (2020). https://doi.org/10.1007/s42979-020-00365-y
7. Uddin, S., Khan, A., Hossain, M.E. Moni, M.A.: Comparing different supervised machine learning algorithms for disease prediction. BMC Med. Inf. Deci. Making **19**(1), 1–16 (2019)
8. Dehkordi, S.K., Sajedi, H.: Prediction of disease based on prescription using data mining methods. Health Technol. **9**, 37–44 (2019). https://doi.org/10.1007/s12553-018-0246-2
9. Le, H.M., Tran, t.D., Tran, l.V.: Automatic heart disease prediction using feature selection and data mining technique. JCC **34**(1), 33–48 (2018)
10. Beulah Christalin Latha, C., Carolin Jeeva, S.: Improving the accuracy of prediction of heart disease risk based on ensemble classification techniques. Informatics in Medicine Unlocked **16**, 100203 (2019). ISSN 2352-9148, https://doi.org/10.1016/j.imu.2019.100203
11. Mohan, S., Thirumalai, C., Srivastava, G.: Effective heart disease prediction using hybrid machine learning techniques. IEEE Access **7**, 81542–81554 (2019). https://doi.org/10.1109/ACCESS.2019.2923707
12. Tarawneh, M., Embarak, O.: Hybrid approach for heart disease prediction using data mining techniques. In: Barolli, L., Xhafa, F., Khan, Z., Odhabi, H. (eds.) Advances in Internet, Data and Web Technologies. EIDWT 2019. Lecture Notes on Data Engineering and Communications Technologies, vol 29. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-12839-5_41

13. Jan, M., Awan, A.A., Khalid, M.S., Nisar, S.: Ensemble approach for developing a smart heart disease prediction system using classification algorithms **9**, 33–45 (2018). https://doi.org/10.2147/RRCC.S172035
14. Singh, P., Singh, G., Bharti, S.: The predictive model of mental illness using decision tree and random forest classification in machine learning. 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), pp. 01–05. Greater Noida, India (2022). https://doi.org/10.1109/ICACITE53722.2022.9823761
15. Sharma, V., Yadav, S., Gupta, M.: Heart disease prediction using machine learning techniques. 2nd International Conference on Advances in Computing, Communication Control and Networking (ICACCCN), pp. 177–181. Greater Noida, India (2020). https://doi.org/10.1109/ICACCCN51052.2020.9362842
16. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978981-99-3611-3
17. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-01829
18. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of first international conference on mathematical modeling and computational science. Advances in Intelligent. Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4
19. Mental disorder dataset: (https://www.kaggle.com/datasets/baselbakeer/mental-disorders-dataset)

The Properties of Types of Real Valued Set Functions Over $\alpha - \sigma-$ Algebra

Hind F. Abbas[1] and Ibrahim S. Ahmed[2(✉)]

[1] Directorate General of Education Salahaddin, Ministry of Education, Salahaddin, Iraq
hind.f.abbas35386@st.tu.edu.iq
[2] Department of Physics, College of Education-Tuzkhurmatu, Tikrit University, Salahaddin, Iraq
ibrahim1992@tu.edu.iq

Abstract. This paper introduces the idea of measure over $\alpha - \sigma-$ algebra and the main properties, examples, theorems, propositions and lemma for this notion has been investigated where a nonnegative extended real valued set function $\mathscr{d}$ on $\alpha - \sigma-$ algebra $\mathfrak{J}$ is named measure over $\alpha - \sigma-$ algebra $\mathfrak{J}$ if $\mathscr{d}(\phi) = 0$ and $\mathscr{d}(\bigcup_{n=1}^{\infty} A_n) = \sum_{n=1}^{\infty} \mathscr{d}(A_n)$ whenever $\{A_1, A_2, \dots\}$ is the family of disjoint set in $\alpha - \sigma-$ algebra $\mathfrak{J}$. Furthermore, we study the idea of countable additive over $\alpha - \sigma-$ algebra which is generalization for measure over $\alpha - \sigma-$ algebra and we conclude that the notion of finite additive over $\alpha - \sigma-$ algebra is weaker than of countable additive over $\alpha - \sigma-$ algebra that is the countable additive over $\alpha - \sigma-$ algebra implies to finite additive over $\alpha - \sigma-$ algebra as well as we proved any measure over $\alpha - \sigma-$ algebra is countable additive over $\alpha - \sigma-$ algebra and the measure over $\alpha - \sigma-$ algebra implies that to finite additive over $\alpha - \sigma-$ algebra. We show that the difference of two measure over $\alpha - \sigma-$ algebra is countable additive over $\alpha - \sigma-$ algebra. It has been proved that a linear combination of measure over $\alpha - \sigma-$ algebra is measure over $\alpha - \sigma-$ algebra and the linear combination of outer measure over $\alpha - \sigma -$ algebra is also outer measure over $\alpha - \sigma-$ algebra. Moreover, we proved that every measure over $\sigma-$ algebra is measure over $\alpha - \sigma-$ algebra and we concluded every outer measure over $\sigma-$ algebra is outer measure over $\alpha - \sigma-$ algebra. Finally, it has been proved that every countable additive over $\sigma-$ algebra is countable additive over $\alpha - \sigma-$ algebra and every finite additive over $\sigma-$ algebra is finite additive over $\alpha - \sigma-$ algebra.

Keywords: $\sigma-$algebra · Fuzzy Set · Countable Additive · Measure · Finite Additive · $\alpha - \sigma-$field

1 Introduction

The $\sigma-$ algebra concept has been studied in (Ash, 1972) [1]. (Wang, 2009) [2] was studied some kinds of family of subsets such as ring, $\sigma-$ ring which are generalizations of $\sigma-$ algebra and proved some important results in the field of real analysis. Measure is a fundamental notion of mathematics, which is provide a mathematical abstraction for common notions like mass, length, distance, volume, area, probability. The set function is

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 160–168, 2025.
https://doi.org/10.1007/978-3-031-91008-1_15

extended real valued defined on family of subsets. (Ahmed et al.) [3–5] were introduced some generalizations of σ− algebra such as fuzzy σ− algebra, $\alpha-$ field and $\alpha-\sigma-$ algebra. A class $\mathfrak{J}$ is $\alpha-\sigma-$ algebra iff $\Phi, \Omega \in \mathfrak{J}$ and $\bigcup_{n=1}^{\infty} A_n \in \mathfrak{J}$ for $A_1, A_2, \cdots \in \mathfrak{J}$. The concept of outer measure was studied by (Dudzik & Skrzyński, 2016) [6]. The notion of measure defined on σ− algebra was studied by (Xue-Mei, 2021) [7]. The notion of monotone measure was studied by (Wang and Li, 2018) [8].

1.1. Objective of the article is to study some notions in real analysis such as measure, outer measure and countable additive over $\alpha-\sigma-$ algebra as well as this article aims to introduce these concepts and investigating some of its properties. Finally, aims to study the relations among these concepts.

2 The Results

Definition 1. The non-negative extended real-valued set function $\mathscr{d}$ on $\mathfrak{J}$ is named measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$ if $\mathscr{d}(\phi)=0$ and $\mathscr{d}(\bigcup_{n=1}^{\infty} A_n)=\sum_{n=1}^{\infty}\mathscr{d}(A_n)$ for $\{A_1, A_2, \dots\}$ is family of disjoint set in $\mathfrak{J}$.

Definition 2. If Ω is universal set,$\mathfrak{J}$ is $\alpha-\sigma-$ algebra & $\mathscr{d}$ is measure over$\alpha-\sigma-$algebra, then $(\Omega, \mathfrak{J}, \mathscr{d})$ is named measure space over$\alpha-\sigma-$ algebra.

Example 1. Let $\Omega=\{1,2,3\}$ and $\mathfrak{J}=\{\phi, \Omega, \{1\}, \{2\}, \{1,2\}\}$.

Then $\mathfrak{J}$ is $\alpha-\sigma-$ algebra.

Define $\mathscr{d}: \mathfrak{J} \to [0,\infty]$ as $\mathscr{d}(H)=\begin{cases} 0\, if\ H=\phi \\ \frac{1}{2}\, if\ H=\{1\} or \{2\} \\ 1 o.w. \end{cases}$

Then $\mathscr{d}(\phi)=0$ and $\{1\}, \{2\}$ are disjoint sets in $\mathfrak{J}$ and
$\mathscr{d}(\{1\}\bigcup\{2\})=\mathscr{d}(\{1\})+\mathscr{d}(\{2\})$.
Hence $\mathscr{d}$ is measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$.

Definition 3. Assume $\mathfrak{J}$ is $\alpha-\sigma-$ algebra, then $\mathscr{d}: \mathfrak{J} \to \overline{\mathbb{R}}$ is called countable additive over $\alpha-\sigma-$ algebra if $\mathscr{d}(\phi)=0$ and $\mathscr{d}(\bigcup_{n=1}^{\infty} A_n)=\sum_{n=1}^{\infty}\mathscr{d}(A_n)$ for $A_1, A_2, \dots$ are disjoint sets in $\mathfrak{J}$.

If this demand true only for finite disjoint set of $\mathfrak{J}$, then $\mathscr{d}$ is called finite additive over $\alpha-\sigma-$ algebra.

Example 2. Let $\Omega=\{a,b,c\}$ and $\mathfrak{J}=\{\phi, \Omega, \{a\}, \{b\}, \{a,b\}\}$.

Then $\mathfrak{J}$ is $\alpha-\sigma-$ algebra.

Define $\mathscr{d}: \mathfrak{J} \to [-\infty,\infty]$ as $\mathscr{d}(H)=\begin{cases} 0\, if\ H=\phi \\ -1\, if\ H=\{a\} or \{b\} \\ -2\, if\ H=\{a,b\} \\ 2\, o.w. \end{cases}$

Then $d(\phi)=0$ and $\{a\}, \{b\}$ are disjoint sets in $\mathfrak{J}$ and.
$d(\{a\}\cup\{b\})=d(\{a\})+d(\{b\})=-2$.
Hence d is a countable additive over $\alpha-\sigma-$ algebra $\mathfrak{J}$.

Lemma 1. Every measure over $\alpha-\sigma-$ algebra is countable additive defined on $\alpha-\sigma-$ algebra.

Proof. Assume $\mathfrak{J}$ is $\alpha-\sigma-$ algebra & $d\colon \mathfrak{J}\to[0,\infty]$ is measure over $\mathfrak{J}$, then $d(\phi)=0$ and $d\left(\cup_{n=1}^{\infty}A_n\right)=\sum_{n=1}^{\infty}d(A_n)$ for $\mathrm{A}_1, \mathrm{A}_2, \ldots$ are disjoint sets in $\mathfrak{J}$, hence d is countable additive over $\alpha-\sigma-$ algebra$\mathfrak{J}$.

Lemma 2. every countable additive over $\mathfrak{J}$ is finite additive over $\mathfrak{J}$ for any $\alpha-\sigma-$ algebra $\mathfrak{J}$.

Proof. Assume $\mathfrak{J}$ is $\alpha-\sigma-$ algebra & $d\colon \mathfrak{J}\to[-\infty,\infty]$ is countable additive over $\alpha-\sigma-$ algebra $\mathfrak{J}$, then $d(\phi)=0$. Let $\mathrm{V}_1, \mathrm{V}_2, \ldots, \mathrm{V}_k$ are disjoint sets in $\mathfrak{J}$ and put $V_m=\phi$ for all $m=\mathrm{k}+1,\ \mathrm{k}+2, \ldots$, then we get $\cup_{t=1}^{\infty}V_t=\cup_{t=1}^{k}V_t$, hence.

$d\left(\cup_{t=1}^{\infty}V_t\right)=\sum_{t=1}^{\infty}d(V_t)$ for $\mathrm{V}_1, \mathrm{V}_2, \ldots$ are disjoint sets in $\mathfrak{J}$ because d is countable additive over $\alpha-\sigma-$ algebra$\mathfrak{J}$.

Now, $d\left(\cup_{t=1}^{\infty}V_t\right)=d\left(\cup_{t=1}^{k}V_t\right)$ and.

$\sum_{t=1}^{\infty}d(V_t)=d(\mathrm{V}_1)+d(\mathrm{V}_2)+\ldots+d(\mathrm{V}_\mathrm{k})+d(\mathrm{V}_{\mathrm{k}+1})+\ldots=\sum_{t=1}^{k}d(V_t)$.

Hence, $d\left(\cup_{t=1}^{k}V_t\right)=\sum_{t=1}^{k}d(V_t)$. Therefore d is finite additive over $\alpha-\sigma-$ algebra$\mathfrak{J}$.

Theorem 1. Every measure over $\alpha-\sigma-$algebra is a finite additive over $\alpha-\sigma-$algebra.

Proof. Follows from Lemma 1 and Lemma 2.

Proposition 1. Assume that d_1, d_2 is measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$ & $d_1(V)\neq\infty ord_2(V)\neq\infty, \forall V\in\mathfrak{J}$. Define $d_1-d_2:\mathfrak{J}\to[-\infty,\infty]$ by: $(d_1-d_2)(V)=d_1(V)-d_2(V), \forall V\in\mathfrak{J}$, then d_1-d_2 is a countable additive over $\sigma-$ algebra $\mathfrak{J}$.

Proof. Since d_1, d_2 is measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$, then $d_1(\phi)=d_2(\phi)=0$, hence $(d_1-d_2)(\phi)=d_1(\Phi)-d_2(\phi)=0$.

Let $V_1, V_2, \ldots$ are disjoint sets in $\mathfrak{J}$. Then $d_i\left(\cup_{t=1}^{\infty}V_t\right)=\sum_{t=1}^{\infty}d_i(V_t)$, $i=1,2$. So, we have

$$(d_1-d_2)\left(\cup_{t=1}^{\infty}V_t\right)=d_1\left(\cup_{t=1}^{\infty}V_t\right)-d_2\left(\cup_{t=1}^{\infty}V_t\right)$$

$$=\sum\nolimits_{t=1}^{\infty}d_1(V_t)-\sum\nolimits_{t=1}^{\infty}d_2(V_t)$$

$$=\sum_{t=1}^{\infty}[d_1(V_t)-d_2(V_t)]$$

$$=\sum_{t=1}^{\infty}[d_1-d_2](V_t)$$

Therefore d_1-d_2 is a countable additive over $\sigma-$ algebra $\mathfrak{J}$..

Theorem 2. Assume $(\Omega,\mathfrak{J},d_\mathfrak{e})$ is measure space over $\sigma-$ algebra $\mathfrak{J}$ & $r_\mathfrak{e}\in[0,\infty)$ $\forall\mathfrak{e}=1,2,\ldots,k$. Let $\sum_{\mathfrak{e}=1}^{k}r_\mathfrak{e}d_\mathfrak{e}\colon\mathfrak{J}\to[0,\infty]$ be define as:

$(\sum_{\mathfrak{e}=1}^{k} r_{\mathfrak{e}} d_{\mathfrak{e}})(\mathcal{A}) = \sum_{\mathfrak{e}=1}^{k} r_{\mathfrak{e}}.d_{\mathfrak{e}}(\mathcal{A}) \forall \mathcal{A} \varepsilon \mathfrak{J}$, then $(\Omega, \mathfrak{J}, \sum_{\mathfrak{e}=1}^{k} r_{\mathfrak{e}} d_{\mathfrak{e}})$ is measure space over $\sigma -$ algebra $\mathfrak{J}$.

Proof. If $k = 2$, then $(r_1 d_1 + r_2 d_2)(\phi) = r_1.d_1(\phi) + r_2.d_2(\phi)$.

$$= r_1.0 + r_2.0 = 0$$

Let $D_1, D_2, \ldots$ are disjoint sets in $\mathfrak{J}$. Since d_e is measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$, $\mathfrak{e} = 1, 2$. Then $d_{\mathfrak{e}}\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right) = \sum_{t=1}^{\infty} d_{\mathfrak{e}}(\mathcal{A}_t)$. So, we have

$$(r_1 d_1 + r_2 d_2)\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right) = r_1.d_1\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right) + r_2.d_2\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right)$$

$$= r_1. \sum_{t=1}^{\infty} d_1(\mathcal{A}_t) + r_2. \sum_{t=1}^{\infty} d_2(\mathcal{A}_t)$$

$$= \sum_{t=1}^{\infty} r_1.d_1(\mathcal{A}_t) + \sum_{t=1}^{\infty} r_2.d_2(\mathcal{A}_t)$$

$$= \sum_{t=1}^{\infty} [r_1.d_1(\mathcal{A}_t) + r_2.d_2(\mathcal{A}_t)]$$

$$= \sum_{t=1}^{\infty} (c_1 d_1 + c_2 d_2)(\mathcal{A}_t)$$

Hence, $(\Omega, \mathfrak{J}, (r_1 d_1 + r_2 d_2))$ is measure space over $\sigma -$ algebra $\mathfrak{J}$.

Now, we assume that $(\Omega, \mathfrak{J}, \sum_{\mathfrak{e}=1}^{k} r_{\mathfrak{e}} d_{\mathfrak{e}})$ is measure space over $\alpha - \sigma -$ algebra $\mathfrak{J}$, where $k = \mathrm{m}$ & we claim it is true where $k = \mathrm{m} + 1$. Suppose that $(\Omega, \mathfrak{J}, d_{\mathfrak{e}})$ is measure space over $\alpha - \sigma -$ algebra $\mathfrak{J}$ & $r_{\mathfrak{e}} \in [0, \infty)$ $\forall \mathfrak{e} = 1, 2, \ldots, m, m + 1$. Then

$$(\sum_{\mathfrak{e}=1}^{m+1} r_{\mathfrak{e}} d_{\mathfrak{e}})(\phi) = \left(\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}} d_{\mathfrak{e}} + r_{m+1} d_{m+1}\right)(\phi)$$

$$= \sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}.d_{\mathfrak{e}}(\phi) + r_{m+1}.d_{m+1}(\phi)$$

$= 0$ since $d_{\mathfrak{e}}$ is measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$.

Let $\mathcal{A}_1, \mathcal{A}_2, \ldots$ are disjoint sets in $\mathfrak{J}$. Since $(\Omega, \mathfrak{J}, \sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}} d_{\mathfrak{e}})$ is measure space over $\alpha - \sigma -$ algebra $\mathfrak{J}$, then $\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}} d_{\mathfrak{e}}\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right) = \sum_{t=1}^{\infty} \left[\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}} \cup_{\mathfrak{e}}\right](\mathcal{A}_t)$. So, we have

$$(\sum_{\mathfrak{e}=1}^{m+1} r_{\mathfrak{e}} d_{\mathfrak{e}})\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right) = \left(\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}} d_{\mathfrak{e}} + r_{m+1} d_{m+1}\right)\left(\cup_{t=1}^{\infty} \mathcal{A}_t\right)$$

$$
\begin{aligned}
&= \sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}.d_{\mathfrak{e}}\big(\cup_{t=1}^{\infty}\mathcal{A}_t\big) + r_{m+1}.d_{m+1}\big(\cup_{t=1}^{\infty}\mathcal{A}_t\big)\\
&= (\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}d_{\mathfrak{e}})\big(\cup_{t=1}^{\infty}\mathcal{A}_t\big) + r_{m+1}.d_{m+1}\big(\cup_{t=1}^{\infty}\mathcal{A}_t\big)\\
&= \sum_{t=1}^{\infty}\left(\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}d_{\mathfrak{e}}\right)(\mathcal{A}_t) + r_{m+1}.\sum_{t=1}^{\infty} d_{m+1}(\mathcal{A}_t)\\
&= \sum_{t=1}^{\infty}[\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}.d_{\mathfrak{e}}(\mathcal{A}_t)] + \sum_{t=1}^{\infty} r_{m+1}.d_{m+1}(\mathcal{A}_t)\\
&= \sum_{t=1}^{\infty}[\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}.d_{\mathfrak{e}}(\mathcal{A}_t) + r_{m+1}.d_{m+1}(\mathcal{A}_t)]\\
&= \sum_{t=1}^{\infty}\left[\sum_{\mathfrak{e}=1}^{m} r_{\mathfrak{e}}d_{\mathfrak{e}} + r_{m+1}d_{m+1}\right](\mathcal{A}_t)\\
&= \sum_{t=1}^{\infty}[\sum_{\mathfrak{e}=1}^{m+1} r_{\mathfrak{e}}d_{\mathfrak{e}}](\mathcal{A}_t).
\end{aligned}
$$

Hence, $\sum_{\mathfrak{e}=1}^{m+1} r_{\mathfrak{e}}d_e$ is measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$, therefore $(\Omega, \mathfrak{J}, \sum_{\mathfrak{e}=1}^{k} r_{\mathfrak{e}}d_{\mathfrak{e}})$ is measure space over $\alpha-\sigma-$ algebra $\mathfrak{J}$.

Definition 4. The set function $d : \mathfrak{J} \to [0, \infty]$ is named outer measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$, if the following condition are satisfies:

1- $d(\phi) = 0$.
2- If $\mathcal{K}, \mathcal{H}\varepsilon\mathfrak{J}$ such that $\mathcal{K} \subset \mathcal{H}$, then $d(\mathcal{K}) \leq d(\mathcal{H})$.
3- If $\mathcal{H}_1, \mathcal{H}_2, \ldots$ disjoints in $\mathfrak{J}$, then $d\big(\cup_{t=1}^{\infty}\mathcal{H}_t\big) \leq \sum_{t=1}^{\infty} d(\mathcal{H}_t)$.

Proposition 2. If d is measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$ and $\mathcal{H}-\mathcal{K} \in \mathfrak{J}$ for $\mathcal{K}, \mathcal{H}\varepsilon\mathfrak{J}$, then d is outer measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$.

Proof. Assume $\mathcal{K}, \mathcal{H}\varepsilon\mathfrak{J}$ & $\mathcal{K} \subset \mathcal{H}$, then $\mathcal{H} = \mathcal{K} \cup (\mathcal{H}-\mathcal{K})$.

Since $\mathcal{K}$ and $(\mathcal{H}-\mathcal{K})$ are disjoint sets in $\mathfrak{J}$ and d is measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$, then $d(\mathcal{H}) = d(\mathcal{K} \cup (\mathcal{H}-\mathcal{K})) = d(\mathcal{K}) + d(\mathcal{H}-\mathcal{K})$, hence $d(\mathcal{K}) \leq d(\mathcal{H})$ because $d(\mathcal{H}-\mathcal{K}) \geq 0$. It is clear that $d(\phi) = 0$ and if $\mathcal{H}_1, \mathcal{H}_2, \ldots \varepsilon\mathfrak{J}$ and each of its disjoint, then $d\big(\cup_{t=1}^{\infty}\mathcal{H}_t\big) \leq \sum_{t=1}^{\infty} d(\mathcal{H}_t)$. Hence proved.

Theorem 3. Assume that $d_1, d_2, \ldots, d_{\mathrm{m}} : \mathfrak{J} \to [0, \infty]$ are outer measure over $\alpha-\sigma-$ algebra $\mathfrak{J}$ & $0 < \mathrm{c}_i < \infty\ \forall i = 1, 2, \ldots, \mathrm{m}$. Let $\sum_{i=1}^{\mathrm{m}} \mathrm{c}_i d_i$: $\mathfrak{J} \to [0, \infty]$ be define as: $(\sum_{i=1}^{\mathrm{m}} \mathrm{c}_i d_i)(\mathrm{A}) = \sum_{i=1}^{\mathrm{m}} \mathrm{c}_i.d_i(\mathrm{A})\forall \mathrm{A}\varepsilon\mathfrak{J}$, then $\sum_{i=1}^{\mathrm{m}} \mathrm{c}_i d_i$ is an outer measure over $\alpha-\sigma-$algebra $\mathfrak{J}$.

Proof. To claim it is true where m = 2. Since each of d_1 and d_2 outer measure over $\sigma -$ algebra $\mathfrak{J}$, then $d_1(\phi) = d_2(\phi) = 0$, hence $c_1 d_1(\phi) + c_2 d_2(\phi) = 0$, thus $(c_1 d_1 + c_2 d_2)(\phi) = 0$. Let $A, B \varepsilon \mathfrak{J}$ such that $A \subset B$. Since d_1, d_2 are outer measure, then $d_1(A) \leq d_1(B)$ and $d_2(A) \leq d_2(B)$. So, we have $(c_1 d_1 + c_2 d_2)(A) = c_1.d_1(A) + c_2.d_2(A) \leq c_1.d_1(B) + c_2.d_2(B) = (c_1 d_1 + c_2 d_2)(B)$.

Let $\mathcal{B}_1, \mathcal{B}_2, \ldots \varepsilon \mathfrak{J}$ and they are disjoints. To prove $(c_1 d_1 + c_2 d_2)\big(\cup_{n=1}^{\infty} \mathcal{B}_n\big) \leq \sum_{n=1}^{\infty} (c_1 d_1 + c_2 d_2)(\mathcal{B}_n)$.

Since d_i is outer measure over $\mathfrak{J}$, $i = 1, 2$. Then $d_i\big(\cup_{n=1}^{\infty} \mathcal{B}_n\big) \leq \sum_{n=1}^{\infty} d_i(\mathcal{B}_n)$. So, we have

$$(c_1 d_1 + c_2 d_2)\big(\cup_{n=1}^{\infty} \mathcal{B}_n\big) = c_1.d_1\big(\cup_{n=1}^{\infty} \mathcal{B}_n\big) + c_2.d_2\big(\cup_{n=1}^{\infty} \mathcal{B}_n\big)$$

$$\leq c_1. \sum_{n=1}^{\infty} d_1(\mathcal{B}_n) + c_2. \sum_{n=1}^{\infty} d_2(\mathcal{B}_n)$$

$$= \sum_{n=1}^{\infty} c_1.d_1(\mathcal{B}_n) + \sum_{n=1}^{\infty} c_2.d_2(\mathcal{B}_n)$$

$$= \sum_{n=1}^{\infty} [c_1.d_1(\mathcal{B}_n) + c_2.d_2(\mathcal{B}_n)]$$

$$= \sum_{n=1}^{\infty} (c_1.d_1 + c_2.d_2)(\mathcal{B}_n)$$

Hence, $(c_1 d_1 + c_2 d_2)$ is outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$.

Suppose $\sum_{i=1}^{t} c_i d_i$ is an outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$ and we claim $\sum_{i=1}^{t+1} c_i d_i$ is outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$.

Assume d_i outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$ & $0 < c_i < \infty \, \forall i = 1, 2, \ldots, t, t+1$. Then

$$(\sum_{i=1}^{t+1} c_i d_i)(\phi) = \left(\sum_{i=1}^{t} c_i d_i + c_{t+1} d_{t+1}\right)(\phi)$$

$$= \sum_{i=1}^{t} c_i.d_i(\phi) + c_{t+1}.d_{t+1}(\phi)$$

$$= (\sum_{i=1}^{t} c_i d_i)(\phi) + c_{t+1}.d_{t+1}(\phi)$$

since $\sum_{i=1}^{t} c_i d_i$ and d_{t+1} are outer measure, then

$$(\sum_{i=1}^{t} c_i d_i)(\phi) = 0 \text{ and } d_{t+1}(\phi) = 0$$

Hence, $(\sum_{i=1}^{t+1} c_i d_i)(\phi) = 0 + c_{t+1}.0 = 0.$

Let $A, B \varepsilon \mathfrak{J}$ such that $A \subset B$. Since $\sum_{i=1}^{t} c_i d_i$ and d_{t+1} are outer measure, then $(\sum_{i=1}^{t} c_i d_i)(A) \leq (\sum_{i=1}^{t} c_i d_i)(B)$ and $d_{t+1}(A) \leq d_{t+1}(B)$. So, we have

$(\sum_{i=1}^{t+1} c_i d_i)(A) = \left(\sum_{i=1}^{t} c_i d_i + c_{t+1} d_{t+1}\right)(A) = \sum_{i=1}^{t} c_i . d_i(A) + c_{t+1} . d_{t+1}(A)$, hence

$$(\sum_{i=1}^{t+1} c_i d_i)(A) = (\sum_{i=1}^{t} c_i d_i)(A) + c_{t+1} . d_{t+1}(A)$$

$$\leq (\sum_{i=1}^{t} c_i d_i)(B) + c_{t+1} . d_{t+1}(B)$$

$$= [\left(\sum_{i=1}^{t} c_i d_i) + c_{t+1} . d_{t+1}\right](B) = (\sum_{i=1}^{t+1} c_i d_i)(B).$$

Let $\mathcal{B}_1, \mathcal{B}_2, \ldots$ disjoint in $\mathfrak{J}$. Since $\sum_{i=1}^{t} c_i d_i$ and d_{t+1} are outer measure, then.

$(\sum_{i=1}^{t} c_i d_i)\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right) \leq \sum_{n=1}^{\infty} (\sum_{i=1}^{t} c_i d_i)(\mathcal{B}_n)$ and

$d_{t+1}\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right) \leq \sum_{n=1}^{\infty} d_{t+1}(\mathcal{B}_n)$, thus

$$(\sum_{i=1}^{t+1} c_i d_i)\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right) = \left(\sum_{i=1}^{t} c_i d_i + c_{t+1} d_{t+1}\right)\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right)$$

$$= \sum_{i=1}^{t} c_i . d_i\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right) + c_{t+1} . d_{t+1}\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right)$$

$$= (\sum_{i=1}^{t} c_i d_i)\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right) + c_{t+1} . d_{t+1}\left(\cup_{n=1}^{\infty} \mathcal{B}_n\right)$$

$$\leq \sum_{n=1}^{\infty} (\sum_{i=1}^{t} c_i d_i)(\mathcal{B}_n) + c_{t+1} . \sum_{n=1}^{\infty} d_{t+1}(\mathcal{B}_n)$$

$$= \sum_{n=1}^{\infty} (\sum_{i=1}^{t} c_i d_i)(\mathcal{B}_n) + \sum_{n=1}^{\infty} c_{t+1} . d_{t+1}(\mathcal{B}_n)$$

$$= \sum_{n=1}^{\infty} [\sum_{i=1}^{t} c_i . d_i(\mathcal{B}_n) + c_{t+1} . d_{t+1}(\mathcal{B}_n)]$$

$$= \sum_{n=1}^{\infty} (\sum_{i=1}^{t+1} c_i d_i)(\mathcal{B}_n)$$

Hence, $\sum_{i=1}^{t+1} c_i d_i$ is an outer measure over $\mathfrak{J}$.

Therefore $(\sum_{i=1}^{m} c_i d_i)$ is an outer measure over $\mathfrak{J}$.

Corollary 1. Assume $d: \mathfrak{J} \to [0, \infty]$ outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$ &a > 0. If $(ad)(H) = a.d(H) \forall H \in \mathfrak{J}$, then (ad) outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$.

Proof. direct from Theorem 3.

Corollary 2. Let $d_1, d_2 : \mathfrak{J} \to [0, \infty]$ be outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$. If $d_1 + d_2: \mathfrak{J} \to [0, \infty]$ is set function as follows:

$(d_1+d_2)(H) = d_1(H)+d_2(H) \forall H \in \mathfrak{J}$, then (d_1+d_2) is outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$.

Proof. follows from Theorem 3 when $m = 2$and $c_1 = c_2 = 1$..

Theorem 4. Assume that d is a set function defined on $\sigma -$ algebra.

1. If d is measure over $\sigma -$ algebra, then it is measure over $\alpha - \sigma -$ algebra.
2. If d is outer measure over $\sigma -$ algebra, then it is outer measure over $\alpha - \sigma -$ algebra.
3. If d is finite additive over $\sigma -$ algebra, then it is finite additive over $\alpha - \sigma -$ algebra.
4. If d is countable additive over $\sigma -$ algebra, then it is countable additive over $\alpha - \sigma -$ algebra.

Proof. The prove follows because every $\sigma -$ algebra is a $\alpha - \sigma -$ algebra.

Remark 1. A reverse for above Theorem is not hold in general, because a $\alpha - \sigma -$ algebra need not be a $\sigma -$ algebra.

Example 3. Let $\Omega = \{a, b, c\}$ and $\mathfrak{J} = \{\phi, \Omega, \{a\}, \{c\}, \{a, c\}\}$.

Then $\mathfrak{J}$ is $\alpha - \sigma -$ algebra.

Define $d: \mathfrak{J} \to [0, \infty]$ as $d(H) = \begin{cases} 0 & if\ H = \phi \\ \frac{1}{2} & if\ H = \{a\} or \{c\} \\ 1 & o.w. \end{cases}$.

Then $d(\phi) = 0$ and $d(\{a\} \cup \{c\}) = d(\{a\}) + d(\{c\})$.

Hence d is measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$.

On the other hand, $\mathfrak{J}$ is not $\sigma -$ algebra, because $\{a\} \in \mathfrak{J}$, but $\{a\}^c = \{b, c\} \notin \mathfrak{J}$.

By the similar way, we can show that for outer measure, finitely additive and countably additive.

This example verifies that the reverse of Theorem 2.16 is not true.

3 Conclusion

- Every measure over $\alpha - \sigma -$ algebra$\mathfrak{J}$ is countable additive over $\mathfrak{J}$.

- Every measure over $\alpha - \sigma -$ algebra$\mathfrak{J}$ is finite additive over $\mathfrak{J}$.
- If d_1, d_2 are measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$ & $d_1(A) \neq \infty \, or \, d_2(A) \neq \infty, \forall A \in \mathfrak{J}$. Define $d_1 - d_2 : \mathfrak{J} \to [-\infty, \infty]$ by: $(d_1 - d_2)(A) = d_1(A) - d_2(A), \forall A \in \mathfrak{J}$, then $d_1 - d_2$ is a countable additive over $\mathfrak{J}$.
- Assume $(\Omega, \mathfrak{J}, d_\mathfrak{e})$ measure space over $\alpha - \sigma -$ algebra $\mathfrak{J}$ & $0 \leq c_\mathfrak{e} < \infty \; \forall \mathfrak{e} = 1, 2, \ldots, k$. Define $\sum_{\mathfrak{e}=1}^{k} c_\mathfrak{e} d_\mathfrak{e} \colon \mathfrak{J} \to [0, \infty]$ by: $(\sum_{\mathfrak{e}=1}^{k} c_\mathfrak{e} d_\mathfrak{e})(A) = \sum_{\mathfrak{e}=1}^{k} c_\mathfrak{e}.d_\mathfrak{e}(A) \forall A \varepsilon \mathfrak{J}$, then $(\Omega, \mathfrak{J}, \sum_{\mathfrak{e}=1}^{k} c_\mathfrak{e} d_\mathfrak{e})$ is measure space over $\mathfrak{J}$.
- Let $d_1, d_2, \ldots, d_\mathrm{m} : \mathfrak{J} \to [0, \infty]$ be outer measure over $\alpha - \sigma -$ algebra $\mathfrak{J}$ & $0 < \mathrm{c}_i < \infty \; \forall i = 1, 2, \ldots, \mathrm{m}$. Define $\sum_{i=1}^{\mathrm{m}} \mathrm{c}_i d_i \colon \mathfrak{J} \to [0, \infty]$ as: $(\sum_{i=1}^{\mathrm{m}} \mathrm{c}_i d_i)(\mathrm{A}) = \sum_{i=1}^{\mathrm{m}} \mathrm{c}_i.d_i(\mathrm{A}) \forall \mathrm{A} \varepsilon \mathfrak{J}$, then $\sum_{i=1}^{\mathrm{m}} \mathrm{c}_i d_i$ outer measure over $\mathfrak{J}$.

References

1. Ash, R.B.: Real Analysis and Probability. Academic Press (1972)
2. Wang, Z., Klir, G.: Generalized Measure Theory. Springer Science and Business Media (2009)
3. Ahmed, I.S., Al-Fayadh, A., Ebrahim, H.H.: Fuzzy σ-algebra and some related concepts. AIP Conf. Proc. **2834**(1) (2023). https://doi.org/10.1063/5.0162037
4. Ahmed, I.S., Ebrahim, H.H.: On α-field and β-field. Journal of Phys. Conf. Ser. **1294**(3) (2019). https://doi.org/10.1088/1742-6596/1294/3/032015
5. Ahmed, I.S., Ebrahim, H.H.: Generalizations of σ-field and new collections of sets noted by δ-field. AIP Conf. Proc. **2096**(20019), 020019-1–020019-6 (2019). https://doi.org/10.1063/1.5097816
6. Dudzik, D., Skrzyński, M.: An outer measure on a commutative ring. Algebr. Discret. Math. **21**(1), 51−58 (2016)
7. Xue-Mei, L.: Measure and integration. Henri Elad Altman Imperial College London (2021)
8. Wang, P., Yu, M., Li, J.: Monotone measures defined by pan-integral. Adv. Pure Math. **8**(6), 535–547 (2018). https://doi.org/10.4236/apm.2018.86031

Improving Adaptive Penalized Likelihood in Poisson Regression Model

Dheyaa N. Ahmed[1(✉)], Zakariya Y. Algamal[2], and Mundher A. Khaleel[1]

[1] Department of Mathematics, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq
dheyaaan39@gmail.com, mun880088@tu.edu.iq
[2] Department of Statistics and Informatics, University of Mosul, Mosul, Iraq
zakariya.algamal@uomosul.edu

Abstract. One for difficulties in utilizing the Poisson reg. Mod. Where explanatory variable are associated is reducing the high dimensional count data using penalized Poisson reg. In order to address the drawbacks of adaptive elastic net in variable select where there is little to medium correlation between explanatory variables, an improving of adaptive elastic net (IAEN) was presented in this study to account for grouping effects in a Poisson regression model. Through simulation, the IAEN performance was showcased. In comparison to other existing penalized approaches, our simulation tests demonstrate that IAEN has an advantage small and medium and very correlate variable in terms for each prediction with variable select accuracy. Thus, IAEN is a trustworthy penalized approach for grouping effects poison reg. Mod., we can conclude.

Keywords: High Dimensional Data · Adaptive Elastic Net · Poisson Regression Model; Penalization

1 Introduction

As technology has developed, vast volumes for data and ever-increasing dimension were produced in a variety of fields, including the social, medical, economic, and genetic sciences. A number for variable and A number for observation each represent two dimensions in which the data is expanded. When there are more measured variables than observations in the data, the situation is referred to as "high-dimensional data." This is not like the usual statistical analysis datasets where we have a large number of observations on a small number of variables. Because many traditional statistical techniques do not always work with high-dimensional data, such as curse for dimensional, which renders some classical reg. Mod—including multiple regression, logistic reg, and Poisson regression—ineffective, high-dimensional data modeling presents additional challenges to statistical analysis. These challenges contain mod. Over fit, estimate instability, and computation difficult (Pourahmadi, 2013).

In statistical applications, one of the key research questions has been how to minimize dimensionality. Data reduction is one method for dealing with the high dimensional

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 169–174, 2025.
https://doi.org/10.1007/978-3-031-91008-1_16

data. To do this, a number of punitive measures have been suggested, starting in (Hoerl and Kennard, 1970). Which estimate a reg. Coefficient through ℓ_2-norm penalty. Ridge reg. Shrink coefficients for correlate predictor variable to every other, they to borrow strengthing from every others (Hastie, 2010). Zou (2005) studied elastic net penalty.

The explanatory variables on high dimensiol data is typically correlate. When the set for highly correlate variable exists, the elastic net will choose all highly correlate explanatory variable in the group, whereas LASSO would randomly select one variable and discard the others (Zou, 2005) (Zhou, 2013). Bondell (2008) studied the penalty named OSCAR. When there is connection between variable, elastic net frequently outperforms LASSO in terms forprediction error; also, OSCAR perform similar, for elastic net (Xie, 2011). Tutz (2009) studied corelation-base to deal group effect. El Anbari and Mkhadri (2014) studied $|\rho| \leq 0.95$.

this work a (IAEN) was proposed to take into account the amount of the correlation among variable in poisson reg.

2 Penalized Poisson Regression Model

In the literature on econometrics and medicine, poisson regression models have drawn a lot of interest as a mod. For representing count data which suppose integer value proportional to a number of event happening in the given interval. Simplest mod. is the Poisson reg. Mod. The define feature for this mod. is outcome's condition mean equal the conditional variance (Algamail, 2012) (Zeng, 2013). Term $P_\lambda(\beta)$ to log-likelihood functions is get better estimate for prediction error about avoid,. Overfitting. Friedman (2010) was developed eff. Algorithm for estimate a generalized lin. Mod. Containing poisson reg. And convex penalty. Fan (2011) develop methodologies for nonconcave penalization. Hossain (2012) studied Stein-type shrinkage estimator. Wang (2014) studied a combination of minimax.

In poisson reg. Mod, number of events y_i has poisson distribution

$$f(y_i|x_i) = \frac{e^{-\theta_i}\theta_i^{y_i}}{y_i!}, \quad y_i = 0, 1, \ldots; \; i = 1, 2, \ldots, n \tag{1}$$

A conditional mean

$$\theta_i = \exp(x_i'\beta). \tag{2}$$

A log-likelihood function is

$$\ell(\beta) = \sum_{i=1}^{n} \left\{ y_i x_i'\beta - \exp(x_i'\beta) - \ln y_i! \right\}. \tag{3}$$

$$PPR = \ell(\beta) + \lambda P(\beta) \tag{4}$$

where ($\lambda \geq 0$). Cross-validation method (Fan, 2013) (James, 2013). so that $\sum_{i=1}^{n} y_i = 0$, $\frac{1}{n}\sum_{i=1}^{n} X_{ij} = 0$, and $\sum_{i=1}^{n} X_{ij}^2 = 1$ for $j = 1, 2, ..., k$, proposed by Park (2007).

This method can accomplish variable selection since it has the ability to reduce some coefficients to zero, The LASSO estimator is

$$\hat{\beta}_{LASSO} = \arg\min_{\beta} \left(-\ell(\beta) + \lambda \sum_{j=1}^{k} |\beta_j| \right) \tag{5}$$

where $\lambda \geq 0$

Zou studied aelastic net estimator in (2005). Poisson reg. Model is

$$\hat{\beta}_{Elastic} = \arg\min_{\beta} \left(-\ell(\beta) + \lambda_1 \sum_{j=1}^{k} |\beta_j| + \lambda_2 \sum_{j=1}^{k} |\beta_j|^2 \right) \tag{6}$$

As Eq. (6), if net estima depended to λ_1, λ_2 & leads to penalize poisson reg. Solution.

3 Improving Elastic Net Penalty

We present our proposed modification for elastic net (IAEN) in poisson reg. Mod. Define the IAEN estimator as

$$\hat{\beta}_{IAEN} = \arg\min_{\beta} \left\{ -\ell(\beta) + \lambda_1 \sum_{j=1}^{p} w_j |\beta_j| + \lambda_2 \sum_{j=1}^{p} \beta_j^2 \right\} \tag{7}$$

where λ_1 and λ_2 is nonnegative & $\mathbf{w}_j = (w_1, ..., w_p)^T$ is $p \times 1$. It depend on the root n-consistent initial values of $\hat{\beta}$ and $\mathbf{w}_j = (|\hat{\beta}_j|)^{-\gamma}$, where γ is a positive constant.

The IAEN was solved using coordinate (Friedman, 2010) A optimal MEN mod. Was parameters λ_1 and λ_2.

Let $\hat{\beta}_{\text{Ridge}} = (\hat{\beta}_{1(\text{Ridge})}, ..., \hat{\beta}_{p(\text{Ridge})})^T$, $\mathbf{s}_{\hat{\beta}_{Ridge}} = (s_{1(\hat{\beta}_{Ridge})}, ..., s_{p(\hat{\beta}_{Ridge})})^T$ then $\mathbf{w}_{Ratio} = (w_{1(ratio)}, ..., w_{p(ratio)})^T$ is ratio weight vector where $\mathbf{w}_j = (\mathbf{s}_{j(\hat{\beta}_{Ridge})}/|\hat{\beta}_{j(Ridge)}|)^{-\gamma}$, $j = 1, 2, ..., p$. Furthermore, let $\mathbf{x}_{ij}^{**} = \mathbf{x}_{ij}^{*}/\mathbf{w}_{Ratio,j}, j = 1, 2, ..., p$, then, the regularized poisson reg use IAEN is defined as:

$$\hat{\beta}_{IAEN}^{**} = \arg\min_{\beta} \left[-\ell(\beta) + \lambda_1 \sum_{j=1}^{p} \mathbf{w}_{Ratio,j} |\beta_j| + \lambda_2 \sum_{j=1}^{p} \beta_j^2 \right]. \tag{8}$$

4 Simulation Study

This part examines a performance for suggested IAEN using simulated studies. Additionally, we contrast IAEN with elastic net and LASSO. With a θ_i. All simulation scenarios are replicate 100 times. Model fitting was done using the training set of data. The tuning parameters were established using the validation data. The penalization techniques were assessed using the test results. Training, Validation, and Testing are used to indicate the observation numbers of the respective data sets for each scenario. We used three metric(MSEt), hits, which represent a number for correctly identified true variable, & false positive (FP),

Furthermore, it varied quantity for variable.

Scenario 1: In this setting, we have 50/50/100 and 100 explanatory variable. Four case is given.

Case A: we put $\varepsilon_i \sim N(0, 0.01), \quad i = 10, 11, ..., 100$. A correlation among variable within every group is 0.98. A true variable' parameter is $\beta = (\underbrace{0.3, ..., 0.3}_{9}, \underbrace{0, ..., 0}_{91})$.

Case B: This except $\varepsilon_i \sim N(0, 0.6), \quad i = 10, 11, ..., 100$. So, correlate within every group around, 0.7.

Case C: Similarty as case A, we get correlation with every group is 0.5.

Case D: Similarty as previous cases, we get correlation with every group is 0.3. Assume $\varepsilon_i \sim N(0, 1.5), \quad i = 10, 11, ..., 100$.

Scenario 2: This scenario is the same as scenario 1 with four cases, E, F, G, and H. Each case is corresponding to each case in scenario 1. A difference is generate data set & sample size 100/100/400 and 1000 explanatory variable.

5 Simulation Results

The IAEN penalty compare with two wellknown penalized meth.; LASSO and elastic net. A sequence of values for λ_2 is given, where $0 \leq \lambda_2 \leq 100$. Clearly IAEN have less variables comparing with LASSO. so, can seen IAEN & elastic net are slightly similar.

The (Std. Dev.) & MSEt, that were calculated use bootstrap and resampling on 100 MSEt, are summarized in Tables 1 and 2. Furthermore, FP and the median number of hits are also provided. The approach that performs best on MSEt, Std. Dev., hits, & FP is indicated in bold text in each example. Tables 1 and 2 show that, in every situation, the MEN approach yields significantly lower median MSEt and standard deviation than any other strategy. For instance, in scenario A, the MSEt of MEN is 4.811 with a Std. Dev. For 1.294, which is less than the corresponding values for the elastic net and LASSO methods, which are 4.887 (1.369) and 4.931 (1.378), respectively. Moreover, when compared to an elastic net, the MSEt is typically much reduced. As an illustration, the reduction in cases E, F, G, and H is, in that order, 0.67%, 1.60%, 5.01%, and 6.60%. Furthermore, there is a substantial degree of collinearity between the variables in cases A and E. Given that elastic net handles extraordinarily large correlations, it should perform better than IAEN. Furthermore, our technique works well for small and medium correlations in terms of MSEt. In addition, we can see from the simulation data that LASSO was the final technique used. This is because grouping effects between variables limit its applicability.

Hits & FP are use to assess how well IAEN, elastic net, & LASSO performed in terms for choosing the nonzero variable. Variable select accuracy, A penalization method must contain each significant variable (nonzero variable). In the majority of cases, IAEN is able to identify the true non-zero variables based on hits from Tables 1 and 2. In scenario 2, for instance, IAEN chooses each of the nine non-zero variables. Furthermore, in comparison to MEN and elastic net, LASSO selects fewer nonzero variable where a correlation coefficient ranges from tiny to highly high. This is to be expected, given grouping effects are LASSO's main weakness. When it comes to FP, the IAEN approach typically chooses fewer ineffective variables than LASSO and elastic net.

Table 1. Comparison between method on100 replication of scenario 1

	MSE_t (Std. Dev.)	Hits	False Positive
$\rho = 0.98$			
LASSO	4.874 (1.327)	5	15
Elastic net	4.714 (1.314)	9	13
IAEN	**4.622 (1.271)**	**9**	**13**
$\rho = 0.7$			
LASSO	7.621 (2.731)	7	14
Elastic net	7.305 (2.620)	8	13
IAEN	**6.877 (2.514)**	**8**	**12**
$\rho = 0.5$			
LASSO	6.881 (2.404)	7	12.5
Elastic net	6.774 (1.870)	7	11.5
IAEN	**6.399 (1.511)**	**7.5**	**10**
$\rho = 0.3$			
LASSO	6.811 (2.641)	7	16
Elastic net	6.697 (2.147)	7	15
IAEN	**6.278 (2.121)**	**7.5**	**12.5**

Table 2. Comparison between method relative100 replication of scenario 2

	MSE_t (Std. Dev.)	Hits	FP
$\rho = 0.98$			
LASSO	6.514 (2.101)	6	26.5
Elastic net	5.783 (1.771)	9	25
IAEN	**4.806 (1.557)**	**8.5**	**23**
$\rho = 0.7$			
LASSO	6.321 (1.831)	5	23
Elastic net	6.114 (1.722)	9	21.5
IAEN	**5.847 (1.514)**	**9**	**21**
$\rho = 0.5$			
LASSO	6.419 (1.877)	5	26
Elastic net	6.277 (1.851)	9	24.5
IAEN	**5.718 (1.611)**	**9**	**24**
$\rho = 0.3$			
LASSO	6.754 (2.152)	5	25
Elastic net	6.711 (1.771)	8	22
IAEN	**6.084 (1.603)**	**9**	**20**

6 Conclusion

A Poisson regression model application was used to suggest a research of an elastic net modification. Through simulation experiments, two penalized approaches, LASSO and elastic net, were evaluated with IAEN. According to the simulation results, the IAEN outperforms the other two techniques in terms of variable selection accuracy and mean-squared error of test data.

References

Algamal, Z.Y.: Diagnostic in poisson regression models. Electr. J. Appl. Statist. Analy. **5**(2), 178–186 (2012)

Bondell, H.D., Reich, B.J.: Simultaneous regression shrinkage, variable Selection, and supervised clustering of predictors with OSCAR. Biometrics **64**(1), 115–123 (2008). https://doi.org/10.1111/j.1541-0420.2007.00843.x

El Anbari, M., Mkhadri, A.: Penalized regression combining the L1 norm and a correlation based penalty. Sankhya B **76**(1), 82–102 (2014). https://doi.org/10.1007/s13571-013-0065-4

Fan, J., Lv, J.: Nonconcave penalized likelihood with NP-dimensionality. Information Theory, IEEE Transactions on **57**(8), 5467–5484 (2011). https://doi.org/10.1109/TIT.2011.2158486

Fan, Y., Tang, C.Y.: Tuning parameter selection in high dimensional penalized likelihood. Journal of the Royal Statistical Society: Series B (Statistical Methodology) **75**(3), 531–552 (2013). https://doi.org/10.1111/rssb.12001

Friedman, J., Hastie, T., Tibshirani, R.: Regularization paths for generalized linear models via coordinate descent. J. Stat. Softw. **33**(1), 1–22 (2010)

Hoerl, A.E., Kennard, R.W.: Ridge regression: biased estimation for nonorthogonal problems. Technometrics **12**(1), 55–67 (1970)

Hossain, S., Ahmed, E.: Shrinkage and penalty estimators of a Poisson regression model. Aust. N. Z. J. Stat. **54**(3), 359–373 (2012). https://doi.org/10.1111/j.1467-842X.2012.00679.x

James, G., Witten, D., Hastie, T., Tibshirani, R.: An introduction to statistical learning. Springer, New York (2013)

Park, M.Y., Hastie, T.: L1-regularization path algorithm for generalized linear models. J. Royal Statis. Soc. Series B (Statistical Methodology) **69**(4), 659–677 (2007). https://doi.org/10.1111/j.1467-9868.2007.00607.x

Pourahmadi, M.: High-dimensional covariance estimation: with high-dimensional data. John Wiley & Sons, Hoboken, New Jersey (2013)

Tibshirani, R.: Regression shrinkage and selection via the lasso. J. Royal Statis. Soc. Series B (Methodological) **58**(1), 267–288 (1996)

Tutz, G., Ulbricht, J.: Penalized regression with correlation-based penalty. Stat. Comput. **19**(3), 239–253 (2009)

Wang, Z., Ma, S., Zappitelli, M., Parikh, C., Wang, C.-Y., Devarajan, P.: Penalized count data regression with application to hospital stay after pediatric cardiac surgery. Stat. Methods Med. Res. (2014). https://doi.org/10.1177/0962280214530608

Zeng, L., Xie, J.: Group variable selection for data with dependent structures. J. Stat. Comput. Simul. **82**(1), 95–106 (2011). https://doi.org/10.1080/00949655.2010.529812

Zeng, P., et al.: Variable selection approach for zero-inflated count data via adaptive lasso. J. Appl. Stat. **41**(4), 879–894 (2013). https://doi.org/10.1080/02664763.2013.858672

Zhou, D.X.: On grouping effect of elastic net. Statist. Probab. Lett. **83**(9), 2108–2112 (2013)

Zou, H., Hastie, T.: Regularization and variable selection via the elastic net. J. Royal Statis. Soc. Series B-Statis. Methodol. **67**, 301–320 (2005)

Blockchain for Verifying IoT-Based Educational Certifications Aligned with Sustainable Development Goals

Swati Jeevan[1(✉)] and Srinath Doss[2]

[1] Department of Computer Science, Azteca University, Chalco de Díaz Covarrubias, Mexico
swatijeevan2307@gmail.com
[2] Faculty of Engineering and Technology, Botho University, Gaborone, Botswana
srinath.doss@bothouniversity.ac.bw

Abstract. The process of academic document verification is complex, and verifying the authenticity of papers requires a series of challenging and time-consuming procedures. The verification procedure includes the printing and transportation of documents, resulting in the use of paper. Additionally, manual verification is an exhausting task, and transportation contributes to the release of air pollutants and carbon emissions. Traditional verification procedures are sometimes time-consuming and need several administrative actions. The energy consumption in administrative offices has increased, resulting in longer processing times and the consequent extended utilization of resources. Therefore, IoT and Blockchain-based digital verification have the potential to revolutionize the process. The incorporation of IoT devices with Blockchain technology gives a sturdy solution for improving data integrity and verification of Certification in the Education sector [1].

This research examines the application of blockchain in storing data from IoT devices, with a particular emphasis on the verification of students' data and certificates to prevent fraud. To speed up the verification procedure, which is required for job applications and studying abroad. For Verifying academic credentials, the decentralised and unchangeable nature of Blockchain guarantees that students' data is reliable. This digital verification process contributes to sustainable development goals as this method also reduces the reliability of paper-based data verification [4]. The results of this research suggest that the integration of blockchain technology into educational verification systems has the potential to improve the efficacy of administrative processes, combat deception, and promote environmentally beneficial practices. This research underscores the potential of Digital Innovation, which is facilitated by Blockchain and IoT, to achieve the sustainable development objective of a critical educational documentation verification process.

Keywords: Blockchain · IoT (Internet of Things) · Sustainable Development Goals · Data Collection · Data Verifications

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 175–191, 2025.
https://doi.org/10.1007/978-3-031-91008-1_17

1 Introduction

In recent years, the integration of blockchain technology and the Internet of Things (IoT) has emerged as a practical option for enhancing the dependability and efficiency of educational certification operations. By using these technologies, educational institutions and organizations may address longstanding difficulties in verification and fraud prevention, ensuring the integrity and authenticity of credentials. Blockchain, a decentralized system for recording and verifying transactions, provides a transparent and immutable log of transactions, while Internet of Things (IoT) devices enable the real-time collection and monitoring of data [4]. Together, these innovations have the capacity to completely transform the traditional system of school accreditation by introducing higher levels of security and reliability. In order to effectively manage large datasets, solutions such as Layer 2 scaling, sharding, or hybrid models could be investigated; however, additional research and innovation are required to combat these obstacles in large-scale applications. The necessity of including robust verification techniques is emphasized by the growing emphasis on connecting educational practices with the Sustainable Development Goals (SDGs), specifically Goal 4: Quality Education. Given the dynamic nature of the global education landscape, there is an urgent requirement for innovative solutions that not only streamline certification processes but also make a positive impact on sustainable development objectives. Integrating blockchain and IoT technology into certification systems aligns with SDG 4 by enabling equitable and inclusive access to excellent education and lifelong learning opportunities. Moreover, it facilitates the attainment of other interrelated goals, such as SDG 9: Industry, Innovation, and Infrastructure, by fostering technological advancement and efficient infrastructure [2].

These articles analyse the ability of blockchain technology and IoT to verify educational credentials, with a particular focus on how these technologies might be used to strengthen and enhance the Sustainable Development Goals (SDGs). The paper examines the limitations of traditional certification methods, evaluates the advantages of integrating blockchain and IoT technologies, and presents case studies and theoretical models that illustrate their impact on educational certification processes. This research aims to provide valuable insights on how educational institutions and policymakers may effectively leverage these innovations to establish safer, more transparent, and sustainable educational practices. It will achieve this by conducting a comprehensive evaluation of these technologies and their correlation with the Sustainable Development Goals (SDGs) [2].

2 Literature Review

Incorporating blockchain technology with the Internet of Things (IoT) in educational certification procedures is an innovative approach to address the challenges of validating and guaranteeing the authenticity of academic certifications. This literature review examines notable research and progress in the field, with a special focus on the application of blockchain and IoT in education. Additionally, it examines the connection between these technologies and the Sustainable Development Goals (SDGs), as well as the possible influence on certification systems.

2.1 The Significance of IoT in Educational Verification

Internet of Things (IoT) devices provide the collection and transmission of real-time data, which may be used to monitor and verify educational activities and achievements. IoT sensors and devices can monitor and document student attendance, level of engagement, and academic performance in educational settings. Afterwards, this data may be incorporated into blockchain systems to offer a comprehensive and accurate record of an individual's educational advancement. Internet of Things (IoT) technology may enhance the granularity and accuracy of educational data [3]. When combined with blockchain technology, this integration provides a robust and dependable approach to verifying academic qualifications [13].

2.2 The Application of Blockchain Technology in Educational Certification

Blockchain technology, renowned for its decentralized and immutable ledger system, has been proposed as a means to enhance the security and transparency of educational diplomas. Blockchain offers a secure and immutable method for recording transactions, making it well-suited for the certification process [5]. This technology allows for the creation of digital certificates that can be easily verified and are extremely resistant to fraudulent activities. In their 2015 study, Wright and De Filippi highlight the significant impact of blockchain's inherent features, including decentralization, transparency, and immutability, in successfully addressing the limitations of traditional certification methods. These encompass issues related to forged credentials and manipulation of data [10].

2.3 Conformity with Sustainable Development Goals

The integration of blockchain and IoT technologies with the Sustainable Development Goals (SDGs) is particularly relevant to Goal 4: Quality Education. Goal 4 of the Sustainable Development Agenda, as declared by the UN in 2015, is to ensure that all people have equal and comprehensive access to high-quality education and to promote opportunities for lifelong learning. Blockchain and IoT technologies improve the accessibility and reliability of educational credentials, hence helping this goal. These technologies can improve transparency and equity in the education system, hence advancing the overall objectives of SDG 4 [6]. Furthermore, the use of these technologies aligns with SDG 9: Industry, Innovation, and Infrastructure, as it fosters technological advancements and enhances the effectiveness of infrastructure [9] (Fig. 1).

3 Obstacles and Possibilities

While the combination of blockchain and IoT in educational certification shows potential, it also faces several challenges. A significant issue is the scalability of blockchain systems and their ability to handle large volumes of certification data [11]. Furthermore, there are concerns regarding privacy and data security, particularly regarding the collection and storage of personal educational data [12]. In order to address these issues, it is

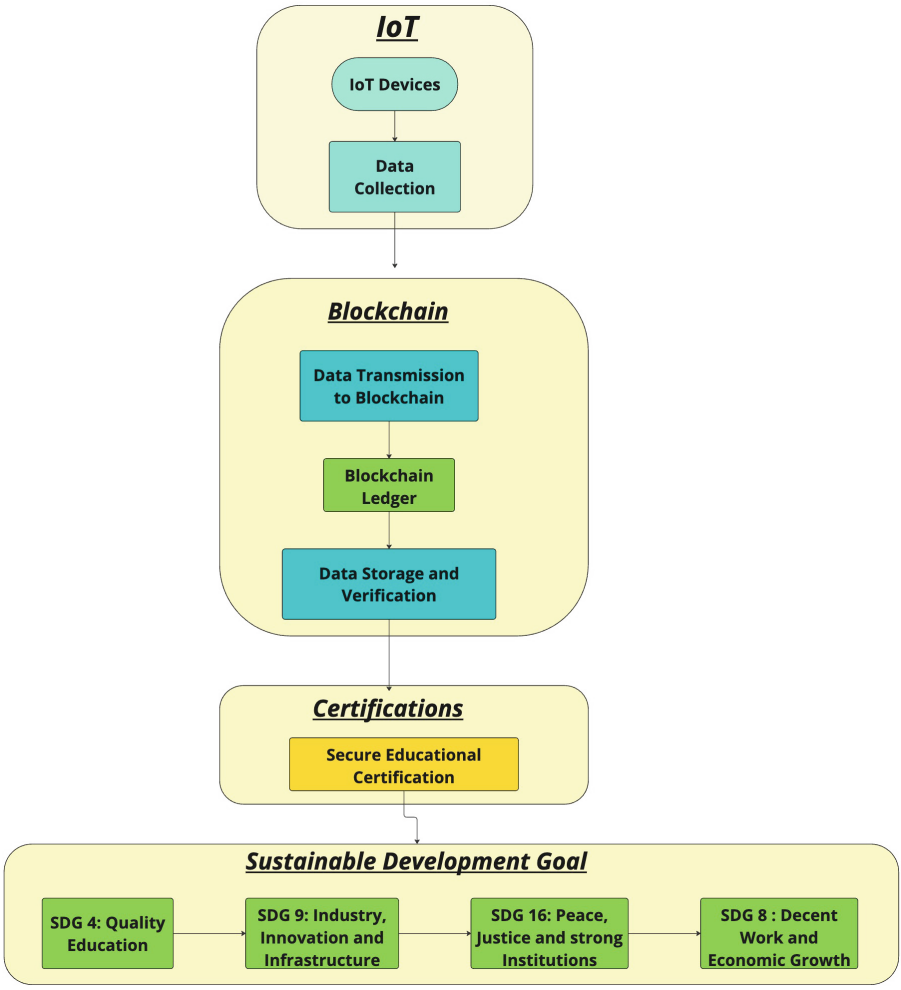


Fig. 1. Overview of the connecting the dots by using different technologies

imperative to engage in ongoing studies and developments to ensure the effective and secure integration of blockchain and IoT technologies. Many Techniques can improve that data security with IOT integration. For Calculations: homomorphic cryptography and strong encryption for data sending and at rest, these ways can be implemented. Only authorised users may access sensitive data using role-based access control (RBAC) and decentralized identity systems. The use of smart contracts to enforce data-sharing regulations and restrict access may increase security in permissioned blockchains. User training on data security best practices as well as transparent data rules are essential, as are security audits and GDPR and FERPA compliance.

4 Analysis of Specific Instances and Practical Implementations

In the subject of teacher certification, there are a number of instances that demonstrate how blockchain technology and the Internet of Things might be put to practical use. One of these institutions is the University of Malta, which has created a system that is based on blockchain technology for the purpose of authenticating degrees and issuing graduation certificates. This technology has the potential to improve the reliability and efficiency of certification operations. In addition, research and pilot projects have proved the use of Internet of Things devices to track the development of students and quickly incorporate this data into blockchain systems [11].

5 Methodology (Hypothetical Case Study on a Fictious Institute)

5.1 Introduction

The aim of this approach is to provide a framework for utilizing blockchain technology to verify educational credentials via the Internet of Things (IoT), ensuring adherence to Sustainable Development Goals (SDGs). The approach involves many stages, such as system design, implementation, testing, and evaluation. These procedures are demonstrated by a case study carried out at a fictional institution known as ENTech institution (ETU).

6 System Design

6.1 Requirements Analysis

The stakeholders encompass the ETU administration, students, academics, employers, accrediting organizations, and the Ministry of Education [13].

Requirements: Ensuring the security and verifiability of educational qualifications, streamlining verification operations, enhancing data integrity, and reducing instances of fraud.

The applicable SDG targets for this topic are as follows: The four Sustainable Development Goals (SDGs) mentioned are as follows: SDG 4, which specifically targets the provision of high-quality education; SDG 9, which highlights the significance of innovation; SDG 10, which advocates for inclusivity; and SDG 8, which attempts to facilitate economic growth.

6.2 Blockchain and IoT Integration

The chosen blockchain platform is Hyperledger Fabric due to its permissioned structure and high level of security suitable for corporate use. Internet of Things (IoT) devices include RFID-enabled student ID cards, smart attendance systems, and secure digital badges.

Architecture: Internet of Things (IoT) devices collect and transmit data (such as attendance and exam results) to the blockchain. Smart contracts validate and preserve certification data, guaranteeing records that cannot be tampered with [1].

6.3 Smart Contract Development

Smart contracts provide certificates based on pre-established criteria, such as the successful completion of a course, attendance, and grades.

Verification: Smart contracts verify the authenticity of certifications upon request from employers or other entities.

Revocation: Certifications may be withdrawn if judged necessary, as long as there is valid authorization.

7 Implementation

7.1 Blockchain Network Setup

Network Configuration: Set up an isolated Hyperledger Fabric network that consists of nodes controlled by ETU, the Ministry of Education, and an external auditing agency.

Security Protocols: Implement robust security measures, including the use of encrypted communications and the enforcement of access limitations.

Smart Contracts: Create contracts that enable the issuance, verification, and cancellation of certificates.

7.2 IoT Device Deployment

Deploy RFID-enabled student ID cards and smart attendance systems in classrooms and examination halls.

Data Capture: Configure Internet of Things (IoT) devices to gather relevant data (such as attendance and test results) and transmit it securely to the blockchain [4].

Communication Channels: Establish secure connections between IoT devices and the blockchain network by leveraging IoT gateways.

7.3 Data Storage and Management

Employ the Interplanetary File System (IPFS) to store large data collections, such as academic transcripts and project reports, using a decentralized method [14].

Ensure data privacy by implementing data encryption and privacy-preserving techniques to comply with GDPR and other regulatory obligations.

8 Testing

8.1 Functional Testing

Smart Contracts are prototype agreements designed for the exact issue, authentication, and annulment of certifications.

connectivity: Ensure seamless connectivity between Internet of Things (IoT) devices and the blockchain network.

Comprehensive Testing: Conduct meticulous evaluations of the whole certification process.

8.2 Security Testing

Vulnerability Assessment: Identify and resolve potential security vulnerabilities.

Perform resilience testing to assess the system's capacity to endure cyber-attacks and data breaches.

Encryption: Guarantee the execution of data encryption and the utilization of secure key management techniques.

Utilizing strong encryption protocols (e.g. AES, TLS) can be implemented to safeguard data, while end-to-end encryption ensure the data security from source to destination. Strong authentication methods, such as Blockchain based identity systems and public key infrastructure (PKI) can prevent unauthorised access. Real-Time surveillance and machine learning algorithms can detect inconsistencies and suspicious activities, which ensure a proactive response to threats.

8.3 Performance Testing

Scalability refers to the evaluation of the network's capacity to effectively manage different levels of demand.

Quantify the time it takes for the transmission of IoT data and the processing of blockchain transactions.

Optimization: Improve system performance to achieve optimal outcomes in real-world scenarios.

9 Evaluation

9.1 Alignment with Sustainable Development Goals (SDGs)

Evaluation: Evaluate the level of assistance provided by the system for the Sustainable Development Goals (SDGs), with a specific focus on the areas of quality education, innovation, inclusion, and economic development.

Request comments from ETU stakeholders about the system's influence on educational certification.

9.2 Pilot Study

Attendees: A select cohort of ETU students and faculty members might be chosen to serve as a pilot group.

Data Collection: Data may be gathered on the effectiveness, efficiency, and user satisfaction of the system.

Analysis: A comprehensive evaluation must be conducted on the pilot results to identify the strengths and areas that need improvement.

9.3 Continuous Improvement

Refinement is the process of enhancing and adjusting a system via meticulous inspection and feedback.

Make necessary revisions to smart contracts and IoT settings.

Continuous monitoring involves consistently observing the performance of the system and making modest improvements.

In General, Educational institutes might find it difficult to use blockchain and IoT Technologies. Usually, continuous technical training, hiring competent employees and infrastructural investments are overlooked. This lack of attention on Technological integration might prevent institutions from properly using blockchain and IoT, emphasizing the need for complete support and resources (Fig. 2).

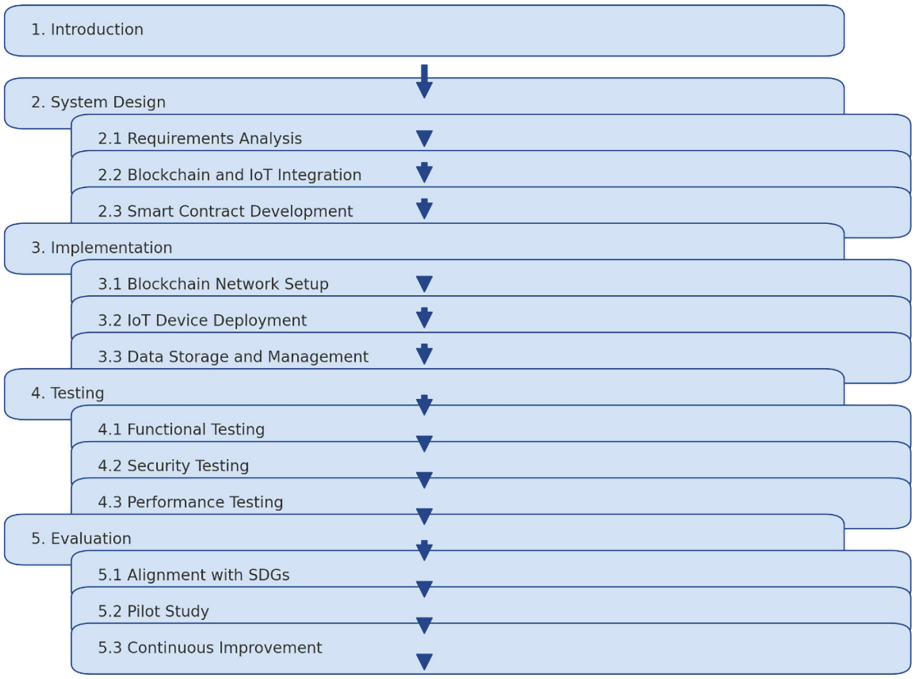


Fig. 2. Analysis: This study provides an overview of ENTech University (ETU Hypothetical).

ETU, a university with a moderate student population and a particular focus on technology and sustainability, opted to trial a system that integrates blockchain and IoT technologies for managing educational credentials. The aim was to enhance the trustworthiness and verifiability of academic records, while aligning with the Sustainable Development Goals (SDGs) [14].

Implementation

The engineering department at ETU has introduced student ID cards featuring RFID technology and smart attendance systems.

The blockchain network, leveraging Hyperledger Fabric, was created with nodes supervised by ETU, the Ministry of Education, and an external auditor.

Smart contracts were developed to optimize the issuance and authentication of certificates through automation.

Preliminary Results

Effectiveness: The introduction of the new system led to a significant reduction in the amount of time required for certification identification, decreasing it from several days to just a few minutes.

Security: The blockchain ensures the integrity of records, enhancing trust among employers and certifying bodies.

Scalability: The system effectively handled larger amounts of data, demonstrating its appropriateness for application throughout the whole university.

The ETU emphasized improvements in the quality and innovation of education, which support the broader objectives of the Sustainable Development Goals (SDGs).

Suggestions for enhancement and refinement:

User Experience: The system was regarded as user-friendly and transparent by both students and teachers.

Data Privacy: Successfully attained complete adherence to data protection regulations, with no recorded instances of breaches.

Future Enhancements: The plans entail incorporating additional Internet of Things (IoT) devices and expanding the system to encompass other departments.

By following this methodology and employing the ETU case study, educational institutions may effectively implement blockchain and IoT technologies to enhance certification processes and contribute to the achievement of Sustainable Development Goals.

10 Advantages

Integrating blockchain technology and the Internet of Things (IoT) into educational certification systems offers several benefits, particularly in enhancing the dependability, efficiency, and alignment of these systems with Sustainable Development Goals (SDGs). The following sections outline the main advantages:

1. **Enhanced security protocols and fraud prevention methods**

   The immutable and distributed nature of blockchain technology ensures the security and integrity of educational certificates, rendering them impervious to alteration. Each certification is recorded as a block in a chain, making it highly challenging to alter or forge credentials without being noticed. By bolstering the overall credibility of academic degrees and mitigating the risk of fraudulent activities, this adds to an elevated level of dependability [5, 14].

   The Internet of Things (IoT) allows for the real-time monitoring and recording of educational activities, providing an additional layer of verification. IoT sensors possess the capacity to observe and document attendance, engagement, and achievement, all of which are later saved on the blockchain. This link ensures that certifications are based on accurate and up-to-date information, hence minimizing the risk of false claims.

2. **Improved transparency and verification**

   Blockchain technology facilitates the development of a distributed ledger that guarantees transparent and verifiable documentation of educational diplomas. Stakeholders, including companies and educational institutions, have the ability to directly acquire and verify credentials, therefore reducing the necessity of intermediaries. This leads to a verification approach that is both more efficient and trustworthy [10].

   The Internet of Things (IoT): IoT devices enhance transparency by continuously collecting and transmitting data related to educational activities. Real-time data collection allows for immediate verification of achievements and progress, providing a clear and accurate record of a student's performance [1].

3. **Improved efficiency and reduced costs**

   Blockchain technology provides a more efficient and cost-effective alternative to conventional certification processes, which frequently depend on several intermediaries and paper-based systems. Blockchain technology simplifies this process by automating verification and reducing reliance on intermediaries. Consequently, this results in faster processing times and lower administrative costs [6].

   The Internet of Things (IoT) enables the automated collection and validation of data in educational systems, hence removing the necessity for manual record-keeping and assessment by humans. This automation streamlines administrative tasks, improving the efficiency and cost-effectiveness of the certification process.

4. **Support for the Sustainable Development Goals (SDGs)**

   Goal 4 - Quality Education: The utilization of blockchain and IoT technologies enhances the dependability and accessibility of educational qualifications, hence aiding the fulfilment of the Sustainable Development Goal (SDG). 4. The use of these technologies ensures that diplomas properly reflect real learning results and capacities, therefore promoting equitable and inclusive high-quality education [9].

   Goal 9 - Industry, Innovation, and Infrastructure: The integration of blockchain and IoT represents a significant advancement in educational technology and infrastructure. It facilitates the development of more advanced and efficient educational frameworks by encouraging innovation in certification systems [6].

5. **Enhanced learner autonomy and the cultivation of lifelong learning skills.**

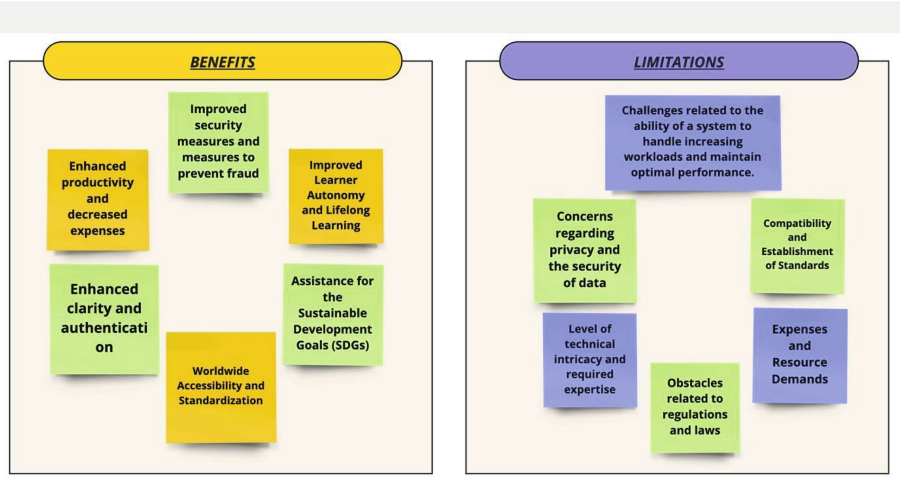
   Blockchain technology empowers learners to exert more control over their educational records by granting them direct access to their credentials stored on a blockchain. This allows individuals to easily convey their qualifications to potential employers or educational institutions, so facilitating smooth transitions in their academic and professional paths [13].

   The Internet of Things (IoT) allows for continuous monitoring and documenting of educational development through the use of IoT devices. This promotes continuous learning by providing in-depth understanding of learners' achievements and areas for improvement. By using data, this method empowers learners and educators to tailor learning experiences according to individual needs and goals.

6. **Global Accessibility and Standardization**

The decentralized and internationally accessible nature of blockchain allows for the standardization of educational credentials across several nations and organizations. This fosters international recognition and reduces discrepancies in certification protocols, hence streamlining global mobility and collaboration [7]. The Internet of Things (IoT)

allows for the placement of devices in various educational environments worldwide, assuring dependable methods for gathering and verifying data. This approach's extensive implementation fosters the utilization of standardized certification techniques and enhances the credibility of certificates on a global scale.



11 Limitations

Limitations or challenges arise when integrating blockchain technology and the Internet of Things (IoT) into educational certification systems, despite the numerous advantages they offer. To fully leverage the potential of these technologies in transforming educational certification systems, it is crucial to address these limitations.

1. **Challenges pertaining to the capacity of a system to manage growing workloads and sustain optimal performance**

   The scalability of blockchain technology is its main constraint. Blockchain systems, particularly those utilizing Proof of Work (PoW) consensus methods, may have performance constraints when handling a substantial volume of transactions. As a result, this might lead to longer processing times and increased costs for maintaining the blockchain network [11]. Efficiently scaling blockchain technology to accommodate the vast amount of educational data and certification transactions remains a significant challenge. Layer 2 scaling technologies like state channels and plasma enable off-chain transactions, reducing the main network. Splitting allows smaller portions to handle transactions independently, increasing bandwidth. Efficient consensus mechanisms like Proof of Stake (PoS) and Byzantine Fault Tolerance (BFT) speed up transactions, while data collection methods like batch processing and off chain storage reduce on chain transactions, speeding up real-time data processing.

   The use of IoT devices to collect educational data may lead to scalability issues. Managing and consolidating data from a wide range of IoT devices may be complex and may need substantial infrastructure and resources. In addition, ensuring a uniform and reliable performance across a diverse array of IoT devices may provide challenges.

2. **Privacy and data security concerns**

   Blockchain technology provides a secure and immutable ledger of transactions. Nevertheless, the system's openness may raise concerns over the safeguarding of personal data. If the management of personal educational data kept on the blockchain is not sufficiently regulated, it might potentially be accessible to unauthorized entities. Striking a balance between safeguarding sensitive information and reaping the benefits of transparency is a complex issue [7, 12]. The Internet of Things (IoT) entails the gathering and transfer of personal and sensitive educational data via IoT devices, rendering them vulnerable to security breaches. Ensuring the security and integrity of instructional material requires securing the transfer of data from IoT devices and protecting against cyber-attacks [12].

3. **Compatibility and Standardization**

   Blockchain platforms may face interoperability issues as a result of using diverse protocols and standards. In order to ensure global recognition and acceptance of educational diplomas, it is imperative to adopt a uniform approach to use blockchain technology that is consistent across various institutions and nations [6].

   The incorporation of diverse Internet of Things (IoT) devices and systems may lead to compatibility obstacles. Establishing standardized IoT protocols and ensuring interoperability across devices and platforms is crucial for seamless data collection and integration.

4. **The expenses and Resource Requirements**

   Implementing and maintaining a blockchain might result in substantial costs, particularly for enterprises with limited financial resources. According to Wright and De Filippi [10], certain educational institutions may consider the initial setup, continuing maintenance, and operational expenses of using blockchain technology to be excessively high.

   Deploying and supervising a network of Internet of Things (IoT) devices requires significant expenditure on hardware, software, and infrastructure. Moreover, the process of maintaining and enhancing this equipment may lead to ongoing costs and resource needs. Initially, open-source and cloud-based technology can save the cost, while government grants and tech companies collaborations can help financially. Associations and shared services enable institutions to combine resources and inexpensive training programs can develop knowledge without affecting budgets. Increased energy consumption can also be the one of the limitations. The energy consumption of blockchain can be decreased in several ways, especially while processing the large amount of IoT data. The optimisation of resource, protocol updates and lightweight blockchain for IoT applications, which can ensure the viability of blockchain systems while processing the large volume if data. Furthermore, Byzantine Fault Tolerance (BFT) algorithms enhance sufficiency and minimise energy consumption. Above all, Blockchain nodes can use renewable energy sources such as wind turbines, hydropower, and solar energy.

5. **Degree of technological complexity and knowledge necessary**

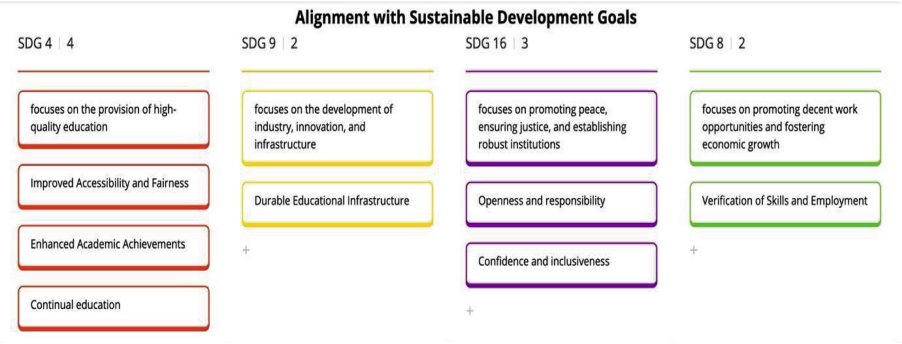
   Implementing blockchain technology requires specialized technical expertise and experience. Educational institutions may have challenges in acquiring the necessary skills and resources to create, administer, and supervise certification systems utilizing blockchain technology [5].

Incorporating IoT devices into educational systems involves complex technological aspects such device setup, data integration, and system upkeep. Organizations may need to commit money towards training and development in order to effectively use the possibilities of IoT technology.

6. **Challenges pertaining to rules and legislation**

   Implementing blockchain technology for educational certificates may encounter regulatory and legal impediments. Data privacy, digital credentials, and blockchain technology may be governed by distinct regulations in different countries and regions. Ensuring compliance with many legal frameworks is of utmost importance [3].

IoT devices and data collection must comply with data protection laws and standards. Organizations must skilfully navigate complex legal duties to ensure that the use of IoT technology aligns with privacy laws and regulations. Regional frameworks should be examined, and compliance guidelines must be examined through legal studies. Educational trust and uniformity are fostered by universal standards and certification programs. Last but not the least, the implementation of educational technology can be simplified by the use of online training events and tools, which can improve legal knowledge.



12 Alignment with Sustainable Development Goals

Integrating blockchain and IoT technologies into school certification systems offers explicit assistance for certain Sustainable Development Goals (SDGs) established by the United Nations. This section outlines the main approaches by which these technologies help achieve these worldwide goals.

13 SDG 4 is Centred on the Delivery of Education that is of Superior Quality

Ensure the provision of inclusive and equitable education of superior quality and promote ongoing opportunities for lifelong learning for all individuals.

13.1 Enhanced Accessibility and Equity

The integration of blockchain and IoT technologies facilitates the democratization of educational credentials by building a transparent and globally accessible system that can be verified. This ensures that individuals from diverse socio-cultural backgrounds may get recognition for their educational achievements, regardless of geographical or financial barriers [9].

13.2 Improved Academic Performance

IoT devices can constantly monitor and measure student engagement and performance in real-time. This allows educators to tailor interventions and assistance based on the individual needs of each student. This personalized approach enhances learning outcomes and ensures that each student could flourish [13].

13.3 Lifelong Learning

Blockchain has the capacity to maintain educational data over an individual's whole lifespan, ensuring their easy accessibility and verifiability. This facilitates continuous learning and skill development, since individuals may easily add new certifications to their digital profiles as they progress [8].

14 SDG 9 is Centred Around the Advancement of Industry, Innovation, and Infrastructure

Develop durable structures, promote inclusive and sustainable industrialization, and foster innovation. Technological innovation is the act of developing and applying novel or enhanced technologies that result in substantial progress and transformations across several domains.

Integrating blockchain and IoT technologies into educational institutions represents a significant advancement in technology. It encourages the adoption of cutting-edge technology in the education sector, fostering a climate of creativity and modernity [6].

14.1 Resilient Educational Infrastructure

The decentralized nature of blockchain and the robust data collection capabilities of IoT contribute to the creation of resilient and efficient educational infrastructures. These technologies ensure the secure storage, easy access, and protection against disruptions or tampering of educational data [3].

15 SDG 16 is Cantered Around the Promotion of Peace, the Guarantee of Justice, and the Establishment of Strong Institutions

Promote the advancement of peaceful and inclusive societies in order to guarantee sustainable development, assure equal access to justice for everyone, and promote effective, transparent, and inclusive institutions at every level.

15.1 Transparency and Accountability

The transparent ledger architecture of blockchain improves accountability in educational certification systems. The use of this system provides a clear and unchangeable record of credentials, reducing the likelihood of dishonesty and ensuring that businesses maintain high standards of integrity and reliability [5].

15.2 Assurance and Comprehensiveness

Blockchain and IoT technologies install trust among stakeholders, including students, educational institutions, and businesses, by providing a reliable and verifiable approach to educational certification. This incorporation fosters an equitable and unbiased educational setting.

16 SDG 8 is to Advance the Creation of Quality Employment Opportunities and Stimulate Sustainable Economic Expansion

Promote sustainable economic growth, inclusive job opportunities, and favourable work circumstances for all individuals.

16.1 Skills and Employment Verification

Blockchain-based educational certificates provide a dependable and easily confirmable record of skills and certifications. This facilitates organizations in identifying individuals with the necessary skills, so enhancing their prospects of securing work and promoting the availability of favourable job opportunities [10].

Economic growth is the expansion of a nation's output of goods and services within a certain timeframe. The growth rate of the Gross Domestic Product (GDP) is frequently used as a measure. These technologies ensure the dependability and verifiability of educational qualifications, hence fostering the development of a skilled workforce. Consequently, this results in sustained economic expansion and the creation of lucrative employment opportunities.

17 Conclusion

A comprehensive and diverse investigation is conducted to explore the possible improvements that these technologies might offer to educational certification procedures and their alignment with the Sustainable Development Goals (SDGs). Blockchain and IoT provide substantial prospects for enhancing educational certification, although they also present hurdles such as scalability, privacy concerns, interoperability issues, economic ramifications, technological intricacy, and legal considerations. Effectively managing the complexities of implementing these technologies and attaining durable and effective solutions requires meticulous focus and oversight of these variables. The use of blockchain and IoT technology into educational certification systems strongly bolsters

several Sustainable Development Goals (SDGs). These technologies improve the accuracy, availability, and dependability of educational qualifications, therefore promoting the objectives of delivering high-quality education, encouraging creativity, ensuring equal opportunities and accountability, and contributing to economic development. By adopting these technology advancements, educational institutions and governments may make substantial strides in achieving the Sustainable Development Goals (SDGs) and constructing a future that is both ecologically sustainable and equitable.

In order to fully harness the capabilities of blockchain and IoT in the field of education, it is imperative to do comprehensive study and employ efficient solutions to overcome current obstacles. To effectively navigate the difficulties of applying these technologies and achieve long-lasting improvements in educational certification, anyone interested in the topic should understand and resolve the limits associated with them.

References

1. Rustemi, F.D., Atanasovski, V., Risteski, A.: Enhancing Academic Credentials: The Synergy of Blockchain and Artificial Intelligence. 2024 7th International Balkan Conference on Communications and Networking (BalkanCom), pp. 206–211. Ljubljana, Slovenia (2024). https://doi.org/10.1109/BalkanCom61808.2024.10557185. keywords: {Reviews; Education; Smart contracts; Authentication; Blockchains; Security; Artificial intelligence; Artificial Intelligence (AI); blockchain system; machine learning; diploma generation and verification; security; transparency}
2. Could Blockchain be the key that unlock the SDGs? (https://www.weforum.org/agenda/2021/10/why-blockchain-is-the-key-to-meeting-the-sdgs/)
3. Xue, H., Guo, K.: The key technologies of blockchain and the design of smart education platform. Int. J. Educ. Humanit. **8**(2), 90–95 (2023)
4. Shakan, Y., Kumalakov, B., Mutanov, G., Mamykova, Z., Kistaubayev, Y.: Verification of university student and graduate data using blockchain technology. International Journal of Computers Communications & Control **16**(5) (2021)
5. Kshetri, N.: 1 Blockchain's roles in meeting key supply chain management objectives. Int. J. Inf. Manage. **39**, 80–89 (2018)
6. Anand, A., Nair, K.: Blockchain technology: Applications and challenges. IEEE Access **7**, 95155–95166 (2019)
7. Crosby, M., Pattanayak, P., Verma, S., Kalyanaraman, V.: Blockchain technology: Beyond bitcoin. Applied Innovation Review **2**, 6–10 (2016)
8. Tapscott, D., Tapscott, A.: Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world. Penguin Random House (2016)
9. United Nations: Transforming our world: The 2030 Agenda for Sustainable Development (2015). Retrieved from UN SDGs website
10. Wright, A., De Filippi, P.: Decentralized blockchain technology and the rise of lex cryptographia. SSRN Electronic Journal (2015)
11. Yli-Huumo, J., Ko, D., Choi, S., Park, S., Smolander, K.: Where is current research on blockchain technology? —a systematic review. PLoS ONE **11**(10), e0163477 (2016)
12. Zyskind, G., Nathan, O., Pentland, A.: Decentralizing privacy: using blockchain to protect personal data. IEEE Sec. Privacy Works. **2015**, 180–184 (2015)
13. Khan, A., et al.: Educational blockchain: a secure degree attestation and verification traceability architecture for higher education commission. Applied Sciences **11**(22), 109172021. https://doi.org/10.3390/app112210917

14. Blockchain in Higher Education: Advancing Security, Verification and Trust in Academic Credentials https://nano-ntp.com/index.php/nano/article/view/596
15. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
16. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4



Federated Learning Approaches Based on Blockchain in Smart Environments

Suyogita Singh[1], Satya Bhushan Verma[1(✉)], V. Sharma[2], Shobhit Mani Tiwari[3], and Anamika Agrawal[1]

[1] Shri Ramswaroop Memorial University, Lucknow, Uttar Pradesh 225003, India
satyabverma1@gmail.com

[2] Computer Science and Engineering, Adjunct Professor, Graphic Era Deemed to Be University, Graphic Era Hill University, Dehradun, India

[3] Faculty of Engineering and Technology, University of Lucknow, Lucknow, Uttar Pradesh, India
tiwari_shobhit@lkouniv.ac.in

Abstract. The robust database system known as blockchain technology is designed to effectively address privacy and security concerns in various fields by securely storing transactions within interconnected blocks. Federated learning (FL) is a promising approach to enhancing data mining accuracy while maintaining information privacy as complex contracts between users and smart devices become more prevalent. During the training and testing phases, the collection and aggregation of sensitive data, such as health records, industrial safety information, and banking details, necessitate high levels of privacy and security in Internet of Things (IoT) sectors like smart cities and industries. Incorporating blockchain technology into intelligent learning practices is crucial for safeguarding information security and privacy. Data science and artificial intelligence research are increasingly relying on blockchain-based FL mechanisms. This study systematically reviews privacy and security concerns in blockchain-based FL by examining scientific databases. The objective is to present a summary of the issue's current state. Blockchain-based FL has grown significantly over the past five years, addressing issues with cancer datasets, industrial equipment, patient healthcare records, image retrieval, and economic data in IoT applications and smart environments.

Keywords: blockchain · federated learning · privacy · security · and the Internet of Things (IoT)

1 Introduction

The Internet of Things (IoT) and other advances in information and communication technologies have brought about significant changes to practically all business strategies in the digital age. Blockchain technology is one innovation that has significantly transformed conventional business models [1, 2]. In a white paper published in 2008, Satoshi Nakamoto introduced Bitcoin. bitcoin operates as a digital currency based on a social

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 192–201, 2025.
https://doi.org/10.1007/978-3-031-91008-1_18

and immutable ledger known as the blockchain. In the present state of blockchain technology is often linked to that of the mid-1990s Internet, when its true value and potential were not yet fully hold. However, in recent years, some countries have recognized the sense of blockchain technology and established research institutes devoted to this field. To unlock the vast potential of blockchain, considerable notice has been directed toward its application in smart environments, including industries, medical systems, and transportation. This has resulted in substantial research efforts, with articles exploring the multiple applications of blockchain. Concurrently, federated learning (FL) has obtained recall as a data analysis technique for its ability to ensure privacy and security, particularly in safety-critical systems such as medical systems and industrial environments. "Smart cities have witnessed the emergence of Federated Learning (FL) as a crucial artificial intelligence technique, as verification by numerous research endeavours. FL, being a specialized machine learning approach, enables the dynamic update of training parameters while preserving datasets on local devices. This is achieved by partitioning data records across designated physical or virtual machines within each federated domain, allowing for rapid and secure dataset training, thereby identifying unstructured and unknown patterns. High accuracy and data privacy are guaranteed by collaborative learning through quick training and testing procedures, which has several benefits for designing smart environments. Blockchain technology has the potential to completely transform data analytics by improving security and privacy while handling vital and sensitive data when integrated with FL systems. Smart environments can effectively support federated learning by utilizing blockchain as a core technology, which emphasizes security and privacy concerns. Notably, a number of studies have looked into smart contract vulnerabilities and attempts to steal cryptocurrency like Ethereum and blockchain technologies. Important factors to take into account are privacy issues like user identification and transaction quantification [18]. Although a number of academics have been working in this area recently, there hasn't been a thorough systematic evaluation of papers about the security and privacy of blockchain research papers that are indexed in ISI databases [19]. Examined blockchain advancements from 2013 to 2018 and suggested blockchain as a means of addressing IoT security issues. Using the Web of Science database, another study concentrated on security-aware blockchain models in power systems. Conti and his research group examined eight years' worth of Bitcoin stories, from 2012 to 2019. In the meantime, Sisi and colleagues focused on blockchain tactics and analysis that took energy into consideration, utilizing databases from Web of Science and Scopus. However, security and privacy concerns have received very little attention in the field of blockchain scientific journals. Considering how serious these issues are, a thorough analysis of blockchain-based FL techniques must be carried out. A thorough evaluation study that classifies the technical aspects of blockchain-based FL Approaches is provided in order to close this gap [16]. This classification includes an analysis of smart environments and a variety of techniques for the statistical and mathematical analysis of scientific articles. Future research decisions are informed by the identification of important concerns, developing trends, and significant personalities in the field of blockchain-based FL methods made possible by this comprehensive analysis of research studies [17].

1.1 Research Techniques and Identifying Significant Information

The applied research methodology, which uses methodical approaches to analyse blockchain-based FL, is described in this section. The statistical population consists of all English-language blockchain-based FL research published between 2018 and 2021 that is indexed in Web of Science. In order to gather the research records, we first found 1,226 items using the same search approach that was used in all study connected to blockchain from 2018 to 2021.Important terms related to the confluence of blockchain and FL have been utilized, as seen in Fig. 1. Afterwards, the subsequent search method has been developed, which includes all research studies that concentrate on security and privacy in blockchain FL. [3] With the use of the previously specified search approach, 1226 research records were found. Following the separation of data related to security and privacy in blockchain FL methods, analyses have been carried out in this section in accordance with the goals and questions of the research, which are stated below [20]. The subsequent statistical and analytical report will address the following questions by the use of inclusion and exclusion criteria:

- What kinds of blockchain have been used in the FL techniques that are currently in use?
- Which FL settings have been studied in relation to smart environments using blockchain technology?
- How has blockchain technology been combined with FL in smart environments?
- Which scholars in field of blockchain-based FL methods receive the most citations?
- How is the state of quantitative research on Quality of Service (QoS) with relation to FL based on blockchain?

2 Federated Learning Techniques Based on Blockchain?

Blockchain organizes data into linked blocks using cryptographic hashes, creating a decentralized storage system free from central authorities. Data is stored in blocks, forming an immutable chain. Each new transaction is shared with all network users and recorded in the ledger. [4] This decentralization makes blockchain ideal for defining authorization policies in data file systems. In this study, we examine key challenges, conduct technical evaluations, and discuss future research opportunities in blockchain-based federated learning (FL).

We categorize blockchain into four types: consortium, public, private, and hybrid. In a public blockchain, every network node can access all the system's data. The chain begins with the genesis block, and each subsequent block is linked to the previous one using cryptographic hashes [21]. Each block includes a header and transactions, with the headers pointing to the preceding block, ensuring the blockchain's immutability. Various consensus mechanisms, like Proof of Work (PoW), Byzantine Fault Tolerance, and the Ripple algorithm, are employed to add new blocks. Bitcoin utilizes PoW, where each node calculates a hash value. Hyperledger technology organizes blocks into smaller, labeled groups to maintain privacy in federated training. We examine existing blockchain technologies, FL environments, models integrating blockchain in FL for smart environments, and relevant implementation and evaluation algorithms [24] (Table 1).



Fig. 1. Paper selection strategy

Table 1. Statistical overview of the blockchain and federated learning methodologies search-based finding report

Keywords	Count of studies prior to applying inclusion and exclusion criteria	Total count of selected papers
Federated learning	2434	154
Blockchain	1632	287
Federated learning + Blockchain	1226	41

2.1 Vertical Federated Learning Techniques Based on Blockchain

To assess vehicle-related data, researchers developed a vertical federated learning technique with an organized blockchain model for training [5, 6]. This hierarchical method was designed to address the unique distribution patterns and privacy concerns of the Internet of Vehicles (IoV) [25]. The approach enhances training quality and facilitates data exchange between vehicles. The blockchain architecture serves as a robust defense against various malicious attacks. Experiments showed that the hierarchical blockchain-based framework is compatible with large-scale vehicle networks, improving the security and reliability of knowledge sharing. Compared to traditional federated learning algorithms, this hierarchical approach demonstrated higher accuracy and better security during information sharing. Another study explored the use of blockchain technology in fog computing to address issues with the Internet of Things (IoT) [22]. Fog computing, a blend of edge and cloud computing, effectively reduces latency, network congestion, and enhances local autonomy. In this model, devices submit local information to fog servers, which then generate global updates. The blockchain stores update pointers while data is saved and block generation is ensured via a distributed hash table (DHT). The findings indicated shorter accuracy times for all evaluation techniques, improving overall system performance. The authors aim to optimize the performance vs. privacy trade-off and incorporate Markov decision processes and game theory for more optimal computations in future enhancements.

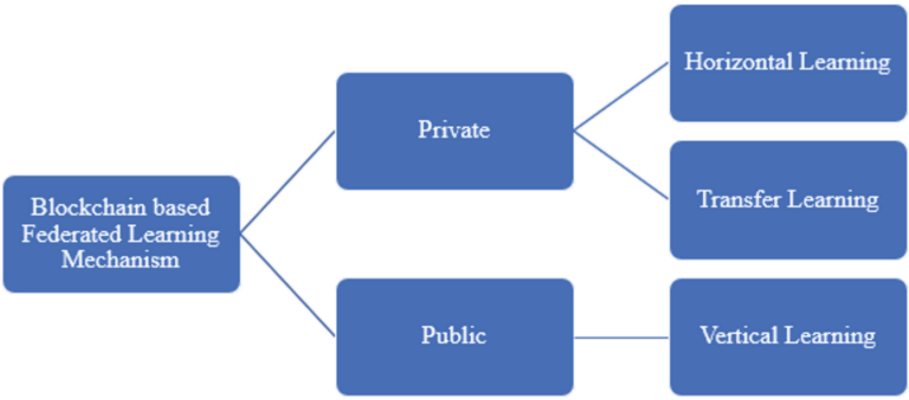


Fig. 2. Comprehensive taxonomy on blockchain-based FL mechanism

The authors of a different study talked about the use of blockchain technology in fog computing and how it might be used to solve Internet of Things (IoT)-related problems. Among other issues, fog computing effectively lowers latency, network congestion, and local autonomy. It's referred to as a blend of edge and cloud computing [25]. This paradigm states that devices send locally accessible data to fog servers, which then generate updates for the worldwide community. While a distributed hash table (DHT) table secures block creation and stores data, the blockchain just keeps update pointers [26]. The outcomes demonstrated that all assessment techniques had shorter accuracy times, which improved overall system performance. In order to accommodate novel scenarios, the authors hope to enhance the model by maximizing the trade-off between efficiency and privacy. In order to accomplish more optimal computations, they also intend to apply the Markov decision process and game theory [23].

2.2 Horizontal Federated Learning Techniques Based on Blockchain

The authors [7] introduced Federated Learning (FL) as a technique to enhance system performance while safeguarding sensitive data and boosting artificial intelligence security. They utilized a combination of local and global blockchain methods to achieve this. Device-to-Device (D2D) communication reduces processing time and streamlines operations, while timestamps record upcoming procedure levels [23]. The global approach mitigates system vulnerabilities, enhancing overall efficiency while maintaining privacy and validation. Future plans include optimizing the model for increased security and functionality by protecting its dynamic components from threats.

In another study, [8] the authors proposed an innovative FL architecture using blockchain technology. This design features a participant selection algorithm and a numerical evaluation component, enabling FL to select devices for each training cycle. This dual-component design addresses security and vulnerability concerns during FL model transmission. The proposed algorithm outperformed others in model update efficiency by integrating blockchain with FL. Future work will focus on creating a more effective selection process to further improve the blockchain-supported FL framework.

Additionally, the authors [9] presented a blockchain-based defense technology aimed at enhancing FL system security. This method protects against threats like model poisoning and streamlines the learning process. The FL implementation used the MNIST dataset, comprising 60,000 handwritten digit images and 10,000 verification photos, with simulations run using Keras and TensorFlow. The proposed algorithm demonstrated improved speed, security, and convergence, enhancing FL security.

The authors [10] proposed a robust, decentralized framework based on blockchain technology within federated learning. This system employs Gaussian Process (GP) hyperparameter optimization, a reward-based deposit mechanism, Ethereum for decentralization, homomorphic encryption, and differential privacy algorithms to ensure safety and confidentiality while enhancing financial viability. To optimize the learning of sequential tasks, Elastic Weight Consolidation was used. The framework's effectiveness was evaluated using a 5×5 involution layer neural network on the MNIST dataset, resulting in improved training outcomes with strong safety and privacy features.

In a related paper [11], the authors developed a blockchain-based FL framework that offers a reliable and secure alternative to centralized FL, which often encounters numerous privacy and security challenges during raw data collection. In this system, miners verify updated models from distributed vehicles, and these verified models are recorded in the blockchain. Additionally, noise is added to the blockchain-based FL process to further enhance security. The authors' future work aims to improve accuracy and efficiency by exploring potential benefits for traffic control and law enforcement systems.

3 Federated Transfer Learning Techniques Based on Blockchain

The authors [12] proposed a method called "FL chain" to enhance the data security of Federated Learning. This approach uses a model called "The Global Model State" and the concept of channels within a blockchain network. The FL chain is implemented within a blockchain network powered by Mobile Edge Computing (MEC) and incorporates features such as Device Registration, Model Updates, and Model Consensus. The FL chain platform creates an Exclusive Channel for each model, facilitating machine learning on global models. These models are securely stored on a distributed server (blockchain) rather than a single data set, using a Merkle Patricia Tree for storage. However, a disadvantage of this platform is that data transit over the blockchain network relies on the integrity of data publisher (user) devices at the network's edge. Future improvements aim to simplify storage platform requirements, reduce latency, and optimize data processing. Additionally, the authors implemented a system for data miner nodes and devices within the FL chain.

In a separate paper, the authors presented a distributed machine learning method known as Federated Learning (FL), which allows ML models to be trained on decentralized private data. FL saves network bandwidth and protects data privacy by not transferring large amounts of training data since ML models are trained locally. FL can be used in various industries, such as predicting hospital stays and patient outcomes, improving core and network edge activities, and providing predictive text recommendations (such as Google Keyboard). The authors created two FL clients and an FL server

to illustrate a scenario. They developed a model using three identical nodes on an HP server to establish a channel. The results showed that the blockchain protocol establishes a secure channel for communication between the server and the clients and that the FL-trained model nearly matches the accuracy of centralized training.

The author [13] suggested using Multi-Agent Systems (MAS) to divide tasks into distinct entities for quick completion. In MAS, encryption techniques and blockchain technology ensure data security. The study focuses on a novel architecture called "Learning of Medical Things" (LoMT) based on MAS. The LoMT model consists of agents and architecture, with the design based on factor creation and cloud framework connections. The agents represent autonomous entities interacting with their environment. The model includes three types of agents: the Learning Agent (LA), the Data Management Agent (DMA), and the Indirect Agent (IA). The DMA handles medical data, the IA categorizes information in response to DMA requests, and the LA works with labeled database entries. Experiments measured the agents' performance in various scenarios using accuracy and processing time.

4 Discussion of the Technical Evaluation

This section delves into an analysis and technical assessment of current blockchain-based Federated Learning (FL) strategies. We address the concerns and propose derived solutions based on a combination of statistical and technical evaluations (Fig. 3).

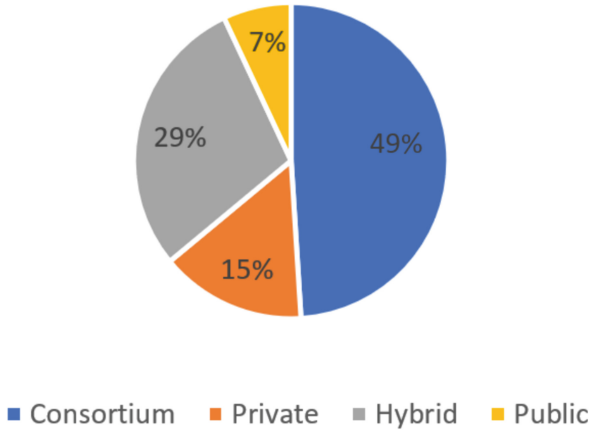


Fig. 3. Statistical view on blockchain technologies in federated learning concept

4.1 Which FL Implementation uses Blockchain Technology in a Smart Environment?

Table 2 shows the two levels into which FL implementations have been divided: public and private. Both of these strategies take privacy into account and cover FL's horizontal,

vertical, and transfer learning techniques. Interestingly, in Fig. 2 i it seems that the field's primary focus is on the implementation of private FL, especially when it comes to blockchain technology [14, 15]. This emphasizes how important privacy concerns are to take into account when incorporating blockchain technology into intelligent settings [26].

Table 2. List of applied federated learning algorithms with full name

Abbreviation	Full name
CFL	Chain Federated learning
FGFL	Fine-Grained Federated Learning
AFL	Auditable Federated Learning
CEFL	Communication Efficient Federated Learning
RFL	Reward Federated Learning
RFL	Reputation-Aware Federated Learning
RAFL	Reliability-aware Federated Learning
IFL	Incentive-aware Federated Learning

5 Conclusion

This study examined the integration of Federated Learning (FL) and blockchain technology in smart environments, focusing on advancements and modifications over the past four years. A review of 1226 research publications using FL was conducted to understand the co-evolution of these two domains, with blockchain studies being a key area of focus. The Scopus database was chosen for this review due to its extensive coverage and frequent use in similar studies. However, this choice may have excluded research not indexed by Scopus. Future investigations should consider additional databases such as ISI Web of Science to enhance inclusivity. To ensure accuracy and consistency, only journal articles from the database were used. Future research could include other types of publications, like book chapters and conference papers, to provide a more comprehensive understanding of the topic. The analytical results highlighted numerous unresolved problems and challenges in applying blockchain technology to FL for unstructured pattern prediction. Experimental results underscored the need to address gaps and new issues in lightweight blockchain approaches. Researchers are encouraged to explore the combination of evolutionary techniques, meta-heuristic algorithms, and TensorFlow processes in FL contexts.

Additionally, classifying vertical and horizontal FL processes based on the type of dataset can guide researchers towards the best methods to improve accuracy during sequential training. The medical and healthcare sectors are particularly critical for leveraging FL to enhance accuracy, protect privacy, and reduce error rates.

References

1. Khalid, U., Asim, M., Baker, T., Hung, P.C.K., Tariq, M.A., Rafferty, L.: A decentralized lightweight blockchain-based authentication mechanism for IoT systems. Cluster Computer. **23**(3), 2067–2087 (2020). https://doi.org/10.1007/s10586-020-03058-6
2. Nakamoto, S.: Re: bitcoin P2P e-cash paper. Cryptogr. Mail. List (2008)
3. Shen, H., Zhang, M., Wang, H., Guo, F., Susilo, W.: A cloudaided privacy-preserving multi-dimensional data comparison protocol. Inf. Sci. (Ny) **545**, 739–752 (2021)
4. Yang, Q., Liu, Y., Chen, T., Tong, Y.: Federated machine learning: concept and applications. ACM Trans. Intell. Syst. Technol. **10**(2), 1–19 (2019)
5. Khan, L.U., Saad, W., Han, Z., Hossain, E., Hong, C.S.: Federated learning for internet of things: Recent advances, taxonomy, and open challenges. IEEE Commun. Surv. Tutorials (2021)
6. Wang, P., Wang, L., Leung, H., Zhang, G.: Super-resolution mapping based on spatial–spectral correlation for spectral imagery. IEEE Trans. Geosci. Remote Sens. **59**(3), 2256–2268 (2020)
7. Zhou, W., Lv, Y., Lei, J., Yu, L.: Global and local-contrast guides content-aware fusion for RGB-D saliency prediction. IEEE Trans. Syst. Man Cybern. Syst. (2019)
8. Lim, W.Y.B., et al.: Federated learning in mobile edge networks: a comprehensive survey. IEEE Commun. Surv. Tutorials **22**(3), 2031–2063 (2020)
9. Li, D., Deng, L., Cai, Z., Souri, A.: Blockchain as a service models in the Internet of Things management: systematic review. Trans. Emerg. Telecommun. Technol. (2020). https://doi.org/10.1002/ett.4139
10. He, Y., Dai, L., Zhang, H.: Multi-branch deep residual learning for clustering and beamforming in user-centric network. IEEE Commun. Lett. **24**(10), 2221–2225 (2020)
11. Zarrin, J., Wen Phang, H., Babu Saheer, L., Zarrin, B.: Blockchain for decentralization of internet: prospects, trends, and challenges. Cluster Comput. (2021). https://doi.org/10.1007/s10586-021-03301-8
12. Tseng, L., Yao, X., Otoum, S., Aloqaily, M., Jararweh, Y.: Blockchain-based database in an IoT environment: challenges, opportunities, and analysis. Cluster Comput. **23**(3), 2151–2165 (2020). https://doi.org/10.1007/s10586-020-03138-7
13. Li, X., Jiang, P., Chen, T., Luo, X., Wen, Q.: A survey on the security of blockchain systems. Future Gener. Comput. Syst. **107**, 841–853 (2020)
14. Conti, M., Kumar, E.S., Lal, C., Ruj, S.: A survey on security and privacy issues of bitcoin. IEEE Commun. Surv. Tutorials **20**(4), 3416–3452 (2018)
15. Sisi, Z., Souri, A.: Blockchain technology for energy-aware mobile crowd sensing approaches in Internet of Things. Trans. Emerg. Telecommun. Technol. (2021). https://doi.org/10.1002/ett.4217
16. Verma, S.B., Yadav, A.K.: Detection of Hard Exudates in Retinopathy Images ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue **8**(4),, 41–48 (2019). eISSN: 2255-2863, https://doi.org/10.14201/ADCAIJ2019844148
17. Verma, S.B., Shashi, B.V.: Data Transmission in BPEL (Business Process Execution Language). ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue **9**(3), 105–117 (2020). eISSN: 2255-2863 https://doi.org/10.14201/ADCAIJ202093105117 105
18. Verma, S.B., Brijesh, P., Gupta, B.K.: Containerization and its Architectures: A Study. ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal **11**(4), 395–409 (2022). eISSN: 2255-2863, https://doi.org/10.14201/adcaij.28351
19. Verma, S.B., Saravanan, C.: Performance analysis of various fusion methods in multi-modal biometric. In: 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES), pp. 5–8. IEEE (2018)

20. Verma, S.B., Yadav, A.K.: Hard Exudates Detection: A Review., Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing, vol 1286. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-9927-9_12
21. Rawat, P., Bajaj, M., Sharma, V., Vats, S.: A comprehensive analysis of the effectiveness of machine learning algorithms for predicting water quality. International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, pp. 1108–1114 (2023). https://doi.org/10.1109/ICIDCA56705.2023.10099968
22. Sharma, A., Sharma, C., Sharma, V., Vats, S.: Comparison & Performance Evaluation of Several Types of ECG Compression Techniques. 2nd International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2023 - Proceedings, pp. 915–921 (2023). https://doi.org/10.1109/ICSCDS56580.2023.10104703
23. Rawat, P., Bajaj, M., Mehta, S., Sharma, V., Vats, S.: A study on cervical cancer prediction using various machine learning approaches. International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, pp. 1101–1107 (2023). https://doi.org/10.1109/ICIDCA56705.2023.10099493
24. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
25. Peng, S.-L., Lin, C.-K., Pal, S. (eds.). Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
26. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4



Vulnerability Assessment and Penetration Testing at the Hypervisor Level

Anamika Agrawal[1], Satya Bhushan Verma[1(✉)], V. Sharma[2], Anil Kumar Pandey[1], and Suyogita Singh[1]

[1] Shri Ramswaroop Memorial University, Barabanki 225003, India
Satyabverma1@gmail.com

[2] Computer Science and Engineering, Adjunct Professor, Graphic Era Deemed to Be University, Graphic Era Hill University, Dehradun, India

Abstract. An outline of security advantages and difficulties of virtualization technology is given in this article. It explains the benefits of virtualization, with enhanced recovery, affordable protection, and safe virus testing. It also explores the security issues that virtualization brings about, such as data leakage and hypervisor vulnerabilities. Along with explaining vulnerability assessment and penetration testing (VAPT) in virtualized systems, the article also introduces pertinent security assessment technologies and makes a distinction between the two. It describes the features of the tools, along with its working with various virtualization products. This document is helpful for businesses trying to strengthen their security and guard against new dangers.

Keywords: Vulnerability Assessment · Security Advantages · Penetration Testing

1 Introduction

The technique known as virtualization makes it possible to divide the resources of a computer system into many separate execution units. Virtualization has becoming popular since it improves resource utilization and makes infrastructure administration easier for organization. Virtualization has security benefits but also raises several warning signs [1]. Penetration testing and vulnerability assessment are methods used by security professionals with specialized instruments to examine security stance of system. These techniques identify weak points in a system and evaluate the effectiveness of the security measures [2]. In order to address the main security problems and their basic reasons, this study first evaluates and reviews the security advantages of virtualization. In next step, go over a few security technologies that are made specifically for virtualized environment. Vulnerability assessment, or VA, is the process of locating, identifying, classifying, and security problems in a computer system (application/ network). Vulnerability assessments are instruments that give businesses' importance and contextualized understanding into cyber security threats, enabling comprehension and effective mitigation. The goal of the vulnerability assessment procedure is to identify these threats

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 202–213, 2025.
https://doi.org/10.1007/978-3-031-91008-1_19

and analyses the risks it poses. Typically, this process makes use of automated testing tools such as network security scanner. When everything is done, an assessment report that compiles the assessment tool's findings is produced. Businesses uses penetration testing (pen testing), as a cybersecurity strategy to find, evaluate, and rank any vulnerabilities in computer systems and networks. These assessments are usually performed by ethical hackers, who might be internal employees or external specialists. They comprise imitating the techniques and tactics employed by malicious users. This helps assess an organization's overall security readiness in relation to its network, computer infrastructure, and web-based applications. Confirmation of adherence to regulatory and industry standards may also be accomplished through penetration testing.

2 Literature Review

We see new developments in the field of information technology, including big data analytics, cloud computing, the Internet of Things (IoT), and artificial intelligence (AI). These days, a lot of companies are working hard to create service-oriented information systems that link customers and businesses quickly and effectively. Understanding the external service information systems that businesses use is the main goal of author Ma, W.M.'s exploration of information security attacks and defenses. Hydra is a tool that practitioners frequently use to evaluate website vulnerabilities. Moreover, novices in this domain might enhance their penetration skills by obtaining hands-on experience in detecting website vulnerabilities [25, 26]. Although classical machine learning algorithms have been widely used to intrusion detection, their efficacy in safeguarding markets is limited by issues with scalability, technical complexity, and accuracy. These restrictions have been lessened by the use of deep learning techniques, particularly when working with large amounts of data. Deep learning is superior in terms of detection accuracy and resilience against deformative assaults, and it also removes the necessity for manual rule construction. Long Short-Term Memory (LSTM) networks are supported by Diro and colleagues for distributed network attack detection in fog-to-object communication. They authorization and evaluate the main dangers and attacks that target Internet of Things devices, especially those that take advantage of flaws in wireless connectivity [36]. Two sets of experiments demonstrate the higher efficacy and efficiency of deep learning models compared to conventional machine learning models [27]. Protecting the network security of these environments has become a top priority for many businesses as private clouds proliferate. For an enterprise's total information security system, infrastructure construction must incorporate information security. A private cloud's vulnerabilities have the ability to disrupt the network as a whole, therefore thorough and methodical administration is necessary to ensure network security. In order to meet this problem, Qing and their colleagues prioritise large data security, private cloud network security, and fundamental network security [37]. They develop an assessment system architecture, examine pertinent evaluation criteria, and go into detail on corporate private cloud network security [28]. The author provides a thorough framework with a trust-enhanced distributed authorization architecture to address these issues [29]. This approach evaluates a platform's trustworthiness for authorization purposes by combining the ideas of "hard" and "soft" trust. The author then goes on to

give a reasoning for the overall model and a hybrid model that includes "hard" and "soft" trust components. After that, this architecture is put into in the context of web services, showcasing how well it may improve authorization decision-making—especially in a dispersed setting. Globalisation and the development of the internet are important developments in the fields of international information sharing and platform networking [32]. Because denial-of-service attacks can cause networks to go down, security has become more important. Penetration testing continues to be an authorial technique for identifying vulnerabilities even as network administrators strive to strengthen network security. Network security concerns have drawn both favourable and bad attention as cybercrime technology advance. The article discusses worries about criminal hackers' ability to compromise web servers [33].

3 Security Benefits of Virtualization

The inherent isolation that virtualization creates between Virtual Machines (VMs) and their respective execution environments confers several important security benefits. Firstly, this isolation allows multiple guest operating systems (OS) to reside on a single host machine, each OS executing its own programmes in a separate environment. Secondly, vulnerabilities within one guest OS do not affect other guest Oss. Finally, virtualization provides systems with the ability to restore to a normal state after security breaches.

Here are some notable security benefits associated with virtualization [3, 4]:

Enhanced and Expedited Recovery after Attacks: Virtualization makes it possible to quickly restore compromised virtual machines (VMs) to a clean snapshot in the case of a security incident. Restoring a virtual server is complicated and time-consuming as compare to this recovery method. Organisations can also make copies of compromised virtual machines (VMs) for further examination, that helps with forensic investigations and incident response.

Safer and More Effective Patching: When a security patch installation fails or creates problems, virtualization makes it easier to restore prior configuration of the system. This increases the possibility that security updates will be applied effectively and without interfering with business. Administrators can also verify the effectiveness of security updates before deploying them to production environments by cloning servers that are currently in use.

Cost-Effective Security Implementations: **VMs** are a useful tool for organisations to store security procedures and equipment including antivirus software, intrusion detection and prevention systems, and firewalls. This approach often results in cost savings because it does not require distinct physical hardware for each security component.

External Monitoring: Virtual machines (VMs) allow for the identification of negative actions and programme that are running outside of the VMs since they share hardware resources on a host. This is in contrast to conventional physical OS installations on a host, which frequently call for additional antivirus protection. An extra degree of protection is offered by the hypervisor's ability to actively monitor virtual machines and finds irregularities [4].

Secure Testing Environment for Malware: Malware testing and evaluation may be conducted in a safe environment. Virtual machines (VMs) created and replicated by security researchers and analysts, facilitating the secure run of malware samples for examination and threat evaluation. It is crucial to remember that certain viruses might make an effort to identify and avoid virtualized environments [5].

Taking everything into account, virtualization improves security by giving effective recovery alternatives, making patch administration safer, cutting expenses with virtual security appliances, enabling external monitoring, and providing a safe environment for malware testing and analysis. These advantages help create a security architecture that is more resilient and flexible in the ever-changing threat.

4 Virtualization Security Challenges

In addition to its many security advantages, virtualization poses a number of difficulties that enterprises must overcome in order to guarantee the integrity and safety of their virtualized environments. Security problems related to virtualization are:

Hypervisor Vulnerabilities:

Privilege Escalation: To function properly,Virtualization platforms need their hypervisors, and any weakness in them can result in serious security breaches. Intruders can try to take advantage of these flaws to elevate their privileges and perhaps compromise several virtual machines (VMs) that are hosted on the same hypervisor.

VM Sprawl:

Management Complexity: To satisfy their demands, businesses are creating more virtual machines (VMs), which makes maintaining and safeguarding them more difficult. Misconfigured virtual machines (VMs) due to VM sprawl pose a danger to security if they are not properly maintained or monitored.

Resource Contention:

Noisy Neighbors: Virtual machines (VMs) compete for physical resources like CPU, memory, and storage in a shared virtualized environment. Resource-intensive virtual machines (VMs)(High resource requirements) have the ability to cause denial-of-service (DoS) attacks by negatively impacting the security and performance of nearby VMs.

Inter-VM Attacks:

VM-to-VM Communication: Virtualization allows for communication between virtual machines (VMs) while also isolating them. This inter-VM communication can be used by attackers to move laterally inside a network and compromise other virtual machines (VMs) if it is not set appropriately.

Data Leakage:

Shared Storage: Virtual machines frequently share storage. Data breaches may result from sensitive data being exposed to or accessed by authorization VMs or users if appropriate access controls and encryption are not in place.

Snapshot Security:

Snapshot Exploitation: Snapshots can be helpful for backup and recovery, but they can also present security risks. If snapshots are not properly protected, attackers can attempt to access or modify them in an effort to retrieve sensitive data or restore a virtual machine to a vulnerable condition [34].

5 Vulnerability Assessment and Penetration Testing (VAPT)

In cybersecurity, vulnerability assessment and penetration testing, or VAPT, are two essential procedures that assist businesses in locating and resolving weaknesses in their IT infrastructure. For systems and data to remain secure and intact, certain procedures are necessary [35]. Let's examine VAPT in more detail:

K.V. Vulnerability Assessment (VA):
Vulnerability assessment is an authorize method of identifying, evaluating, and authorization vulnerabilities in the organization's network structure, applications, and information systems. The primary goal of VA is to give a comprehensive knowledge of the security posture with a focus on vulnerabilities that a threat may exploit. The primary components of risk assessment are as follows:

Scanning and Discovery: To VA begins with automated tools and manual examination to locate devices, services, and applications inside the network. Part of this involves looking for open ports, services, and system configurations.

Vulnerability Identification: Vulnerability scanners, like Nessus and Qualys, are used to detect known vulnerabilities, configuration errors, and flaws in the target environment.

Risk Prioritisation: Vulnerabilities are graded based on the impact and probability of occurrence once they are discovered.

Reporting: A full analysis that includes a list of all vulnerabilities found, risk ratings for each, and ideas for fixing them is created. A strategy for resolving discovered vulnerabilities is given in the report.

Frequent Assessments: Vulnerability assessments need to be executed regularly in order to keep up with the organization's IT infrastructure upgrades and the ever-changing threat environment (Fig. 1).

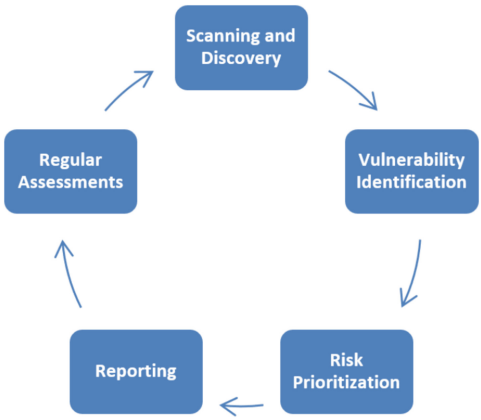


Fig. 1. Process of Vulnerability Assessment

K.V. Penetration Testing (Pen Test):
Penetration testing is a continuous security assessment process that simulates real attacks on an organization's networks, systems, and applications. It is also known as ethical hacking or pen testing. Pen testing's main goal is to find gaps in security and vulnerabilities that hackers may use against customers. The principal elements of penetration testing are listed below (Fig. 2):



Fig. 2. Process of penetration testing

Planning: The pen testing method starts with a defined scope, objectives, and rules of engagement. The organization and the testing team select the systems and goals to be tested [37].

Information Gathering: The penetration tester obtains information about the target environment, such as IP addresses, domain names, and application details. At this point, open-source intelligence (OSINT) and network reconnaissance are active.

Vulnerability Exploitation: Pen testers use both automated tools and human techniques to exploit vulnerabilities discovered during the information gathering phase. They attempt to carry out many attack situations raise their degree of authority, and gain authorization entry [38].

Documentation: The steps, effects, and methods of the penetration test are documented in great detail. This includes screenshots, logs, and any hacked data.

Reporting: All of the vulnerabilities that were successfully attacked are listed in a comprehensive report that also includes an analysis of the potential consequences and recommendations for corrective action. After each successful attack, a report usually includes a "proof of concept".

Testing Continuously: Periodic penetration testing or responses to significant changes in the organization's IT infrastructure should be conducted. Maintaining a strong safety profile is made easier by regular evaluations.

In conclusion, vulnerability assessment and penetration testing are related processes in the field of cybersecurity. Assessments of vulnerabilities may help organisations identify holes, but penetration testing takes a step further by actively analysing security

Table 1. Key Differences Between VA and Pen Testing

S. No.		Vulnerability Assessment	Penetration Testing
1	**Scope**	VA focuses on identifying vulnerabilities and weaknesses in an environment but does not attempt to exploit them	Pen testing actively seeks to exploit vulnerabilities and gain unauthorized access, mimicking the actions of a malicious attacker
2	**Purpose**	The primary goal is to provide a comprehensive view of vulnerabilities to guide remediation efforts	The primary goal is to assess the effectiveness of security controls and discover vulnerabilities through active exploitation
3	**Level of Detail**	VA provides a detailed list of vulnerabilities, their descriptions, and risk scores	Pen testing goes a step further by demonstrating how vulnerabilities can be exploited and providing actionable recommendations
4	**Methodology**	VA relies on automated scanning tools and manual checks to identify vulnerabilities	Pen testers use a mix of automated tools and manual testing techniques to actively exploit vulnerabilities

measures. Both are required to maintain strong cybersecurity and safeguard valuable information and systems [38].

Vulnerability assessment and penetration testing have similar goals of finding vulnerabilities and assessing system security, but they use distinct methodologies. Computer systems are usually examined using a variety of techniques during vulnerability assessment in order to find possible weak areas in such systems. On the other hand, penetration testing probes farther, modelling an actual assault to evaluate the system's reaction to legitimate dangers. This procedure produces a report that describes the assault's success or failure and frequently contains in-depth details about the attack itself. There are several types of penetration testing, which are classified based on the specific features an authorization plans to test or the scope (internal vs external). Generally, two primary approaches exist in penetration testing: Black-box and White-box, distinguished by the tester's level of prior knowledge about the system [2].

A. Black-box Testing The hallmark of black-box testing, often referred to as "external testing" or "remote testing," is that testers are not familiar with the system's architecture beforehand. Testers use real-world assault methods without any knowledge of the past. For example, testers could just be provided with the network IP address or website of the company [2].

B. White-box Testing As opposed to this, white-box testing uses testers who are already familiar with some aspects of the system, such the application code, network IP address schemes, operating system specifics, and occasionally even passwords. Verifying

network integrity and lowering the likelihood of internal attacks are the primary goals of white-box testing [2].

C. Virtualization Security Assessment Tools A variety of software applications and technologies are available for security assessment and penetration testing in different circumstances, including virtualization. It's necessary to understand that an operating system on a network with freely accessible ports and authorization services is analogous to a hypervisor in the context of virtualization. As a result, there are several technologies available for assessing the security of a hypervisor. Some of these tools must be used from a hypervisor-based virtual machine (VM) guest. Two important tools in this domain are Metasploit and V.A.S.T.O.

• Metasploit is not simply a vulnerability assessment tool; it is a sophisticated penetration testing platform developed to identify and exploit vulnerabilities. Metasploit has a number of modules for performing security audits and simulating attacks. Using scanning tools to identify vulnerabilities and selecting the appropriate attack tools to exploit them are the standard phases in the process. This may be a difficult process for testers with limited experience, but Metasploit is a helpful tool to assist streamline these tasks [17].
• VM-Informer Unlike V.A.S.T.O., VM-Informer analyses the security of a virtual environment based on pre-established security guidelines rather than an intruder's point of view. These principles serve as standards for security which can be modified to meet specific requirements. VM-Informer creates a report detailing the environment's security strength and vulnerabilities after doing an environment scan. VM-Informer assesses vulnerabilities in areas such as improper configurations, lack of security upgrades, unsuitable network schemes, and management layer defects [18].
• Nessus Nessus is a vulnerability assessment tool that can concurrently scan many hosts while assessing scan results against continuously updated vulnerability databases. Nessus's goal is to be a "free, powerful, up-to-date, and user-friendly remote security scanner." It relies on either NASAL or C-written plugins to identify vulnerabilities and provide guidance on how to solve them. Finding vulnerabilities such as buffer overflows, virtual machine escape vulnerabilities, code execution exploits, and denial of service (DoS) attacks is made easier with the help of Nessus. With the help of Nessus, testers may engage with SOAP APIs for VMWare vulnerability assessment, which expands their understanding of virtualization settings and the vulnerabilities that go along with them [19, 20].
• Hydra Brute-force attacks are used by the application Hydra to crack passwords. An attacker using a brute-force attack attempts several passwords in hope of finding out which one is correct. Hydra offers support for a wide range of online services, including HTTP, IMAP, and POP3. In virtualized environments, Hydra may be used to scan password authentication methods for weaknesses, primarily by checking the presence of any security measures [20, 22].
• Nmap Using the tool Nmap, one may scan a range of IP addresses, locate open ports, decide which devices are in operation right now, and discover what operating system is installed on those systems. Nmap is a valuable resource for learning about the target system, including the services that are up and running as well as their versions. Nmap is

an essential tool in penetration testing as this data is frequently the first stage of security evaluations [23, 24].

These tools collectively play a vital role in evaluating and enhancing the security of virtualized environments, ensuring they are well-protected against potential threats (Table 2).

Table 2. Virtualization Security Assessment Tools and Vulnerabilities

	V.A.S.T.O	NESSUS	CAIN&ABLE	CP-REPLAY	HYDRA	ETTERCAP
Hypervisor Vulnerabilities	✓	✓				
Inter-VM Attacks		✓				
Data Leakage	✓	✓	✓	✓		✓
Resource Contention	✓	✓				
Virtualization-Specific Malware	✓	✓				
Virtualization-Specific Malware	✓	✓		✓	✓	
Insecure VM Templates	✓					

The bulk of tools are general-purpose tools that can also be modified for usage in virtualized systems, however others, like V.A.S.T.O. or VM-Informer, are designed specifically for virtualization. It's also vital to remember that although certain tools, like Nessus, are mostly focused on vulnerability identification, others, like V.A.S.T.O. and Metasploit, are penetration testing tools that can carry out real assaults. What counts is whether the tool can detect or exploit vulnerabilities, not the kind of tool it is or how it evaluates vulnerabilities. The tools and the vulnerabilities they are associated with are listed in Table 1 [18].

Table 3. V.A.S.T.O for Penetration Testing of Virtualization

	VMWARE	XEN	ABIQUO	ORACLE-VM
Hypervisor Vulnerabilities	✓		✓	
Inter-VM Attacks				
Data Leakage	✓		✓	
Resource Contention	✓			
Virtualization-Specific Malware	✓	✓		✓
Virtualization-Specific Malware	✓	✓		
Insecure VM Templates	✓			

Tables 3 and 4 illustrate the connection between V.A.S.T.O and Nessus when evaluating vulnerabilities related to virtualization products. The remaining tools primarily focus on network assessment or can be employed in tandem for conducting penetration testing. One practical strategy for improving security in smaller businesses looking

Table 4. Virtualization Security Assessment Tools and Vulnerabilities

	VMWARE	XEN	K.V.M
Hypervisor Vulnerabilities	✓	✓	✓
Inter-VM Attacks	✓		
Data Leakage	✓	✓	
Resource Contention	✓	✓	✓
Virtualization-Specific Malware	✓		✓
Virtualization-Specific Malware	✓		
Insecure VM Templates			

for low-cost solutions would be to carry out a fundamental security assessment that focuses on vulnerability detection. As part of this evaluation, a report must be created and concerns must be authorization. Because of their ease of use, ability to do routine system checks, and ability to provide helpful information that aids in issue resolution, tools such as Nessus may be quite important in these kinds of situations. In such cases, VM-Informer can also be used.On the other hand, businesses where security is critical may choose to take a more thorough approach, going deep into the workings of their systems. This entails being aware of potential attack vectors for their systems as well as how quickly they can bounce back from them. This assignment requires an experienced penetration expert with sufficient understanding of using the system and resources. The process of penetration testing frequently involves complex testing scenarios that call for the usage of many technologies. During the information-gathering phase, tools like Nmap may be used to scan operating system versions, ports, services, and other relevant data. Furthermore, useful tools for sniffing and inspecting the hypervisor's network connections are Ettercap and Wireshark. Metasploit modules enable both password cracking and sniffing, with Hydra being a helpful tool for the latter.

6 Conclusion

The article examines virtualization's security, highlighting both its advantages and disadvantages. Virtualization technology has several advantages, like better recovery, safer patching, cost-effective security, and so on. However, it also comes with some security dangers, such data leakage and hypervisor vulnerabilities.To overcome these concerns, organisations should implement a comprehensive plan that includes access limits, patch management, and monitoring. The article looks at vulnerability assessment and penetration testing (vapt) techniques in addition to offering a number of tools for security assessments.Finally, the tools used for basic assessments or thorough testing have to align with the security goals of the company. By proactively addressing virtualized security concerns, organisations can maintain strong cybersecurity standards.

References

1. Pooja, K., Nagpal, R., Singh, T.P.: A survey on virtualization service providers, security issues, tools and future trends. Int. J. Comput. Appl. **69**(24), 36–42 (2013)
2. Shrestha, N.: Security Assessment via Penetration Testing: A Network and System Administrator's Approach, Master's thesis. Univ, OSLO (2012)
3. Rasmussen, E.R.: Reducing IT Costs and Increasing IT Efficiency by Integrating Platform-Virtualization in the Enterprise. Univ. Oregon., vol. 1277 (2009)
4. Randell, R.: Virtualization Security and Best Practices. RSA Secur. Conf. (2006)
5. Obasuyi, G., Sari, A.: Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment. J. Commun. Netw. Syst. 260–273 (2015)
6. Mahjani, A.: Security Issues of Virtualization in Cloud Computing Environments, Master's thesis, Luleå Univ. Technol. (2015)
7. Zahedi, S.: Virtualization Security Threat Forensic and Environment Safeguarding. Linnéus Univ, Degree project (2014)
8. Yu, A., Brée, D.: Side channel Attack- Survey Joy. Inf. Technol. Coding **1**(4), 54–57 (2004)
9. Kirch, J.: Virtual Machine Security Guidelines Version 1.0, The Centre for Internet Security (CIS) (2007)
10. Oberheide, J., Cooke, E., Jahanian, F.: Empirical exploitation of live virtual machine migration. Proc. BlackHat DC, no. VMM (2008)
11. Tayab, A., et al.: Virtualization and Information Security A Virtualized DMZ Design Consideration Using Vmware ESXi 4.1. Unitec Institute of Tech, New Zealand vol. 2, p. 89 (2012)
12. Wan, X., Zhang, X., Chen, L., Zhu, J.: An improved vTPM migration protocol based trusted channel. Int. Conf. Syst. Informatics, ICSAI 2012, no. Icsai, pp. 870–875 (2012)
13. Gurav, U., Shaikh, R.: Virtualization – A key feature of cloud computing. Int. Conf. Work. Emerg. Trends Technol., no. Icwet, pp. 227–229 (2010)
14. Benzidane, K., Khoudali, S., Sekkaki, A.: Secured architecture for inter-VM traffic in a Cloud environment, 2nd IEEE Lat. Am. Conf. Cloud Comput. Commun. LatinCloud **2013**, 23–28 (2013)
15. Tsai, H., Chiao, N., Steinmetz, R., Darmstadt, T.U.: Threat as a Virtualization's Impact on Cloud Security. 28th IEEE Int. Conf. Data Eng., no. February, pp. 32–38 (2012)
16. Wei, J., Zhang, X., Ammons, G., Bala, V., Ning, P.: Managing security of virtual machine images in a cloud environment. Proc. 2009 ACM Work. Cloud Comput. Secur. – CCSW '09, no. Vm, p. 91 (2009)
17. Greenwood, B.: An Introduction to Metasploit Project for the Penetration Tester, SANS Institute report, https://cyberdefense.sans.org/resources/papers/gsec/introduction-metasploit-project-penetrationtester-107151. Accessed: June 2018
18. Chauhan, S.: Hacking Vmware with VASTO, Infosec Inst. Report, http://resources.infosecinstitute.com/virtualization-security/#gref. June 2018
19. Mitchell, J.: Proactive Vulnerability Assessments with Nessus, SANS Inst. Report, https://www.sans.org/readingroom/whitepapers/auditing/paper/78. Accessed: June 2018
20. Thongthua, A., Ngamsuriyaroj, S.: Assessment of hypervisor vulnerabilities. Proc. – Int. Conf. Cloud Comput. Res.Innov., 71–77 (2016)
21. Norton, D.: An Ettercap Primer, SANS Inst.report, https://www.sans.org/readingroom/whitepapers/tools/paper/1406. Accessed: uth 2018
22. Yiannis, C.: Modern Password Cracking: A hands-on approach to creating an optimized and versatile attack. Inf. Secur. Group, R. Holloway, Univ. London (2013)
23. Corcoran, T.: An Introduction to NMAP,SANS Inst. Report. https://www.sans.org/readingroom/whitepapers/tools/paper/72. Accessed: June 2018

24. Hussain, A., Pradkin, Y., Heidemann, J.: Replay of malicious traffic in network testbeds, IEEE Int. Conf. Technol. Homel. Secur. HST **2013**, 322–327 (2013)
25. Yeo, J.: Using penetration testing to enhance your company's security. Comput Fraud Secur. **2013**(4), 17–20 (2013)
26. Ma, W.M.: Research on website penetration test. Glob Bus Manag J. **11**, 121–132 (2019)
27. Diro, A., Chilamkurti, N.: Leveraging LSTM networks for attack detection in fog-to-things communications. IEEE Commun. Mag. **56**(9), 124–130 (2018)
28. Verma, S.B., Yadav, A.K.: Detection of Hard Exudates in Retinopathy Images ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue **8**(4),, 41–48 (2019). eISSN: 2255-2863 https://doi.org/10.14201/ADCAIJ2019844148
29. Verma, S.B., Shashi, B.V.: Data Transmission in BPEL (Business Process Execution Language), ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal Regular Issue **9**(3), 105–117 (2020). eISSN: 2255-2863 https://doi.org/10.14201/ADCAIJ202093105117 105
30. Verma, S.B., Brijesh, P., Gupta, B.K.: Containerization and its Architectures: A Study, ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal **11**(4), 395–409 (2022). eISSN: 2255-2863, https://doi.org/10.14201/adcaij.28351
31. Verma, S.B., Saravanan, C.: Performance analysis of various fusion methods in multimodal biometric. In: 2018 International Conference on Computational and Characterization Techniques in Engineering & Sciences (CCTES), pp. 5–8. IEEE(2018)
32. Verma, S.B., Yadav, A.K.: Hard Exudates Detection: A Review. Emerging Technologies in Data Mining and Information Security. Advances in Intelligent Systems and Computing, vol 1286. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-9927-9_12
33. Rawat, P., Bajaj, M., Sharma, V., Vats, S.: A Comprehensive analysis of the effectiveness of machine learning algorithms for predicting water quality. International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, pp. 1108–1114 (2023). https://doi.org/10.1109/ICIDCA56705.2023.10099968
34. Sharma, A., Sharma, C., Sharma, V., Vats, S.: Comparison & Performance Evaluation of Several Types of ECG Compression Techniques. 2nd International Conference on Sustainable Computing and Data Communication Systems, ICSCDS 2023 - Proceedings, pp. 915–921 (2023). https://doi.org/10.1109/ICSCDS56580.2023.10104703
35. Rawat, P., Bajaj, M., Mehta, S., Sharma, V., Vats, S.: A study on cervical cancer prediction using various machine learning approaches. International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings, pp. 1101–1107 (2023). https://doi.org/10.1109/ICIDCA56705.2023.10099493
36. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
37. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
38. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4

Study of $\mathcal{L}-$ Local Function with Respect to Ideal Topology and $\mathcal{L}-$ Space

Zinah T. Abdulqader[1](✉), Rana B. Esmaeel[2], and Nabeel E. Arif[1]

[1] Department of Mathematics, College of Computer Science and Mathematics, Tikrit University, Salahaddin, Iraq
{ztaha,nabarif}@tu.edu.iq

[2] Department of Mathematics, College of Education for Pure Sciences-Ibn AL-Haithatham, University of Baghdad, Baghdad, Iraq
rana.b.i@ihcoedu.uobaghdad.edu.iq

Abstract. The present work is concerned with the new space namely ideal $\mathcal{L}-$ space. It is accordingly devoted to the basic properties of this new space and the relation between open set, $\mathcal{L}-$ open set and $\mathcal{L}^*-$ open set are studied as well as the concept of $\mathcal{L}-$ local function and some of their basic properties, examples and characterizations are presented. If $\mathfrak{F}$ is topology on $\mathcal{X}$, then $\mathcal{H}$ is $\mathcal{L}-$ open set if $\mathcal{H} \subseteq T \bigcup Int(\mathcal{H})\ \forall T \in \mathfrak{F} \& T \neq \Phi$. The $\mathcal{L}-$ kuratowski closure operator for any subset $\mathcal{A}$ of $\mathcal{X}$ with respect to $\mathcal{I}_{\mathcal{X}}$ and $\mathcal{L}O_{\mathcal{X}}$ is defined as $cl^*_{\mathcal{L}}(\mathcal{A}) = \mathcal{A} \bigcup \mathcal{A}^*_{\mathcal{L}}$. The $\mathcal{L}-$ closure of $\mathcal{H} \subseteq \mathcal{X}$ is denoted by $cl_{\mathcal{L}}(\mathcal{H})$ and it is the intersection for every $\mathcal{L}-$ closed sets that contains $\mathcal{H}$. Furthermore, this paper contains a study of some concepts in ideal $\mathcal{L}-$ space such as $\mathcal{L}-$ dense set and $\mathcal{I}_{\mathcal{X}} - \mathcal{L}-$ dense set as well as characterizations and examples of the proposed idea are given. Finally, we studying the definition of $\mathcal{L}-$ dense set and $\mathcal{L}-$ codense set in order to introduce the concept of $\mathcal{L}-$ codense ideal and some important results related to these concepts are proven.

Keywords: Open Set · Ideal Topology · Graph · Closure · Local Function

1 Introduction

Topology is offshoot of the mathematics which deal with the discussion of continuity and compactly.

Some kinds of sets game a substantial turn in the study of several properties in topological space as well as some authors introduced different generalized of an open set [1–4].

The idea for semi-open has been introduced by (Levine, 1963) [5] which is generalization for open.

(Njastad, 1965) [6] first proposed the notion of α −open which is also generalization of open set.

The topic for ideal in topology is treated in the classic.

Text.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 214–225, 2025.
https://doi.org/10.1007/978-3-031-91008-1_20

Ideal topology and related concepts have been studied in [7–9], where a class $\mathcal{I}_{\mathcal{X}}$ of subset is called ideal on $\mathcal{X}$ if

1. $\mathcal{X} \notin \mathcal{I}_{\mathcal{X}}$.
2. $\mathcal{B} \in \mathcal{I}_{\mathcal{X}}$ and $\mathcal{A} \subseteq \mathcal{B}$, then $\mathcal{A} \in \mathcal{I}_{\mathcal{X}}$.
3. $\mathcal{A} \cup \mathcal{B} \in \mathcal{I}_{\mathcal{X}}$ for $\mathcal{A}\&\mathcal{B} \in \mathcal{I}_{\mathcal{X}}$.

And $\mathcal{A}^* = \{\varkappa \in \mathcal{X} : (\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{I}_{\mathcal{X}}$ for every open $\mathcal{H}$ containing $\varkappa\}$ is named local function of $\mathcal{A}$.

The objective of this work is to introduce some new concepts of sets in ideal topological spaces such as $\mathcal{L}-$ open set, $\mathcal{L}-$ closure, $\mathcal{L}-$ dense, $\mathcal{L}-$ codense and $\mathcal{L}-$ local function in order to obtains many new results as shown in this paper.

2 Related Works

The pair $(\mathcal{X}, \mathfrak{F})$ means that topological space and $\mathcal{H} \subseteq \mathcal{X}$.

Definition 1.
A subset $\mathcal{H}$ is $\mathcal{L}-$ open set if $\mathcal{H} \subseteq T \bigcup Int(\mathcal{H})\ \forall T \in \mathfrak{F}\&T \neq \Phi$.
The set for every $\mathcal{L}$ − open is $\mathcal{L}O_{\mathcal{X}}$ and $(\mathcal{X}, \mathcal{L}O_{\mathcal{X}})$ is call $\mathcal{L}-$ space.

Proposition 1.

1. $\Phi, \mathcal{X}$ *are* $\mathcal{L}-$open sets.
2. If $\{\mathcal{H}\}_{\alpha \in \mathrm{I}}$ is $\mathcal{L}-$ open sets, then so is $\bigcup_{\alpha \in \mathrm{I}} \mathcal{H}_{\alpha}$.
3. Assume $\mathcal{H}_1$and $\mathcal{H}_2$ are $\mathcal{L}-$ open, then so is $\mathcal{H}_1 \cap \mathcal{H}_2$.

Definition 2.
The $\mathcal{L}-$ closure of $\mathcal{H} \subseteq \mathcal{X}$ is $cl_{\mathcal{L}}(\mathcal{H})$ and it is intersection of each of $\mathcal{L}-$ closed set which includes $\mathcal{H}$.

Theorem 1.
$cl_{\mathcal{L}}(\mathcal{H})$ is smallest $\mathcal{L}-$ closed set including $\mathcal{H}$.

Corollary 1.
$\mathcal{H}$ is a $\mathcal{L}-$ closed set iff $\mathcal{H} = cl_{\mathcal{L}}(\mathcal{H})$.

Definition 3.
A point $\varkappa \in \mathcal{X}$ is $\mathcal{L}-$ limit point for $\mathcal{H}$ if $\mathcal{F}$-$\{\varkappa\} \bigcap \mathcal{H} \neq \Phi\ \forall \mathcal{F} \in \mathcal{L}O_{\mathcal{X}}$ contains$\varkappa$.
The set of $\mathcal{L}-$ limit points of $\mathcal{H}$ is $\mathcal{L}\mathcal{P}(\mathcal{H})$.

Theorem 2.
$cl_{\mathcal{L}}(\mathcal{H}) = \mathcal{H} \bigcup \mathcal{L}\mathcal{P}(\mathcal{H})$.

3 Methodology

3.1 The $\mathcal{L}-$ Local Function

This part aims to study the idea for $\mathcal{L}-$ local function and presented some of their the basic properties, examples, characterizations.

Definition 4.
The ideal $\mathcal{L}-$ space is $\mathcal{L}-$ space $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}})$ with ideal $\mathcal{I}_{\mathcal{X}}$ and it is defined as $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$.

Definition 5.
If $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space & $\mathcal{A} \subseteq \mathcal{X}$, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \{\varkappa \in \mathcal{X} : (\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{I}_{\mathcal{X}}$ for every $\mathcal{L}-$ open $\mathcal{H}$ containing $\varkappa\}$ is named $\mathcal{L}-$ local function for$\mathcal{A}$.

Note 1.
When there is no ambiguity, we will write $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}})$ or simply $\mathcal{A}^*_{\mathcal{L}}$ for $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

Definition 6.
The $\mathcal{L}-$ kuratowski closure operator for any subset $\mathcal{A}$ of $\mathcal{X}$ with respect to $\mathcal{I}_{\mathcal{X}}$ and $\mathcal{LO}_{\mathcal{X}}$ is defined as $cl^*_{\mathcal{L}}(\mathcal{A}) = \mathcal{A} \bigcup \mathcal{A}^*_{\mathcal{L}}$.

Definition 7.
For $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space. Define a class $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ as follows $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \{\mathcal{A} \subseteq \mathcal{X} : cl^*_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{A}^c\}$.

Definition 8.
The members in $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ are called $\mathcal{L}^*-$ open sets.

Definition 9.
A complement for $\mathcal{L}^*-$ open is named $\mathcal{L}^*-$ closed.

Note 2.
We simply write $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}})$ or $\mathcal{LO}^*_{\mathcal{X}}$ for $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

Example 1.
If $\mathcal{X} = \{u, z, w\}$ & $\mathfrak{F} = \{\Phi, \{u, z\}, \mathcal{X}\}$ with $\mathcal{I}_{\mathcal{X}} = \{\Phi, \{u\}\}$. Then $\mathcal{LO}_{\mathcal{X}} = \{\Phi, \{u\}, \{z\}, \{u, z\}, \mathcal{X}\}$.

So, we have: $\Phi^*_{\mathcal{L}} = \Phi$, $\{u\}^*_{\mathcal{L}} = \Phi$, $\{z\}^*_{\mathcal{L}} = \{z, w\}$, $\{w\}^*_{\mathcal{L}} = \{w\}$, $\{u, z\}^*_{\mathcal{L}} = \{z, w\}$, $\{u, w\}^*_{\mathcal{L}} = \{w\}$, $\{z, w\}^*_{\mathcal{L}} = \{z, w\}$ and $\mathcal{X}^*_{\mathcal{L}} = \{z, w\}$.

Now, $cl^*_{\mathcal{L}}(\Phi) = \Phi \bigcup \Phi^*_{\mathcal{L}} = \Phi$, then $cl^*_{\mathcal{L}}(\mathcal{X}^c) = \mathcal{X}^c$, hence, $\mathcal{X} \in \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\{u\}) = \{u\} \bigcup \Phi = \{u\}$, then $cl^*_{\mathcal{L}}(\{z, w\}^c) = \{z, w\}^c$, hence, $\{z, w\} \in \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\{z\}) = \{z\} \bigcup \{z, w\} = \{z, w\}$, then $cl^*_{L}(\{u, w\}^c) = \{z, w\} \neq \{u, w\}^c$, hence, $\{u, w\} \notin \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\{w\}) = \{w\} \bigcup \{w\} = \{w\}$, then $cl^*_{\mathcal{L}}(\{u, z\}^c) = \{u, z\}^c$, hence, $\{u, z\} \in \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\{u,z\}) = \{u,z\}\bigcup\{z,w\} = \mathcal{X}$, Then $cl^*_{\mathcal{L}}\big(\{w\}^c\big) = \mathcal{X} \neq \{w\}^c$, hence, $\{w\} \notin \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\{u,w\}) = \{u,w\}\bigcup\{w\} = \{u,w\}$, then $cl^*_{\mathcal{L}}\big(\{z\}^c\big) = \{z\}^c$, hence, $\{z\} \in \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\{z,w\}) = \{z,w\}\bigcup\{z,w\} = \{z,w\}$, then $cl^*_{\mathcal{L}}\big(\{u\}^c\big) = \{u\}^c$, hence, $\{u\} \in \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

$cl^*_{\mathcal{L}}(\mathcal{X}) = \mathcal{X}\bigcup\{z,w\} = \mathcal{X}$, then $cl^*_{\mathcal{L}}(\Phi^c) = \Phi^c$, hence, $\Phi \in \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$. So, we have: $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \{\mathcal{X}, \{z,w\}, \{u,z\}, \{u\}, \{z\}, \Phi\}$.

Proposition 2.
If $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space, then:

1. $\Phi^*_{\mathcal{L}} = \Phi$.
2. $cl^*_{\mathcal{L}}(\Phi) = \Phi$.
3. $cl^*_{\mathcal{L}}(\mathcal{X}^c) = \mathcal{X}^c$.
4. $cl^*_{\mathcal{L}}(\mathcal{X}) = \mathcal{X}$.
5. $cl^*_{\mathcal{L}}(\Phi^c) = \Phi^c$.
6. $\mathcal{A} \subseteq cl^*_{\mathcal{L}}(\mathcal{A})$ and $\mathcal{A}^*_{\mathcal{L}} \subseteq cl^*_{\mathcal{L}}(\mathcal{A})$ for any subset $\mathcal{A}$ of $\mathcal{X}$.

Theorem 3.
$\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ is a topology on $\mathcal{X}$.

Definition 10.
$(\mathcal{X}, \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}))$ is called $\mathcal{L}^*-$ space.

Proposition 3.
Every $\mathcal{L}-$ open is $\mathcal{L}^*-$ open.

Proof.
Let $\mathcal{A}$ $\mathcal{L}-$ open. To claim $\mathcal{A}$ $\mathcal{L}^*-$ open, we must prove $cl^*_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{A}^c$. Since $cl^*_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{A}^c \bigcup (\mathcal{A}^c)^*_{\mathcal{L}}$, then $cl^*_{\mathcal{L}}(\mathcal{A}^c) \supseteq \mathcal{A}^c$. So, it is only remain we prove $cl^*_{\mathcal{L}}(\mathcal{A}^c) \subseteq \mathcal{A}^c$, let $\varkappa \in cl^*_{\mathcal{L}}(\mathcal{A}^c)$ and assume that $\varkappa \notin \mathcal{A}^c$, then $\varkappa \in (\mathcal{A}^c)^*$, hence $\big(\mathcal{A}^c \bigcap \mathcal{H}\big) \notin \mathcal{I}_{\mathcal{X}}$ for all $\mathcal{L}-$ open $\mathcal{H}$ containing $\varkappa$. Since $\varkappa \notin \mathcal{A}^c$, then $\varkappa \in \mathcal{A}$, but $\mathcal{A}$ is $\mathcal{L}-$ open set, then $\big(\mathcal{A}^c \bigcap \mathcal{A}\big) \notin \mathcal{I}_{\mathcal{X}}$ this imposable because $\mathcal{A}^c \bigcap \mathcal{A} = \Phi \in \mathcal{I}_{\mathcal{X}}$. so, $\varkappa \in \mathcal{A}^c$, thus $cl^*_{\mathcal{L}}(\mathcal{A}^c) \subseteq \mathcal{A}^c$. Hence proved.

Corollary 2.
$(\mathcal{X}, \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}))$ is finer than $\mathcal{L}-$ space $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}})$.

Remark 1.
The reverse of Proposition 3, is not hold, in example 1, $\mathcal{X} = \{u,z,w\}$ & $\mathfrak{F} = \{\Phi, \{u,z\}, \mathcal{X}\}$ with $\mathcal{I}_{\mathcal{X}} = \{\Phi, \{u\}\}$ then $\mathcal{LO}_{\mathcal{X}} = \{\Phi, \{u\}, \{z\}, \{u,z\}, \mathcal{X}\}$ and $\mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \{\mathcal{X}, \{z,w\}, \{u,z\}, \{u\}, \{z\}, \Phi\}$. So, we note $\{z,w\} \in \mathcal{LO}^*_{\mathcal{X}}(I_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$, but $\{z,w\} \notin (\mathcal{X}, \mathcal{LO}_{\mathcal{X}})$.

Proposition 4.
Every open set is a $\mathcal{L}^*-$ open set.

Proof.
Assume $\mathcal{A}$ an open, so $\mathcal{A}$ must be $\mathcal{L}-$ open thus $\mathcal{A}$ is $\mathcal{L}^*-$ open.

Corollary 3.
$(\mathcal{X}, \mathcal{LO}^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}))$ is finer than $(\mathcal{X}, \mathfrak{F})$.

Proof.
The prove direct from the fact $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}})$ finer than $(\mathcal{X}, \mathfrak{F})$.

Remark 2.
The reverse of Proposition 4 is not hold, in example 1, $\mathcal{X} = \{u, z, w\}$ & $\mathfrak{F} = \{\Phi, \{u, z\}, \mathcal{X}\}$ with $I_{\mathcal{X}} = \{\Phi, \{u\}\}$ then $\mathcal{LO}_{\mathcal{X}} = \{\Phi, \{u\}, \{z\}, \{u, z\}, \mathcal{X}\}$ and $\mathcal{LO}^*_{\mathcal{X}} = \{\mathcal{X}, \{z, w\}, \{u, z\}, \{u\}, \{z\}, \Phi\}$. So, we note $\{z, w\} \in \mathcal{LO}^*_{\mathcal{X}}$, but $\{z, w\} \notin \mathfrak{F}$.

Proposition 5.
Every $\mathcal{L}-$ closed is $\mathcal{L}^*-$ closed.

Proof.
For $\mathcal{A}$ is $\mathcal{L}-$ closed set, then $\mathcal{A}^c$ is $\mathcal{L}-$ open set, hence $\mathcal{A}^c$ is $\mathcal{L}^*-$ open set, therefore $\mathcal{A}$ is $\mathcal{L}^*-$ closed set.

Proposition 6.
Every closed is $\mathcal{L}^*-$ closed.

Proof.
Let $\mathcal{A}$ be closed, so $\mathcal{A}$ is $\mathcal{L}-$ closed, hence $\mathcal{A}$ is $\mathcal{L}^*-$ closed.

Theorem 4.
For $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$. If $\mathcal{I}_{\mathcal{X}} = \{\Phi\}$, then:

1. $\mathcal{A}^*_{\mathcal{L}} = cl_{\mathcal{L}}(\mathcal{A})$.
2. $cl^*_{\mathcal{L}}(\mathcal{A}) = cl_{\mathcal{L}}(\mathcal{A})$.
3. $\mathcal{LO}^*_{\mathcal{X}} = \mathcal{LO}_{\mathcal{X}}$.

Proof.

1. To prove $\mathcal{A}^*_{\mathcal{L}} \subseteq cl_{\mathcal{L}}(\mathcal{A})$, let $\varkappa \in \mathcal{A}^*_{\mathcal{L}}$ and we claim $\varkappa \in cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{A} \bigcup \mathcal{LP}(\mathcal{A})$. So, assume $\varkappa \notin \mathcal{A}$ and we prove that $\varkappa \in \mathcal{LP}(\mathcal{A})$, suppose that $\mathcal{H}$ is $\mathcal{L}-$ open containing $\varkappa$ and we claim $\left(\mathcal{A} \bigcap \mathcal{H} - \{\varkappa\}\right) \neq \Phi$. Since $\varkappa \in \mathcal{A}^*_{\mathcal{L}}$ & $\mathcal{H}$ $\mathcal{L}-$ open containing $\varkappa$, then $\left(\mathcal{A} \bigcap \mathcal{H}\right) \notin \mathcal{I}_{\mathcal{X}} = \{\Phi\}$, hence $\left(\mathcal{A} \bigcap \mathcal{H}\right) \neq \Phi$, therefore $\left(\mathcal{A} \bigcap \mathcal{H} - \{\varkappa\}\right) \neq \Phi$ because $\varkappa \notin \mathcal{A}$. This implies $\varkappa \in cl_{\mathcal{L}}(\mathcal{A})$. Now, assume $\varkappa \in cl_{\mathcal{L}}(\mathcal{A})$, to prove $\varkappa \in \mathcal{A}^*_{\mathcal{L}}$, let $\mathcal{H}$ be $\mathcal{L}-$ open containing $\varkappa$. Since $\varkappa \in cl_{\mathcal{L}}(\mathcal{A})$, then either $\varkappa \in \mathcal{A}$ or

$\varkappa \in \mathcal{LP}(\mathcal{A})$. If $\varkappa \in \mathcal{A}$, then $\varkappa \in \left(\mathcal{A} \bigcap \mathcal{H}\right)$, hence $\left(\mathcal{A} \bigcap \mathcal{H}\right) \neq \Phi$, thus $\left(\mathcal{A} \bigcap \mathcal{H}\right) \notin \{\Phi\} = \mathcal{I}_{\mathcal{X}}$, therefore $\varkappa \in \mathcal{A}^*_{\mathcal{L}}$. If $\varkappa \in \mathcal{LP}(\mathcal{A})$, then $\left(\mathcal{A} \bigcap \mathcal{H} - \{\varkappa\}\right) \neq \Phi$ since $\mathcal{H}$ be $\mathcal{L}-$ open containing $\varkappa$. Hence $\left(\mathcal{A} \bigcap \mathcal{H}\right) \neq \Phi$, thus $\left(\mathcal{A} \bigcap \mathcal{H}\right) \notin \{\Phi\} = \mathcal{I}_{\mathcal{X}}$ and $\varkappa \in \mathcal{A}^*_{\mathcal{L}}$, therefore $cl_{\mathcal{L}}(\mathcal{A}) \subseteq \mathcal{A}^*_{\mathcal{L}}$. Hence proved.

2. Since $cl^*_{\mathcal{L}}(\mathcal{A}) = \mathcal{A} \bigcup \mathcal{A}^*_{\mathcal{L}}$, then by the first part of this theorem we have $cl^*_{\mathcal{L}}(\mathcal{A}) = \mathcal{A} \bigcup \mathcal{A}^*_{\mathcal{L}} = \mathcal{A} \bigcup cl_{\mathcal{L}}(\mathcal{A}) = cl_{\mathcal{L}}(\mathcal{A})$.
3. Since $\mathcal{LO}^*_{\mathcal{X}}$ is finer than $\mathcal{LO}_{\mathcal{X}}$, then $\mathcal{LO}_{\mathcal{X}} \subseteq \mathcal{LO}^*_{\mathcal{X}}$. so, it is only remains we prove that $\mathcal{LO}^*_{\mathcal{X}} \subseteq \mathcal{LO}_{\mathcal{X}}$, thus we assume that $\mathcal{A} \in \mathcal{LO}^*_{\mathcal{X}}$, then $cl^*_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{A}^c$, hence by part two from this theorem we get $cl^*_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{A}^c = cl_{\mathcal{L}}(\mathcal{A}^c)$. Therefore $\mathcal{A}^c$ is $\mathcal{L}-$ closed set, hence then $\mathcal{A}$ is $\mathcal{L}-$ open set, that is, $\mathcal{A} \in \mathcal{LO}_{\mathcal{X}}$, this fact completed the proof.

Proposition 7.
Assume that $\mathfrak{F}$ is indiscrete topology on $\mathcal{X}$, then $\mathcal{LO}^*_{\mathcal{X}} = \mathcal{LO}_{\mathcal{X}}$.

Proof.
since $\mathfrak{F}$ is indiscrete topology, then $\mathcal{LO}_{\mathcal{X}}$ is a discrete space, hence $\mathcal{LO}_{\mathcal{X}} = \mathrm{P}(\mathcal{X})$, this implies $\mathcal{LO}^*_{\mathcal{X}} = \mathrm{P}(\mathcal{X})$ since $\mathcal{LO}_{\mathcal{X}} \subseteq \mathcal{LO}^*_{\mathcal{X}}$. Therefore proved.

Theorem 5.
Where $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is ideal $\mathcal{L}-$ space & $\mathcal{A}$ and $\mathcal{B} \subseteq \mathcal{X}$, then the following are holds:

1. $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ is $\mathcal{L}-$ closed set.
2. $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl_{\mathcal{L}}(\mathcal{A})$.
3. $\mathcal{A}$ is $\mathcal{L}-$ closed set, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}$.
4. $(\mathcal{A}^*_{\mathcal{L}})^*_{\mathcal{L}} \subseteq \mathcal{A}^*_{\mathcal{L}}$.
5. If $\mathcal{A} \subseteq \mathcal{B}$, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{B}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.
6. $(\mathcal{A} \bigcap \mathcal{B})^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.
7. $(\mathcal{A} \bigcap \mathcal{B})^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{B}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.
8. $(\mathcal{A} \bigcap \mathcal{B})^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \bigcap \mathcal{B}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.
9. $(\mathcal{A} \bigcup \mathcal{B})^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \bigcup \mathcal{B}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.
10. $\mathcal{A}^*_{\mathcal{L}} - \mathcal{B}^*_{\mathcal{L}} = (\mathcal{A} - \mathcal{B})^*_{\mathcal{L}} - \mathcal{B}^*_{\mathcal{L}}$.
11. $\mathcal{A}^*_{\mathcal{L}} - \mathcal{B}^*_{\mathcal{L}} \subseteq (\mathcal{A} - \mathcal{B})^*_{\mathcal{L}}$.
12. If $\mathcal{F}$ is $\mathcal{L}-$ open set, then $\mathcal{F} \bigcap \mathcal{A}^*_{\mathcal{L}} = \mathcal{F} \bigcap (\mathcal{A} \bigcap \mathcal{F})^*_{\mathcal{L}}$.
13. If $\mathcal{F}$ is $\mathcal{L}-$ open set, then $\mathcal{F} \bigcap \mathcal{A}^*_{\mathcal{L}} \subseteq (\mathcal{A} \bigcap \mathcal{F})^*_{\mathcal{L}}$.
14. If $\mathcal{C} \in \mathcal{I}_{\mathcal{X}}$, then $\mathcal{C}^*_{\mathcal{L}} = \Phi$.
15. If $\mathcal{C} \in \mathcal{I}_{\mathcal{X}}$, then $\mathcal{D} \in \mathcal{I}_{\mathcal{X}}$ and $\mathcal{D}^*_{\mathcal{L}} = \Phi$ for all $\mathcal{D} \subseteq \mathcal{C}$.
16. If $\mathcal{C} \in \mathcal{I}_{\mathcal{X}}$, then $(\mathcal{A} \bigcup \mathcal{C})^*_{\mathcal{L}} = \mathcal{A}^*_{\mathcal{L}} = (\mathcal{A} - \mathcal{C})^*_{\mathcal{L}}$.
17. If $\mathcal{LP}(\mathcal{A}) = \Phi$, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}$.
18. $\mathcal{A}^*_{\mathcal{L}} = cl_{\mathcal{L}}(\mathcal{A}^*_{\mathcal{L}})$.
19. $\mathcal{A}$ is $\mathcal{L}-$ closed set, then $cl_{\mathcal{L}}(\mathcal{A}^*_{\mathcal{L}}) \subseteq \mathcal{A}$.

Proposition 8.
For ideal $\mathcal{L}-$ space $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$. If $\mathcal{A}, \mathcal{B} \subseteq \mathcal{X}$, then

1. $cl^*_{\mathcal{L}}\left(\mathcal{A} \bigcup \mathcal{B}\right) = cl^*_{\mathcal{L}}(\mathcal{A}) \bigcup cl^*_{\mathcal{L}}(\mathcal{B})$.

2. $(cl^*_{\mathcal{L}}(\mathcal{A}))^*_{\mathcal{L}} \subseteq cl^*_{\mathcal{L}}(\mathcal{A})$
3. $cl^*_{\mathcal{L}}(\mathcal{A}) = cl^*_{\mathcal{L}}\big(cl^*_{\mathcal{L}}(\mathcal{A})\big)$.
4. $cl^*_{\mathcal{L}}(\mathcal{A}) \subseteq cl^*_{\mathcal{L}}(\mathcal{B})$ where $\mathcal{A} \subseteq \mathcal{B}$.
5. $cl^*_{\mathcal{L}}\big(\mathcal{A} \bigcap \mathcal{B}\big) \subseteq cl^*_{\mathcal{L}}(\mathcal{A}) \bigcap cl^*_{\mathcal{L}}(\mathcal{B})$.

Proposition 9.
For $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ & $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{P}_{\mathcal{X}})$, If $\mathcal{I}_{\mathcal{X}} \subseteq \mathcal{P}_{\mathcal{X}}$, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

Proof.
Assume $\mathcal{I}_{\mathcal{X}} \subseteq \mathcal{P}_{\mathcal{X}}$ & $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ and let $\mathcal{H}$ be any $\mathcal{L}-$ open contain $\varkappa$, then $(\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{P}_{\mathcal{X}}$, hence $(\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{I}_{\mathcal{X}}$ since $\mathcal{I}_{\mathcal{X}} \subseteq \mathcal{P}_{\mathcal{X}}$, therefore $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ and the proof finished.

Proposition 10.
If each of $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ & $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{P}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space, then $\mathcal{A}^*_{\mathcal{L}}\big(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}}\big) = \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \bigcup \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}})$ for any subset $\mathcal{A}$ of $\mathcal{X}$.

Proof.
Since $\mathcal{I}_{\mathcal{X}}and\mathcal{P}_{\mathcal{X}}$ are ideal, then $\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}}$ is ideal.

Since $\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}} \subseteq \mathcal{I}_{\mathcal{X}}$ and $\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}} \subseteq \mathcal{P}_{\mathcal{X}}$, then by Proposition 9, we get $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}})$ and $\mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}})$, hence $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \bigcup \mathcal{A}^*(\mathcal{P}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}})$.

To prove $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \bigcup \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}})$, assume $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}})$ and let $\mathcal{H}$ be any $\mathcal{L}-$ open contain $\varkappa$, then $(\mathcal{A} \bigcap \mathcal{H}) \notin (\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}})$, hence either $(\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{I}_{\mathcal{X}}$ or $(\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{P}_{\mathcal{X}}$, thus either $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}})$ or $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}})$, hence $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \bigcup \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}})$, so $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \bigcup \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}})$.

Therefore, $\mathcal{A}^*_{\mathcal{L}}\big(\mathcal{I}_{\mathcal{X}} \bigcap \mathcal{P}_{\mathcal{X}}\big) = \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}) \bigcup \mathcal{A}^*_{\mathcal{L}}(\mathcal{P}_{\mathcal{X}})$.

Proposition 11.
If $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ ideal $\mathcal{L}-$ space & $(\mathcal{X}, \mathfrak{F}, \mathcal{I}_{\mathcal{X}})$ ideal topological space. Then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F})$.

Proof.
Assume $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$, then $(\mathcal{A} \bigcap \mathcal{H}) \notin \mathcal{I}_{\mathcal{X}}$ for all $\mathcal{L}-$ open $\mathcal{H}$ containing $\varkappa$. To prove $\varkappa \in \mathcal{A}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F})$, let $\mathcal{F}$ be any open contain $\varkappa$, then $\mathcal{F}$ is $\mathcal{L}-$ open contain $\varkappa$, hence we have $(\mathcal{A} \bigcap \mathcal{F}) \notin \mathcal{I}_{\mathcal{X}}$. Therefore $\varkappa \in \mathcal{A}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F})$ and $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq \mathcal{A}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F})$.

Remark 3.
In Example 1 we have $\mathcal{X} = \{u, z, w\}$, $\mathfrak{F} = \{\Phi, \{u, z\}, \mathcal{X}\}$, $\mathcal{I}_{\mathcal{X}} = \{\Phi, \{u\}\}$ and $\mathcal{LO}_{\mathcal{X}} = \{\Phi, \{u\}, \{z\}, \{u, z\}, \mathcal{X}\}$.

Put $\mathcal{A} = \{z\}$, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \{z\}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \{z, w\}$.

While, $\mathcal{A}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F}) = \{\ddagger\}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F}) = \mathcal{X}$ because the open sets which containing $u\&z$ are $\{u, z\}$ and $\mathcal{X}$ such that $\{z\} \bigcap \{u, z\} = \{z\} \notin \mathcal{I}_{\mathcal{X}}$ & $\{z\} \bigcap \mathcal{X} = \{z\} \notin \mathcal{I}_{\mathcal{X}}$ then $u\&z \in \{z\}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F})$ since $\mathcal{X}$ is only open which containing w and $\{z\} \bigcap \mathcal{X} = \{z\} \notin \mathcal{I}_{\mathcal{X}}$, then $w \in \{z\}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F})$.

So, we concluded that $\mathcal{A}^*(\mathcal{I}_{\mathcal{X}}, \mathfrak{F}) \subsetneq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

3.2 Some Types of Dense in Ideal $\mathcal{L}-$ Space

This part deal with studying the definition of $\mathcal{L}-$ dense set and $\mathcal{L}-$ codense set in order to introduce the concept of $\mathcal{L}-$ codense ideal. Moreover, some important results related to these concepts are proven.

Definition 11.
$\mathcal{A}$ is named $\mathcal{L}-$ dense set if $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X}$.

Definition 12.
The $\mathcal{L}-$ dense set whose complement is also $\mathcal{L}-$ dense set is named $\mathcal{L}-$ codense set.

Definition 13.
If $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space. Then $\mathcal{A}$ is $\mathcal{I}_{\mathcal{X}}-\mathcal{L}-$ dense set if $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \mathcal{X}$.

Definition 14.
Assume $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ ideal $\mathcal{L}-$ space. Then $\mathcal{I}_{\mathcal{X}}$ is a $\mathcal{L}-$ dense ideal if each nonempty set in $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ dense set.

Definition 15.
For ideal $\mathcal{L}-$ space $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$. Then $\mathcal{I}_{\mathcal{X}}$ is a $\mathcal{L}-$ codense ideal if each nonempty set in $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense set.

Proposition 12.
Every closed must be $\mathcal{L}-$ closed.

Proof.
Assume $\mathcal{A}$ closed, so $\mathcal{A}^c$ open, hence $\mathcal{A}^c$ $\mathcal{L}-$ open set, therefore $\mathcal{A}$ is $\mathcal{L}-$ closed.

Proposition 13.
$cl_{\mathcal{L}}(\mathcal{A}) \subseteq cl(\mathcal{A})$.

Proof.
Since $cl(\mathcal{A})$ is closed, then by Proposition 12 we get $cl(\mathcal{A})$ is $\mathcal{L}-$ closed. But $\mathcal{A} \subseteq cl(\mathcal{A})$ and $cl_{\mathcal{L}}(\mathcal{A})$ is smallest $\mathcal{L}-$ closed set containing $\mathcal{A}$, so we have $cl_{\mathcal{L}}(\mathcal{A}) \subseteq cl(\mathcal{A})$.

Proposition 14.
$\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl(\mathcal{A})$.

Proof.
From [Theorem 5: (2)] we have $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl_{\mathcal{L}}(\mathcal{A})$. But $cl_{\mathcal{L}}(\mathcal{A}) \subseteq cl(\mathcal{A})$ by Proposition 13. Hence $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl(\mathcal{A})$.

Theorem 6.

1. Every $\mathcal{I}_{\mathcal{X}} - \mathcal{L}-$ dense set is $\mathcal{L}-$ dense set.
2. Every $\mathcal{L}-$ dense set is dense set.
3. Every $\mathcal{I}_{\mathcal{X}} - \mathcal{L}-$ dense set is dense set.

Proof.

1. Assume $\mathcal{A}$ is $\mathcal{I}_{\mathcal{X}} - \mathcal{L}-$ dense set, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{L}O_{\mathcal{X}}) = \mathcal{X}$. By [Theorem 5: (2)] we have $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{L}O_{\mathcal{X}}) \subseteq cl_{\mathcal{L}}(\mathcal{A})$ and we know that $cl_{\mathcal{L}}(\mathcal{A}) \subseteq \mathcal{X}$, hence $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X}$, so $\mathcal{A}$ is $\mathcal{L}-$ dense set.
2. Suppose $\mathcal{A}$ is $\mathcal{L}-$ dense set. To prove $\mathcal{A}$ is dense set we must prove $cl(\mathcal{A}) = \mathcal{X}$. Clearly $cl(\mathcal{A}) \subseteq \mathcal{X}$. Now, we have $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X}$ because $\mathcal{A}$ is $\mathcal{L}-$ dense.By Proposition 13, we have $cl_{\mathcal{L}}(\mathcal{A}) \subseteq cl(\mathcal{A})$. Hence $\mathcal{X} \subseteq cl(\mathcal{A})$. So, $cl(\mathcal{A}) = \mathcal{X}$, therefore $\mathcal{A}$ is dense set.
3. Assume $\mathcal{A}$ is $\mathcal{I}_{\mathcal{X}} - \mathcal{L}-$ dense set, then by (1) we get $\mathcal{A}$ is $\mathcal{L}-$ dense set, hence by (2) we get $\mathcal{A}$ is dense set.

Proposition 15.
Every $\mathcal{L}-$ dense ideal is a dense ideal.

Proof.
Assume $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ dense ideal & $\mathcal{A}$ is a nonempty set in$\mathcal{I}_{\mathcal{X}}$, then $\mathcal{A}$ is $\mathcal{L}-$ dense set, hence $\mathcal{A}$ is dense set by [Theorem 6: (2)], therefore $\mathcal{I}_{\mathcal{X}}$ is a dense ideal.

Proposition 16.
Assume that $(\mathcal{X}, \mathcal{L}O_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space. If $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal, then for each nonempty set $\mathcal{A}$ in $\mathcal{I}_{\mathcal{X}}$ we have:

1. $\mathcal{A}$ is not $\mathcal{L}-$ open.
2. $\mathcal{A}$ is not $\mathcal{L}-$ closed.
3. $\mathcal{A}^c$ is not $\mathcal{L}-$ open.
4. $\mathcal{A}^c$ is not $\mathcal{L}-$ closed

Proof.
Assume $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal & $\mathcal{A}$ is any nonempty set in$\mathcal{I}_{\mathcal{X}}$, then $\mathcal{A}$ is $\mathcal{L}-$ codense set, so $\mathcal{A}$ is $\mathcal{L}-$ dense set and $\mathcal{A}^c$ is $\mathcal{L}-$ dense set, that is, $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X}$ and$cl_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{X}$. Since $\mathcal{A} \in \mathcal{I}_{\mathcal{X}}$ and $\mathcal{A} \neq \Phi$, then $\mathcal{A} \neq \mathcal{X}$ and$\mathcal{A}^c \neq \mathcal{X}$.Hence $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X} \neq \mathcal{A}$ and$cl_{\mathcal{L}}(\mathcal{A}^c) = \mathcal{X} \neq \mathcal{A}^c$, so $\mathcal{A}$ is not $\mathcal{L}-$ closed and $\mathcal{A}^c$ is not $\mathcal{L}-$ closed. Hence $\mathcal{A}^c$ is not $\mathcal{L}-$ open and $\mathcal{A}$ is not $\mathcal{L}-$ open.

Remark 4.
In Example 1: we have $\mathcal{X}$=$\{u, z, w\}$, $\mathfrak{F} = \{\Phi, \{u, z\}, \mathcal{X}\}$, $\mathcal{I}_{\mathcal{X}} = \{\Phi, \{u\}\}$, $\mathcal{L}O_{\mathcal{X}}$ =$\{\Phi$, $\{u\}, \{z\}, \{u, z\}, \mathcal{X}\}$ and$\mathcal{X}^*_{\mathcal{L}} = \{z, w\}$. So, we conclude that$\mathcal{X}^*_{\mathcal{L}} \subseteq \mathcal{X}$, but$\mathcal{X}^*_{\mathcal{L}} \neq \mathcal{X}$.

Hence, in the following proposition we establish necessary and sufficient conditions to obtain the equality.

Proposition 17.
Assume $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space. If $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal, then $\mathcal{X}^*_{\mathcal{L}} = \mathcal{X}$.

Proof.
Clearly $\mathcal{X}^*_{\mathcal{L}} \subseteq \mathcal{X}$. To prove $\mathcal{X} \subseteq \mathcal{X}^*_{\mathcal{L}}$, let $\varkappa \in \mathcal{X}$ and $\mathcal{H}$ be any $\mathcal{L}-$ open include $\varkappa$, then $\mathcal{X} \bigcap \mathcal{H} = \mathcal{H}$. Since $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal, then $\mathcal{H} \notin \mathcal{I}_{\mathcal{X}}$, because if$\mathcal{H} \in \mathcal{I}_{\mathcal{X}}$, then by [Proposition 16: (1)] we get $\mathcal{H}$ is not $\mathcal{L}-$ open this is contradiction. So, $\forall \varkappa \in \mathcal{X}$ and for any $\mathcal{L}-$ open $\mathcal{H}$ include $\varkappa$, then $\mathcal{X} \bigcap \mathcal{H} \notin \mathcal{I}_{\mathcal{X}}$, hence $\varkappa \in \mathcal{X}^*_{\mathcal{L}}$, so $\mathcal{X} \subseteq \mathcal{X}^*_{\mathcal{L}}$, therefore $\mathcal{X}^*_{\mathcal{L}} = \mathcal{X}$.

Theorem 7.
If $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}}$ ideal $\mathcal{L}-$ space then $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal iff $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$.

Proof.
Suppose $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal and $\mathcal{A} \in \mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}}$, then $\mathcal{A} \in \mathcal{LO}_{\mathcal{X}}$ and $\mathcal{A} \in \mathcal{I}_{\mathcal{X}}$ if $\mathcal{A} \neq \Phi$, then by Proposition 16: (1) we have $\mathcal{A}$ is not $\mathcal{L}-$ open this contradiction because$\mathcal{A} \in \mathcal{LO}_{\mathcal{X}}$, thus $\mathcal{A} = \Phi$. Hence $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$.

Now, let $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$. If $\mathcal{I}_{\mathcal{X}}$ is not $\mathcal{L}-$ codense ideal, then there exist $\mathcal{L}-$ dense set $\mathcal{A}$ in $\mathcal{I}_{\mathcal{X}}$ such that $\mathcal{A}^c$ is not $\mathcal{L}-$ dense set, that is $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X}$ but $cl_{\mathcal{L}}(\mathcal{A}^c) \neq \mathcal{X}$. Hence $\exists \varkappa \in \mathcal{X}$ but $\varkappa \notin cl_{\mathcal{L}}(\mathcal{A}^c)$, so there is $\mathcal{L}-$ closed set include $\mathcal{A}^c$ say $\mathcal{F}$ such that $\varkappa \notin \mathcal{F}$. Now, since $\mathcal{A}^c \subseteq \mathcal{F}$, then $\mathcal{F}^c \subseteq \mathcal{A}$, but $\mathcal{F}$ is $\mathcal{L}-$ closed, then $\mathcal{F}^c$ is $\mathcal{L}-$ open. Now, $\mathcal{F}^c \subseteq \mathcal{A} \in \mathcal{I}_{\mathcal{X}}$ and $\mathcal{I}_{\mathcal{X}}$ is ideal, then $\mathcal{F}^c \in \mathcal{I}_{\mathcal{X}}$ but $\mathcal{F}^c \in \mathcal{LO}_{\mathcal{X}}$, so $\mathcal{F}^c \in \mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$, hence $\mathcal{F}^c = \Phi$, therefore $\mathcal{F} = \mathcal{X}$ this is contradiction since $\varkappa \in \mathcal{X}$ but $\varkappa \notin \mathcal{F}$. So, $\mathcal{I}_{\mathcal{X}}$ must be $\mathcal{L}-$ codense ideal.

Corollary 4.
For space $(\mathcal{X}, \mathfrak{F})$ &where $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}})$ is $\mathcal{L}-$ space with ideal $\mathcal{I}_{\mathcal{X}}$. If $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal, then $\mathfrak{F} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$.

Proof.
Let $\mathcal{I}_{\mathcal{X}}$ be an $\mathcal{L}-$ codense ideal, then by Theorem 7, we have $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$. Now, let $\mathcal{A} \in \mathfrak{F} \bigcap \mathcal{I}_{\mathcal{X}}$, then $\mathcal{A} \in \mathfrak{F}$ and $\mathcal{A} \in \mathcal{I}_{\mathcal{X}}$. Since $\mathfrak{F} \subseteq \mathcal{LO}_{\mathcal{X}}$, then $\mathcal{A} \in \mathcal{LO}_{\mathcal{X}}$, hence $\mathcal{A} \in \mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}}$. so, we have $\mathcal{A} \neq \Phi$. Therefore, $\mathfrak{F} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$.

Proposition 18.
suppose that $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space. If $\mathcal{X}^*_{\mathcal{L}} = \mathcal{X}$, then $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal.

Proof.
Let $\mathcal{X}^*_{\mathcal{L}} = \mathcal{X}$. Then $\forall \varkappa \in \mathcal{X}$ we get $\varkappa \in \mathcal{X}^*_{\mathcal{L}}$. Hence $\mathcal{X} \bigcap \mathcal{H} \notin \mathcal{I}_{\mathcal{X}}$ for all $\mathcal{L}-$ open $\mathcal{H}$ contain $\varkappa$, that is $\mathcal{H} \notin \mathcal{I}_{\mathcal{X}}$ for all $\mathcal{L}-$ open $\mathcal{H}$ contain $\varkappa$.

Now, if $\mathcal{I}_{\mathcal{X}}$ is not $\mathcal{L}-$ codense ideal, then there exist $\mathcal{L}-$ dense set $\mathcal{A}$ in $\mathcal{I}_{\mathcal{X}}$ such that $\mathcal{A}^c$ is not $\mathcal{L}-$ dense set, that is $cl_{\mathcal{L}}(\mathcal{A}) = \mathcal{X}$ but $cl_{\mathcal{L}}(\mathcal{A}^c) \neq \mathcal{X}$. Hence $\exists \rceil \in \mathcal{X}$ but $\rceil \notin cl_{\mathcal{L}}(\mathcal{A}^c)$, so there is $\mathcal{L}-$ closed set include $\mathcal{A}^c$ say $\mathcal{F}$ such that $\rceil \notin \mathcal{F}$, then $\rceil \in \mathcal{F}^c$.

Now, since $\mathcal{A}^c \subseteq \mathcal{F}$, then $\mathcal{F}^c \subseteq \mathcal{A}$, but $\mathcal{F}$ is $\mathcal{L}-$ closed, then $\mathcal{F}^c$ is $\mathcal{L}-$ open. So, $\mathcal{F}^c \subseteq \mathcal{A} \in \mathcal{I}_{\mathcal{X}}$ and $\mathcal{I}_{\mathcal{X}}$ is ideal, then we have $\mathcal{F}^c \in \mathcal{I}_{\mathcal{X}}$ this impossible because $\mathcal{F}^c$ is $\mathcal{L}-$ open containing $\rceil$. So, $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal.

Theorem 8.
For ideal $\mathcal{L}-$ space $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$, we have $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal iff$\mathcal{X}^*_{\mathcal{L}} = \mathcal{X}$.

Proof.
The proof is follows by Proposition 17 & Proposition 18.

Remark 5.
In Example 1: we have $\mathcal{X}$=$\{u, z, w\}$, $\mathfrak{F} = \{\Phi, \{u, z\}, \mathcal{X}\}$, $\mathcal{I}_{\mathcal{X}} = \{\Phi, \{u\}\}$, $\mathcal{LO}_{\mathcal{X}}$ =$\{\Phi$, $\{u\}$, $\{z\}$, $\{u, z\}$, $\mathcal{X}\}$. Then the $\mathcal{L}-$ closed sets are$\mathcal{X}$,$\{z, w\}$, $\{u, w\}$, $\{w\}$ and Φ.

Consider, $\mathcal{A} = \{u\}$, then $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \Phi$ and $cl_{\mathcal{L}}(\mathcal{A}) = \{u, w\}$, hence $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl_{\mathcal{L}}(\mathcal{A})$, but $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \neq cl_{\mathcal{L}}(\mathcal{A})$.

Now, in the following Theorem we put necessary and sufficient conditions to obtain the equality between $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})\&cl_{\mathcal{L}}(\mathcal{A})$.

Theorem 9.
Let $(\mathcal{X}, \mathcal{LO}_{\mathcal{X}}, \mathcal{I}_{\mathcal{X}})$ is an ideal $\mathcal{L}-$ space. Then $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal iff $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = cl_{\mathcal{L}}(\mathcal{A})$ for any $\mathcal{L}-$ open $\mathcal{A}$.

Proof.
Assume $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal and $\mathcal{A}$ is any $\mathcal{L}-$ open. If $\mathcal{A} = \Phi$, then we are done since $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = cl_{\mathcal{L}}(\mathcal{A}) = \Phi$. So, we suppose $\mathcal{A} \neq \Phi$. To prove $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = cl_{\mathcal{L}}(\mathcal{A})$ we must prove $cl_{\mathcal{L}}(\mathcal{A}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$ & $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl_{\mathcal{L}}(\mathcal{A})$.

By [Theorem 5: (2)] we have $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) \subseteq cl_{\mathcal{L}}(\mathcal{A})$.

Since $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal, then by Theorem 7 we get $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$.

Now, let $\varkappa \in cl_{\mathcal{L}}(\mathcal{A})$, to prove $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$, let $\mathcal{H}$ be $\mathcal{L}-$ open containing $\varkappa$. Since $\varkappa \in cl_{\mathcal{L}}(\mathcal{A})$, then either $\varkappa \in \mathcal{A}$ or $\varkappa \in \mathcal{LP}(\mathcal{A})$.

Now, $\mathcal{A}$ and $\mathcal{H}$ are $\mathcal{L}-$ open, then $\mathcal{A} \bigcap \mathcal{H}$ is $\mathcal{L}-$ open.

If $\varkappa \in \mathcal{A}$, then $\varkappa \in \left(\mathcal{A} \bigcap \mathcal{H}\right)$ since $\varkappa \in \mathcal{H}$, hence $\left(\mathcal{A} \bigcap \mathcal{H}\right) \neq \Phi$ and $\left(\mathcal{A} \bigcap \mathcal{H}\right) \in \mathcal{LO}_{\mathcal{X}}$.

Now, if $\left(\mathcal{A} \bigcap \mathcal{H}\right) \in \mathcal{I}_{\mathcal{X}}$, then $\left(\mathcal{A} \bigcap \mathcal{H}\right) \in (\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}})$, hence.

$\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} \neq \{\Phi\}$ this contradiction since $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} = \{\Phi\}$. So, we have $\left(\mathcal{A} \bigcap \mathcal{H}\right) \notin \mathcal{I}_{\mathcal{X}}$, therefore $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$.

If $\varkappa \in \mathcal{LP}(\mathcal{A})$, then $\left(\mathcal{A} \bigcap \mathcal{H} - \{\varkappa\}\right) \neq \Phi$ since $\mathcal{H}$ be $\mathcal{L}-$ open containing $\varkappa$. Hence $\left(\mathcal{A} \bigcap \mathcal{H}\right) \neq \Phi$.

Since $\mathcal{A} \bigcap \mathcal{H}$ is nonempty $\mathcal{L}-$ open, then $\left(\mathcal{A} \bigcap \mathcal{H}\right) \notin \mathcal{I}_{\mathcal{X}}$ because if $\left(\mathcal{A} \bigcap \mathcal{H}\right) \in \mathcal{I}_{\mathcal{X}}$, then $\left(\mathcal{A} \bigcap \mathcal{H}\right) \in (\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}})$, hence $\mathcal{LO}_{\mathcal{X}} \bigcap \mathcal{I}_{\mathcal{X}} \neq \{\Phi\}$ this impossible. So, must be $\left(\mathcal{A} \bigcap \mathcal{H}\right) \notin \mathcal{I}_{\mathcal{X}}$, hence $\varkappa \in \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$, therefore $cl_{\mathcal{L}}(\mathcal{A}) \subseteq \mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}})$. So, $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = cl_{\mathcal{L}}(\mathcal{A})$.

Conversely: Assume $\mathcal{A}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = cl_{\mathcal{L}}(\mathcal{A})$ for any $\mathcal{L}-$ open $\mathcal{A}$. Since $\mathcal{X}$ is $\mathcal{L}-$ open, then by hypothesis we get:

$\mathcal{X}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = cl_{\mathcal{L}}(\mathcal{X})$, hence $\mathcal{X}^*_{\mathcal{L}}(\mathcal{I}_{\mathcal{X}}, \mathcal{LO}_{\mathcal{X}}) = \mathcal{X}$ since $cl_{\mathcal{L}}(\mathcal{X}) = \mathcal{X}$. Therefore by Theorem 8, we get $\mathcal{I}_{\mathcal{X}}$ is $\mathcal{L}-$ codense ideal.

4 Conclusion

In this paper we concluded some important goals in topological space and many results in ideal topology were obtained such as $\mathcal{L}O^*_{\mathcal{X}}(\mathcal{I}_{\mathcal{X}}, \mathcal{L}O_{\mathcal{X}})$ is a topology on $\mathcal{X}$, every $\mathcal{L}-$ open is $\mathcal{L}^*-$ open, every $\mathcal{I}_{\mathcal{X}} - \mathcal{L}-$ dense is $\mathcal{L}-$ dense and every $\mathcal{L}-$ dense is dense.

References

1. Esmaeel, R.B., Mohammad, R.J.: On Nano soft J-semi-G-closed sets. J. Phys. Conf. Ser. **1591**(1) (2020). https://doi.org/10.1088/1742-6596/1591/1/012071
2. Ali, M., Massed, A., Mohammad, A.: β*-open sets and β*-continuity in topological spaces. Thai J. Math. **8**, 142–148 (2014). https://doi.org/10.1016/j.jtusci.2013.09.006
3. Mohammad, R.J., Esmaeel, R.B.: On separation axioms with soft-J-semi-g-open sets. IOP Conf. Ser. **12052**, 1–11 (2020). https://doi.org/10.1088/1757-899X/871/1/012052
4. Mohammed, A.S., Ahmed, I.S., Asaad, S.H.: Study of the rings in which each element express as the sum of an idempotent and pure. Int. J. Nonlinear Anal. Appl. **12**(2), 1719–1724 (2021). https://doi.org/10.22075/IJNAA.2021.5311
5. Levine, N.: Semi-open sets and semi-continuity in topological spaces. Am. Math. Mon. **70**(1), 36–41 (1963). https://doi.org/10.1080/00029890.1963.11990039
6. Njastad, O., O.: On some classes of nearly open sets. Pacific J. Math. **15**(3), 961–970 (1965)
7. Nasef, A.A., Radwan, A.E., Esmaeel, R.B.: Some properties of α-open sets with respect to an ideal. Int. J. Pure Appl. Math. **102**(4), 613–630 (2015). https://doi.org/10.12732/ijpam.v102i4.3
8. Jankovic, D., Hamlett, T.R.: New topologies from old via ideals. Am. Math. Mon. **97**(4), 295–310 (1990). https://doi.org/10.1080/00029890.1990.11995593
9. Dontchev, J., Ganster, M., Rose, D.: Ideal resolvability. Topol. Appl. **93**(1), 1–16 (1999). https://doi.org/10.1016/s0166-8641(97)00257-5

Blockchain Technology and Its Implications in Data Management System: A Empirical Analysis on Corporate Database Management

Saikat Maity[1], S. Brindha[2], Maheswari Mookiaha[3], S. Jeyalaksshmi[4], and D. Akila[5(✉)]

[1] Department of Computer Science and Engineering, Sister Nivedita University (Techno India Group), Kolkata, India
saikat.ma@snuniv.ac.in

[2] Department of Computer Application, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chennai 603203, India
brindhas1@srmist.edu.in

[3] Department of Computer Science, Government Arts and Science College, Thiruchuli, Tamilnadu, India

[4] Department of Information Technology, Vels Institute of Science, Technology and Advanced Studies (VISTAS), Chennai, India

[5] Department of Computer Applications, Saveetha College of Liberal Arts and Sciences, Saveetha Institute of Medical and Technical Sciences, Chennai, India
akiindia@yahoo.com

Abstract. The financial and accounting sectors are among the areas that have been affected most by blockchain technology (BCT). This study examines how BCT may affect accounting processes in Corporate and their relationship with financial reporting. The research is based on mixed methods design, where qualitative interviews were conducted with Corporate accounting experts while quantitative analysis of financial data was done. To ascertain how BCT has impacted the reliability, transparency and efficacy of financial reporting procedures of Corporate enterprises, this study examined financial reports and conducted interviews. Some of the findings include increased transparency; lowered fraud risks; simplified data reconciliation and auditing process that could be some advantages that BCT can bring into Corporate's finance reporting system. There are a number of challenges to the widespread adoption of BCT such as concerns about personal information privacy, legal compliance difficulties and need for skilled administrators to manage block chain networks. Aspects like organizational readiness, regulatory climate, comparative benefits over conventional reporting techniques remain critical to understanding why firms in Corporate adopt or reject BCT in their Database management. The outcomes from this study will help for improving financial reporting by governmental agencies, accounting firms etc., so as they can adapt to various issues in digital economy using BCT. Therefore further research is wanted to explore wider implications of blockchain usage for financial statement in both Corporate and overseas as well as its viable long-term impact on finance reporting processes.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 226–237, 2025.
https://doi.org/10.1007/978-3-031-91008-1_21

Keywords: BCT · Financial Reporting · Digital Economy · Corporate Database management

1 Introduction

In current years, it has been one of the hottest subjects due to its disruptive capability, making it appealing throughout special industries including accounting and finance sectors too. Blockchain, as an allotted ledger gadget that cannot be reversed, has other packages other than virtual money transactions that are most effective. It was devised as a technological foundation in the back of Bitcoin, among other cryptocurrencies. Hence, better performance, accuracy, and transparency in financial reporting through new ways, together with blockchains, can revolutionize accounting thanks to BCT. Further insights into such traits can also assist researchers in understanding the expected outcomes resulting from those elements in business structures, specifically the ones primarily based on elements encompassed in economic statements. In relation to different foremost economic facilities, Corporate's economic system is small but rapidly growing and has greater links with worldwide markets. Consequently, it's crucial for accountants, regulators, and legislators in Corporate to realize the implications of BCT on finance reporting.

In the study of, [1] analysed how BCT changed financial reporting in Corporate. By utilising combined strategies, which include quantitative evaluation of monetary information and qualitative interviews with accounting specialists in the United States, this research intends to focus on the pros and cons of the usage of BCT in Corporate accounting structures. This research contributes to the developing frame of understanding approximately economic reporting and blockchain technology, for this reason its necessity. Although some literature has tested blockchain's potential blessings somewhere else, there may be little acknowledged about its effect on accounting within one-of-a kind styles of economies like Corporate that have specific institutional and prison frameworks.

Although BCT has numerous viable advantages, there are also numerous issues and boundaries that must be addressed before it can be fully utilized in Corporate accounting. They encompass issues about infrastructure requirements, statistics protection, regulatory compliance, and the availability of professional employees to control blockchain systems [2]. It is necessary to acknowledge those barriers and broaden appropriate strategies if one wants to take advantage of BCT's sufficient accounting methods in Corporate. This observation aims at figuring out how accounting in Corporate is embracing the new BCT by examining the reasons behind its good adoption and use. Accounting professionals, regulators, and lawmakers in Corporate can also benefit from the study's illumination of these demanding situations, and the findings can add to the worldwide communication about the consequences of BCT on financial reporting [3].

2 Literature Work

In [4] analysed the financial enterprises registered on the Iraqi Stock Exchange. Data was retrieved from annual reports and data streams using a purposive sampling method. It analyses data using Stata and applies the random effect model to panel data regression. The results showed that, except for the meeting frequency, government mechanisms had no discernible impact on management practices. As a moderating variable across banking sectors, BCT, on the other hand, had a positive and substantial impact. These findings provided evidence that Iraqi financial businesses' management practices were reined in during the Chairman's time on the board. There aren't many studies that look at the impact of Iraqi government procedures on managerial practices, so this one stands out.

The literature on corporate governance and BCT has been surveyed in this research. To establish a connection between BCT and governance systems, theoretical and conceptual considerations are used. According to [5] BCT aids businesses in mitigating the detrimental and immoral impacts of long-serving managers and the knowledge gap between company leadership and stockholders. The distributed and decentralised ledger known as BCT does this by enhancing the record-keeping process with superior security, precision, transparency, and accountability. Accordingly, BCT may reduce agency expenses and the responsibilities of conventional CG methods in businesses. Nevertheless, there is a dearth of empirical research in this specific domain.

Earnings quality and bank continuity are the empirical variables that are investigated in this research. In addition, it looks at Iraqi listed banks' social performance via the lens of corporate social responsibility, and how ownership structure and the representation of women on boards of directors affect this index. Using panel data, the researchers checked whether gender diversity and ownership structure affected the correlation between bank continuity and earnings quality. Iraqi banks are experiencing financial instability and have very poor earning quality, according to the survey. It demonstrates that the administration's motivations for preserving the continuity and earning quality of a bank are unaffected by management and concentrated ownership as moderating factors. In [6] also discovered that gender diversity on the board of directors enhances the association between earning quality and a bank's continuity, suggesting that the inclusion of women on the board is a key moderating influence.

The impact of blockchain technology on long-term efficiency is examined in this research, with a focus on the growing nation of Vietnam. This is when the management accounting system comes into play as a moderator. One more thing: the study model uses digital transformation as a moderating variable for linkages. Based on interviews with Vietnamese manufacturers, it draws conclusions regarding this situation and a quantitative approach was used in the execution of the financial reports. Vietnam is already home to industrial enterprises that reflect to the people. Emails were sent out to those who would be interested in taking part in the survey. Examine 568 observations after deleting outliers and missing responses. The results show that blockchain technology significantly improves sustainable performance, and that management accounting system mediates this effect favourably, using partial least squares structural equation modelling [7].

Focusing on the properties of blockchain data its immutability, append-only nature, sharing, verification, and agreed-upon status this article evaluates existing research on the ways in which blockchain technology might influence accounting and AI-enabled auditing. Using blockchain technology, the research finds four topics that have altered accounting record-keeping: event-based accounting, continuing auditing, accounting with three entries, and real-time data collecting. [8] Concludes with a list of recommendations for further study on how to modernize accounting and auditing using blockchain technology by enhancing current procedures and fostering stakeholder participation. Blockchain-related data security [16–19] has been clearly described in the healthcare sector. The research papers in the previous proceedings also helped us to preparation of this papers (Fig. 1).

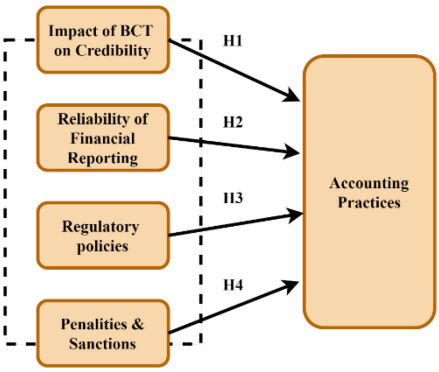


Fig. 1. Conceptual Framework of BCT and its Implications for Financial Reporting

1. **Hypothesis 1 (Impact of BCT on Credibility):**
   Creative Database management negatively impact the credibility of monetary reviews in Corporate commercial banks. Organisation that interact in BCT may also guide accounting data misleadingly, affecting the judgments of monetary statement customers.
2. **Hypothesis 2 (Reliability of Financial Reporting):**
   The reliability of financial reporting in Corporate commercial banks is encouraged by the extent of BCT employed by using these banks. As BCT will increase, the credibility of monetary reports can also lower.
3. **Hypothesis 3 (Regulatory Policies):**
   Regulatory agencies in Corporate play a crucial role in the banking sectors. If they adopt effective policies to detect and address creative accounting methods in financial statements, it can mitigate the negative impact of BCT on financial reporting credibility.
4. **Hypothesis 4 (Penalties and Sanctions):**
   Implementing check laws with penalties and sanctions for harmful techniques in creative accounting can discourage organisations involving with BCT, thereby enhancing financial reporting credibility.

3 Methodology

3.1 Research Design

A robust studies strategy is important for producing credible findings whilst analysing the consequences of BCT on financial reporting in Corporate accounting procedures. Integrating qualitative and quantitative methodologies in a combined-methods technique would possibly provide useful consequences. To get a greater nuanced understanding of the viewpoints, problems, and feasible blessings of using BCT in economic reporting, qualitative procedures like interviews with accountants and regulators are best. The statistical proof of the breadth of BCT use are defined and its consequences at the precision, openness, and efficacy of monetary reporting can be acquired by means of quantitative evaluation, perhaps in the form of surveys or data analytics. The purpose of any sampling approach in Corporate's economy must be to accumulate information this is consultant of the country, consisting of all industries and business sizes. Additionally, the influences and development of BCT adoption over the years is probably captured through longitudinal statistics accumulating. To thoroughly grasp the outcomes of BCT on financial reporting in Corporate, an intensive have a look at design is necessary to guarantee the validity and reliability of the outcomes.

3.2 Population and Sample

Numeric data from all financial statements' face financials is available in the Financial Statement Data Sets below. Companies submit their financial reports to the Commission using extensible Business Reporting Language exhibits, which include these data. While the Financial Statement and Notes Data Sets are comprehensive and include narrative and numerical disclosures from all financial statements and their notes, the Financial Statement Data Sets are smaller and more focused on financial statements (https://www.kaggle.com/datasets/securities-exchange-commission/financial-statement-extracts). Each registrant's financial reports are published here "as filed" without any changes made to those reports. Users can examine and compare company disclosure information among registrants and across time because to the data's flattened presentation. The data sets also include other elements that help make the data more usable, such as a company's Standard Industrial Classification. [9] analysis the population includes all organizations involved in financial reporting in Corporate, spanning all industries and corporate sizes. The results will be generalizable since a representative sample will be chosen from such a large population. To provide a balanced representation of industries and company sizes, stratified random sampling will be used to choose the sample. This approach will increase the credibility and validity of the examiner's findings on how BCT has affected monetary reporting in Corporate with the aid of making sure that a extensive kind of people's evaluations are covered (Fig. 2).

3.3 Measures

It is vital to have a robust studies method if you want to generate credible findings at the same time as carrying out studies at the outcomes of block chain technology on monetary

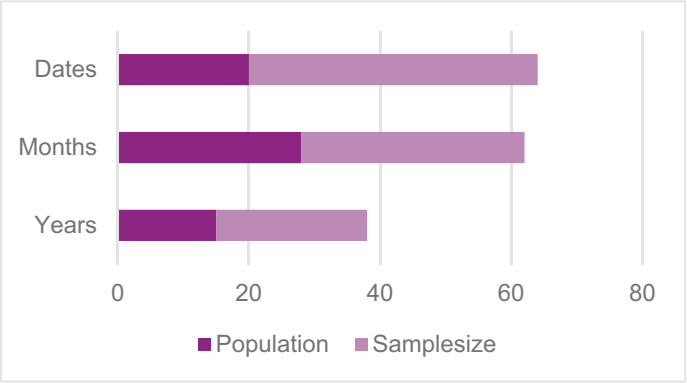


Fig. 2. Demographic profile of the sample

reporting in Corporate Database management. In a combined-methods design, the use of each qualitative and quantitative methodologies can bring about suited effects. Therefore, for an improved comprehension of the views, complexities, and feasible benefits of BCT in monetary reporting, qualitative methods inclusive of interviewing accountants and regulators are best. According to Malik S (2020), the statistical evidence at the volume of BCT adoption and its implications for the accuracy, transparency, and effectiveness of economic reporting can be obtained through quantitative analysis, perhaps thru surveys or facts analytics. Any sampling strategy for Corporate's financial system should are trying to find to acquire information that is consultant of the country inclusive of all business sectors and varieties of groups.

3.4 Analytical Methods

In this regard, numerous measures will be hired to comprehensively have a look at how BCT has impacted economic reporting inside Corporate accounting methods. Efficiency, timeliness, and accuracy are applicable quantitative indices that need to no longer be ignored while making ready financial reviews. Evaluating the have an impact on of BCT deployment on accounting procedures involves measuring time saved as well as the as the quantity of energy directed toward other elegant organization sports. For the better notion into how BCT implementation influences corporation tradition, stakeholder be given the truth and regulatory compliance can also be supplied by using qualitative measurements. Surveys or interviews need to display what accounting professionals think about or feel closer to BCT or why they have now not ventured into it but, among others. Merging blockchain era into gift financial reporting systems offers chances and barriers which could handiest be acknowledged. By combining various each quantitative and qualitative indicators, [10] gives an effective illustration of the way BCT influences economic reporting strategies in Corporate.

4 Findings

4.1 Measurement Model Assessment

To understand the impact of BCT on economic reporting in Corporate accounting requirements, this paper assesses 4 giant components. At first the impact of BCT on credibility indicates how the use of BCT impacts the trustworthiness and transparency of economic information (Table 1).

Table 1. Result of Validity and Reliability

Constructs	Items	Cronbach's Alpha	Composite Reliability (CR)	Average Variance Extracted (AVE)
Impact of BCT on Credibility	4	0.646	0.561	0.805
Reliability of Financial Reporting	5	0.657	0.674	0.598
Regulatory Policies	6	0.692	0.705	0.512
Penalties and Sanctions	3	0.622	0.603	0.743

The regulatory policies which can be a assemble in this look at refer to people who alter using blockchain technology (BCT) in financial reporting environments. It measures stakeholders' perspectives approximately the openness or simplicity/supervision over policies regarding reporting criteria primarily based on the usage of Blockchain Technology with six gadgets. The Penalties and Sanctions to check stakeholders' knowledge on results arising from mistakes made all through monetary reports or lack of knowledge to BCT standards as outlined through [11]. In 2024. Alpha values among 0.622 $<$ Cronbach's $<$ 0.692 suggest inner consistency as it is measured for these constructs which additionally mean their reliability is acceptable too. Correspondingly, CR rankings ranging 0.561–0.705 exhibit a mild degree of assemble reliability. The constructs have managed to capture exceptional dimensions of phenomena being studied as indicated through Average Variance Extracted (AVE) values spanning from 0.512 to 0.805 indicating precise convergent validity in addition to this. The outputs obtained display a satisfying degree on account that AVE values range from at least 0.512 as much as 0.805 which shows they own terrific composite reliability degrees.

4.2 Descriptive Statistics

According to [12] the research looks at how different groups in Corporate see four main concepts connected to how Blockchain Technology (BCT) may change financial reporting in the country's accounting systems. With an average score of 5.61 and a standard deviation of 0.415, the "Impact of BCT on Credibility" construct shows that the incorporation of BCT significantly enhances perceived credibility. Similarly, the "Reliability

of Financial Reporting" construct shows that people have a positive impression of the dependability of financial reporting procedures when BCT is used in the banking sectors (Table 2).

Table 2. Mean, Standard Deviation, and correlation

Constructs	Mean	SD	1	2	3	4	5
Impact of BCT on Credibility	5.61	0.415	0.841	1			
Reliability of Financial Reporting	5.74	0.567	0.782	0.759	1		
Regulatory Policies	5.51	0.625	0.624	0.598	0.627	1	
Penalties and Sanctions	5.44	0.743	0.322	0.673	0.563	0.473	1

The construct has a mean score of 5.74 and a standard deviation of 0.567. With a standard deviation of 0.625 and an average score of 5.51 for "Regulatory Policies," stakeholders show moderate agreement on the efficacy and clarity of regulations governing the use of BCT in financial reporting. There is conflicting opinion on the efficacy of penalties and sanctions in ensuring adherence to BCT-driven reporting requirements, as shown by the construct of "Penalties and Sanctions" which has an average score of 5.44 and a standard deviation of 0.743. The different levels of linkage between these constructs in the correlation matrix, which shows the links between them. The results provide light on how various parties in Corporate see the consequences of BCT on financial reporting.

4.3 Structural Model Assessment

Accounting firms in Corporate must conduct structural model evaluations to have a look at the results of BCT on monetary reporting. Examining the interrelationships of many ideas is on the important part of these evaluations; for instance, we study how BCT affects credibility, the trustworthiness of financial reviews, regulatory rules, and fines and punishments (Fig. 3).

Evaluating structural models involves looking at perfect indicators like RMSEA, Comparative Fit Index (CFI), and Tucker-Lewis Index (TLI). Indicative of the model's validity and explanatory capacity, these indices measure how well the suggested model fits the observed data. Reason, Y. G., (2023) proposes the structural model's mediating linkages and indirect effects may be tested for significance using bootstrapping approaches. Researchers may test their assumptions and get useful findings on BCT's effect on Corporate's financial reporting methods by conducting thorough structural model evaluations.

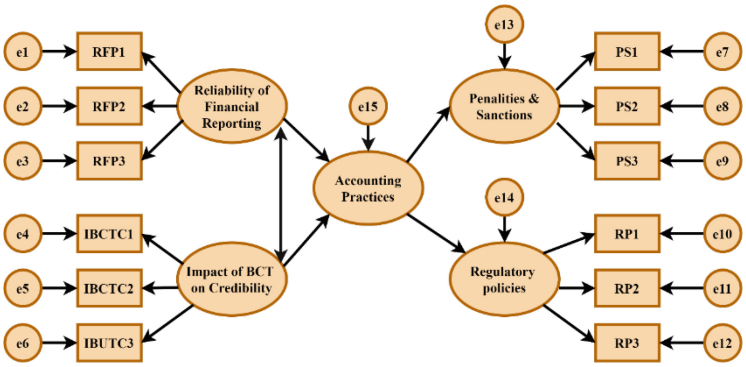


Fig. 3. Structural model for BCT and its Implications for Financial Reporting

Table 3. Result of path coefficients

	B	β	S.E.	t-value	P-value
Impact of BCT on Credibility	0.121	0.136	0.173	4.81	0.01
Reliability of Financial Reporting	0.124	0.134	0.167	5.51	0.001
Regulatory Policies	0.126	0.143	0.169	6.52	0.006
Penalties and Sanctions	0.321	0.193	0.171	7.22	0.002

Results from the structural model analysis show that there are strong connections between the different concepts and how they affect accounting in Corporate. "Regulatory Policies" (B = 0.126), "Reliability of Financial Reporting" (B = 0.124), and "Impact of BCT on Credibility" (B = 0.121) had the smallest effects, while the coefficients (B) showed the largest effects for "Penalties and Sanctions" (B = 0.321). The standardized effects are shown by the associated beta coefficients (β), which indicate their relative significance. These connections are statistically significant, indicating that regulatory regulations, fines, and BCT adoption substantially effect Database management in Corporate, with t-values ranging from 4.81 to 7.22 and p-values < 0.01 is shown in Table 3.

5 Discussion

The discussion part discusses corporate accounting practices and the relevance and usefulness of BCT research results on financial reporting. It examines how BCT adoption affects reliability, financial reporting, regulatory norms, and punishment/sanctions. Large positive correlations show that BCT adoption favourably affects financial statement credibility, reliability in report production, attachment to reporting and awareness about rules. BCT might adjust reporting procedures under corporate accounting requirements, according to the article. This includes accountants, investors, stock market traders, and others who needed financial data protection. This discussion shows

politicians and business magnates' real-life perspectives on BCT integration's pros and cons. Besides that, this part extensively examines study constraints such limited sample size and relevance difficulties. Therefore, future researches should examine ways to overcome these limits to better comprehend blockchain technology's financial reporting duties in accounting organisations. The analysis provides a full description of this study's findings, ramifications, and suggestions for further research on integrating technology with accounting practice in intriguing areas.

6 Recommendation and Conclusion

Research results imply creative opportunities that emerge when blockchain is carried out in improving economic reporting at some point of Corporate. To whole use of BCT absolutely experts in accounting department have include its adoption coupled with investment in training activities too. Regulatory companies should provide suggestions regarding standards and help in the direction of integration of block chain generation in order that innovation may be allowed to take vicinity freely. This implies that greater emphasis is needed on cybersecurity measures to secure in addition privacy regarding monetary records facilitated via BCT. There is no doubt that it'd create good surroundings for innovation if a few agencies regulated the use of BCT in various industries and there have been some standards set apart to deal with such integration. Even with ability prospects to enhance monetary reporting methods, regulatory, technical and organizational issues need to be contemplated upon earlier than imposing BCT. Implementation of block chain generation in accounting operations of Corporate will cause higher consider on monetary statements, transparency and effectiveness through solving associated challenges. Therefore, this may be instrumental in increasing the economic system while on the equal time enabling it stay solid as nicely in the Database management.

Limitations and Potential Paths for Future Research

Although this study has many benefits, it also has several downsides. First, the research was restricted to corporate accounting systems and couldn't be extended elsewhere. The second issue is that participants provided the data, which may have introduced inaccuracies and biases. If the sample size doesn't represent Corporate's accounting firms, the study's external validity may suffer. Since the study was cross-sectional, it can't confirm the relationships. To discover how BCT affects financial reporting if future research address these gaps. First, longitudinal studies may track BCT adoption trends to evaluate its long-term effects on financial reporting. Second, comparative research across regions or countries should examine regulatory frameworks and BCT adoption to better understand cultural and institutional factors that affect BCT implementation. Qualitative methods like case studies and interviews may help determine how stakeholders interpret and handle BCT adoption in financial reporting. Finally, therapies or training programs to promote accounting professionals' BCT acceptance and use may be investigated experimentally. Future research on these channels may help it understand BCT-affected global financial reporting methods.

References

1. Alkhwaldi, A.F., Alidarous, M.M., Alharasis, E.E.: Antecedents and outcomes of innovative blockchain usage in accounting and auditing profession: an extended UTAUT model. J. Organ. Change Manag. **37**, 1102 (2024)
2. Alkhwaldi, A.F., Aldhmour, F.M.: Beyond the bitcoin: analysis of challenges to implement blockchain in the Corporate public sector. In: Convergence of Internet of Things and Blockchain Technologies, pp. 207–220. Springer International Publishing, Cham (2021)
3. Abu Afifa, M.M., Nguyen, T.H., Nguyen, L.T.L., Tran, T.H.T., Dao, N.T.: Nexus among blockchain technology adoption and firm performance: perspective from mediating and moderating effects. Int. J. Organ. Anal. (2024). https://doi.org/10.1108/IJOA-11-2023-4076
4. Ahmed, M.G., Ganesan, Y., Hashim, F., Sadaa, A.M.: The effect of chairman tenure on governance and earnings management: a case study in Iraq. J. Asian Financ. Econ. Bus. **8**(3), 1205–1215 (2021)
5. Akhtar, T.: Blockchain technology: the beginning of a new era in reforming corporate governance mechanisms. J. Knowl. Econ.Knowl. Econ. **15**, 1–26 (2023)
6. Sadaa, A.M., Ganesan, Y., Ahmed, M.G.: The effect of earnings quality and bank continuity: the moderating role of ownership structure and CSR. J. Sustain. Financ. Invest. **13**(1), 366–386 (2023)
7. Nguyen, N.M., Abu Afifa, M., Van Bui, D.: Blockchain technology and sustainable performance: moderated-mediating model with management accounting system and digital transformation. Environ. Dev. Sustain. **27**, 1–23 (2023)
8. Lalwani, N.: Accounting and auditing with block chain technology and artificial intelligence–an empirical study. Int. J. Manag. Public Policy Res. **2**(4), 63–74 (2023)
9. Ben-Avraham, R., et al.: Feasibility and preliminary effectiveness of mobile cognitive control training during basic combat training in the military. Mil. Psychol. **34**(1), 55–67 (2022)
10. Balzarova, M.A.: Blockchain technology–a new era of ecolabelling schemes? Corp. Gov. Int. J. Bus. Soc. **21**(1), 159–174 (2021)
11. Mishra, N.K., Raj, A., Jeyaraj, A., Gupta, R.: Antecedents and outcomes of blockchain technology adoption: meta-analysis. J. Comput. Inf. Syst.Comput. Inf. Syst. **64**(3), 342–359 (2024)
12. Saadan, N.B.: Mapping blockchain adoption challenges: a bibliometric analysis. J. Muamalat Islam. Financ. Res. (2024). https://doi.org/10.33102/jmifr.576
13. Smith, C.D., et al.: Impact of mindfulness training and yoga on injury and pain-related impairment: a group randomized trial in basic combat training. Front. Psychol. **14**, 1214039 (2023)
14. Rawashdeh, A., Bakhit, M.: Exploring the mediating role of willingness to continue in AI-based data analytics adoption in audit firms. In: 2023 International Conference on Business Analytics for Technology and Security (ICBATS), pp. 1–8. IEEE (2023)
15. Shubailat, O., Al-Zaqeba, M., Madi, A., Ababneh, A.: Customs intelligence and risk management in sustainable supply chain for general customs department logistics. Uncertain Supply Chain Manag. **12**(1), 387–398 (2024)
16. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
17. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9

18. Pal, S., Díaz, V.G., Le, D.-N. (eds.): IoT: Security and Privacy Paradigm, 1st edn. CRC Press (2020). https://doi.org/10.1201/9780429289057
19. Mukhopadhyay, K., Chattopadhyay, S., Dutta, S.P., Bhattacharyya, S., Pal, S., Alzeyadi, A.K.: September. Recent advancement of block chain in health care. In: AIP Conference Proceedings, vol. 2845, no. 1. AIP Publishing (2023). https://doi.org/10.1063/5.0156992



Stock Market Prediction Using News Sentiment Analysis

Shikha Gupta[1(✉)], Shefali Arora[2], and Narendra Kumar[2]

[1] Department of Information Technology, Maharaja Agrasen Institute of Technology, Delhi, India
shikha.gpt1@gmail.com

[2] Department of Computer Science and Engineering, Dr. BR Ambedkar National Institute of Technology, Jalandhar, India
chouhansa@nitj.ac.in

Abstract. As people's demand for easy access to information grows, they increasingly use social media platforms like Twitter and Facebook to share, provide, and seek information. Every second, Twitter users send a vast number of tweets, which can be transformed into valuable information through sentiment analysis. A rapid and accurate classification model is needed to analyze large volumes of tweets, and this approach can be applied to stock price projections based on market-related tweets. Accurately predicting stock investment strategies is a significant challenge for investors. This paper uses sentiment analysis to develop models supporting investment decision-making in the Indian stock market. By employing the VADER model, we forecast investment strategies, arguing that sentiment analysis of headlines and tweets influences stock market values. During the research period, we collected headlines and stock market investment data, finding that the model accurately predicts investment strategies when applied to Sensex.

Keywords: Sentiment Analysis · Twitter · Stock Market Prediction · VADER Model · Sensex Investment Strategies

1 Introduction

Stock price prediction forecasts future stock prices based on past prices, aiding investors in maximizing trading profits. There are two traditional approaches: technical analysis, which identifies patterns from historical data, and fundamental analysis, which considers the overall economy, a company's financial condition, and management [1]. This task is highly challenging due to the stock market's volatility, non-linearity, and dynamic nature, influenced by factors like political conditions, economic situations, trends, seasonality, and investor psychology. Twitter, a popular social media platform, receives up to 55 million tweets daily, offering valuable data for analysis. Sentiment analysis, which classifies tweets into positive, negative, or neutral, is crucial for understanding public opinion [2]. Various methods like naïve Bayes regression, support vector machines, and deep learning have been used for sentiment analysis, with the accuracy of deep learning algorithms depending on the training data [1].

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 238–246, 2025.
https://doi.org/10.1007/978-3-031-91008-1_22

Predicting stock market prices remains a significant interest for analysts and researchers due to its inherent unpredictability and the influence of numerous economic and political factors. This paper forecasts the stock market in real-time using a combination of Vader and LSTMs.

1.1 Objectives

The ultimate objective of this project was to develop an algorithm to predict the stock prices for future days using previous news tweets. This is done with the steps such as data cleaning, pre-processing and application of forecasting models. With LSTM and VADER we achieve an accurate prediction of the stock prices.

2 Related Work

In [3] B. Liu, describes the sentiment analysis or opinion mining as the process of automatically comprehending, extracting, and processing textual data to gather information about the emotions expressed in an opinion statement. Sentiment analysis is used to discover a proclivity for an opinion or opinion, regardless of whether that opinion or opinion is likely to be negative or good about someone's problem or goal [4]. Sentiment analysis, for example, is used to classify the polarity of a document, sentence, or feature text. That is, it determines if a document, sentence, or function expresses a positive, negative, or neutral opinion [5]. Different scenarios can be predicted using this polarity and stock is one of them.

VADER (Valence Aware Dictionary and Sentiment Reasoner) is a sentiment analysis tool designed for social media, using a lexicon of words classified by their semantic orientation as positive or negative [6]. VADER not only indicates positivity and negativity but also measures their intensity. It calculates a compound score, which is the normalized sum of all lexicon scores, ranging from -1 (most negative) to $+1$ (most positive) [12]. Sentiment classifications are: positive (compound score ≥ 0.05), neutral (compound score between -0.05 and 0.05), and negative (compound score ≤ -0.05). Deep learning [7] is a field of scientific learning in which computers are taught to perform behaviours that are deemed natural by humans using artificial neural networks (ANNs). For instance, to learn from an example. Deep learning allows computers to learn classifications directly from images, sounds, texts, and even films [5]. Computers are used to label and learn on a large number of datasets. The dataset can be used to convert the image's pixel values to an internal representation or feature vector. Classification can be used to identify and categorise input patterns. Deep learning is a method of learning a multi-level expression that develops a neural network architectural field with several layers [4]. Sequence prediction has long been a challenging problem in data science [8], encompassing tasks like forecasting sales, analyzing stock market patterns, understanding movie plots, speech recognition, language translation, and predicting the next word on a keyboard. Recent advancements have shown that long short-term memory networks (LSTMs) are highly effective for these tasks, outperforming traditional feed-forward neural networks and RNNs due to their ability to selectively remember patterns

over long periods [9]. This paper explains LSTMs and demonstrates their application to real-world problems.

There are multiple ways to gather datasets for research. In previous studies, a program was created to automatically collect tweets by searching Twitter for emoticons that signify "positive" (e.g., ":)", "") and "negative" (e.g., " = (", ":("). Some researchers manually annotate their own databases, a time-consuming task. A balanced dataset is necessary, with an adequate number of positive tweets for accuracy. We identified a dataset of 1,578,612 English tweets from Kaggle and Sentiment 140, containing columns for ItemID, Sentiment, Sentiment Source, and Sentiment Text. The Sentiment column is binary: 0 for negative and 1 for positive. The dataset presents challenges such as acronyms ("Gf" for "girlfriend" or "Great"?), repeated letter sequences ("Juuuuust"), emoticons, spelling mistakes, and modern writing ("wr doinit"). Emotions are also conveyed through nouns, actions (laughs), and negations ("can't"). These elements make sentiment analysis complex. For better understanding, visualizing the dataset shows 790,176 positive and 788,434 negative tweets, nearly perfectly balanced. Duplicates have been removed. Key Twitter terminology includes: Hashtag: Words or phrases with the # symbol, linking to similar tweets. @user-name: Identifiable usernames preceded by the @ symbol (e.g., @KleinCarly). MT: "Modified Tweet", a retweet with changes. Retweet (RT): Sharing someone else's tweet with your followers. Emoticons: Punctuation and letters conveying emotions (e.g., ":p:/:(").

3 Methodology

The procedure of making a model for sentiment analysis in testing has five stages:

3.1 Data Retrieval

To access data from Twitter, connect to the Twitter API by building a Twitter application at https://apps.twitter.com/ and obtaining the required key and access token. Use a Python library like Tweepy to implement Twitter API calls. Install the Tweepy library in Spyder and utilize the Twitter API to retrieve tweets using hashtags or keywords. The recorded tweets are in English and come from regular users or official Twitter accounts.

Tweets from the popular @NDTVProfit news were taken using the TwintScraper Library. Historical data is used for the last 5 years, that is from January 1, 2015 to December 31, 2019. Nifty50 stock data and news from popular Twitter handles are indexed in this index. Historical data on Nifty50's stock price over the last 20 years, dBbeautifulSoup according to investing.com). Figure 1 shows the Nifty-50 index data over the fifteen-year period.

3.2 Pre-processing

TextBlob library is then used to collect the data from Twitter and is pre-processed, which includes a tweet cleaning process and a tweet classification process based on negative, positive, or neutral mood classes. The goal of data preprocessing [10] is to convert raw data into an analysis-ready format. Figure 2 depicts the process of data pre-processing.

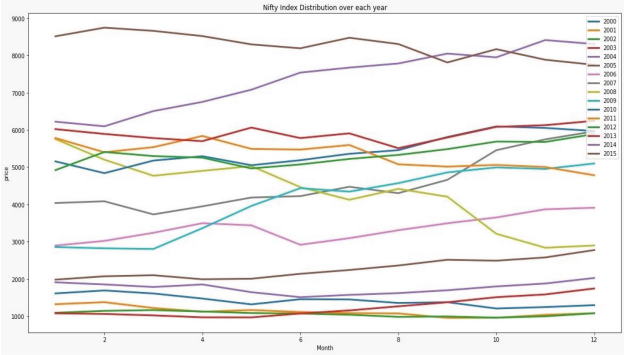


Fig. 1. Distribution of data

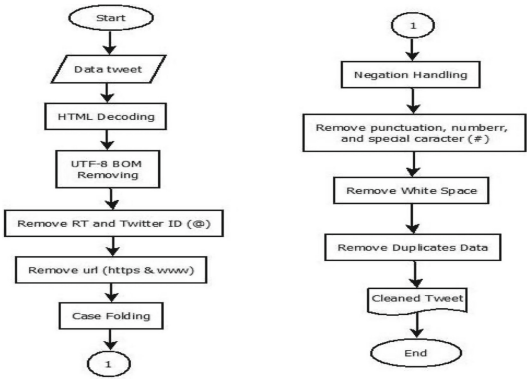


Fig. 2. Data pre-processing

3.3 Cleaning Data

Twitter is a social media platform where the grammar of a language is not accounted. We expect tweets to be written in the official language because this is a news station. Figure 3 visualizes the same.

Subsequent operations on the tweets have been carried out such as:

- Change into lowercase
- Separate all of the hyperlinks beginning with both http or pic.twitter.com or https.
- Detach all of unique characters, emotions.
- Undo all of the hashtags (#), (@) symbol.
- Eliminate words such as: ETMarkets, money control, market update, biznews, NewsAlert, click right here for some LIVE upcoming events.
- Get rid of all of the numbers.

Following the cleaning, we'll combine all of the tweets into a single paragraph for each day.

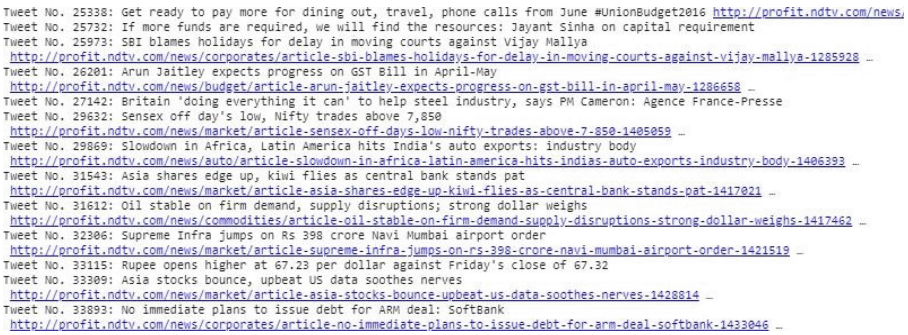


Fig. 3. Data cleaning

3.4 Model Design and Training

The polarity is then calculated using the data that has undergone a cleaning process and has been classified using the TextBlob library. This polarity with the NIFTY50 price of the LSTM model is used to predict the price of the stock.

3.5 Split Dataset

All the data that is training, validation, and test taken from the tweets is identified as emotion classes are then utilised to predict market movements. The split train test method of the Python package, Scikit-learn, was used to split the data in this study. The information is separated into three sections [11]:

1) Data train: A dataset utilised by classifier model for learning process.
2) Data validation: A dataset applies to a classifier framework and given a disinterested assessment of the project.
3) Data test: A dataset usage for evaluation of the show for the last model. Since this is time series data, it cannot be split randomly. As a result, think of the final 20.ta as a test set and the first 80.ta as a move set. Test data form: (3977, 2), train data form: (3977, 2) (995, 2). Figure 4 depicts the price distribution.

3.6 Research Method

3.6.1 Designing the VADER Model

Each information headline has been broken down into sentences. Furthermore, the statements are broken down into phrases to determine the VADER ratings based entirely on the positive terrible rating in addition to the depth of feelings thinking about the subsequent five heuristics: Punctuations, Capitalization, Degree Modifiers, Conjunctions and Polarity Negation. The final score is generated as the average of the individual scores, and the polarity is obtained by mapping the scores to the thresholds. It maps the combined final score to the threshold and classifies it as positive, negative, or neutral. The next step is to compare the composite score to the threshold and determine the text's

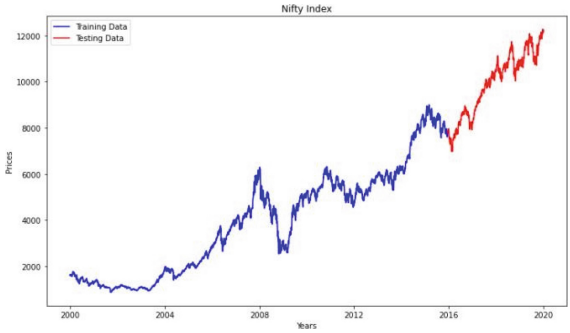


Fig. 4. Price distribution for training and test data

polarity. To determine polarity, apply the following rule [12]. The text emphasizes positive sentiments if the compound value is greater than 0.6. A neutral composite score ranges from 0.5 to 0.54. If the total score for & lt; is 0.5, the text has a negative tone. The VADER score is given between −1 and +1. The graph shown below defines the score for each data set and the probability of the score that the VADER algorithm has assigned to the dataset. Figure 5 shows the probability of distribution of scores using VADER.

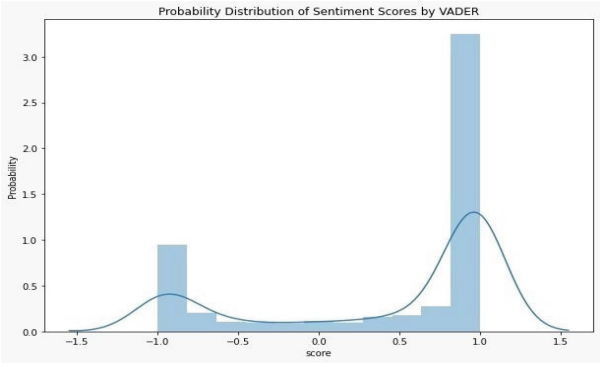


Fig. 5. Probability distribution of sentiment score by VADER

3.6.2 Visualization and Results

VADER distributed the text and the words in the tweets into positive, neutral, and negative. This is just a representation of the words used. The average word count can be increased by using more tweets. This will enhance the research result. Figure 6 visualizes the count plots based on the achieved scores.

3.6.3 Design of Long Short Term Model

LSTM model was used to create a model with VADER. NIFTY-50 data was first trained and tested to predict the NIFTY-50 prices for the next 20 years. To make data, the

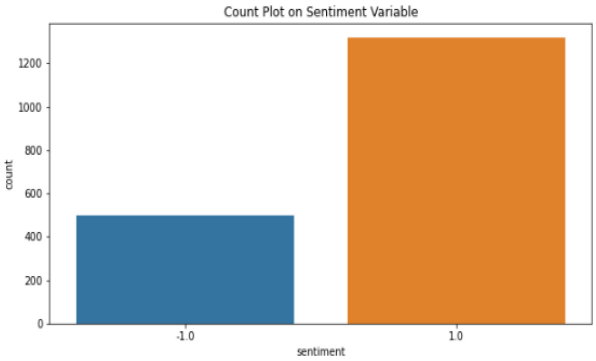


Fig. 6. Count plot for VADER polarity calculation

data of the stock price is first scaled with MinMaxScaler. Provides LSTM60 functions. Consecutive stock prices for the last 60 days as a characteristic of X = 60. Y = Current stock price on the 61st day. This model was then enhanced with VADER. The polarity of tweets calculated with VADER was then used to create a data set of date, Stock price, words and VADER polarity altogether. This data set was then trained and tested using LSTM to predict the stock prices [4]. This model uses only 5-year inventory data. There is only 5 years of news from 2015 to 2019. This model employs 61 features. X = 60 features on day 60 and stock prices over the last 60 days as news sentiment. Y = Current stock price on the 61st day. Once more, every single stock price is scaled. Figure 7 visualizes the results of prediction.

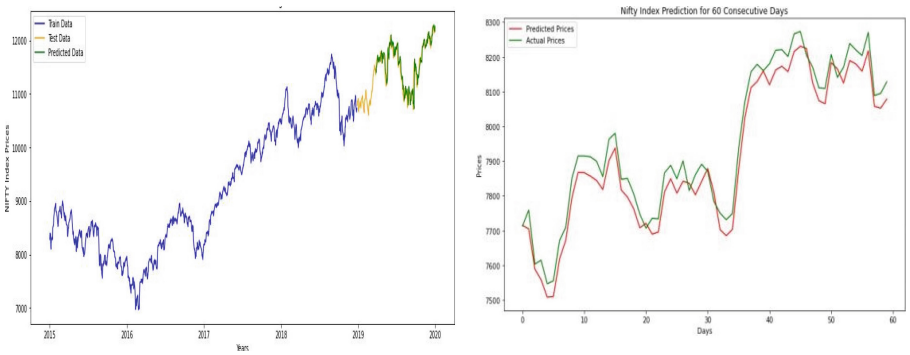


Fig. 7. NIFTY-50 stock prediction using VADER and LSTM model

4 Results and Discussion

The ultimate goal of this project was to develop an algorithm to predict the stock prices for future days using previous NEWS tweets. This was done with the steps performed. With LSTM and VADER we could achieve an accurate prediction of the stock prices. The

root mean square error of the task was 44.35 and the task for each day was concluded in 3640 ms. A quantization process has been performed to perform the task faster. Quantization is a technique for performing calculations and storing tensors with bit widths that are smaller than the precision of floating point numbers. Instead of using a floating point number, the quantization model uses an integer tensor for some or all operations. This allows the model to run faster, but accuracy suffers as a result. This accelerated the process, but the RMSE rises to 67.62 as shown in Fig. 8.

Model	Time Taken to Predict	RMSE
Regular Model: Single Day Price Prediction	649 ms	-
Regular Model with Quantization: Single Day Price Prediction	60.8 ms	-
Regular Model: 60 days Price Prediction	3640 ms	44.35
Regular Model with Quantization: 60 days Price Prediction	472 ms	67.62

Fig. 8. Results

5 Conclusion and Future Work

The goal of this paper is to develop an algorithm to predict the stock prices for future days using previous NEWS tweets. This was done with the steps performed. With LSTM and VADER we could achieve an accurate prediction of the stock prices. Based on the inference outcomes, several steps are proposed for further advancement and growth. First, collecting more data, such as news data spanning more years and obtaining hourly stock data instead of daily data, will provide additional points for a more comprehensive market analysis, enhancing precision. Improving model accuracy can be achieved by utilizing the LSTM architecture and optimizing hyperparameters. Training a custom model, rather than using a pre-trained VADER sentiment analyzer, can deliver better emotional results as it is tailored to stock market news language. Additionally, incorporating GANs (reinforcement learning) can enhance stock market predictions, as suggested by recent research. A custom sentiment analyzer can help manage anomalies more effectively by retraining data with correct sentiment scores. Finally, quantizing the model to speed up predictions, although this will significantly reduce accuracy.

References

1. Ratnawati, F., Winarko, E.: Sentiment analysis of movie opinion in twitter using dynamic convolutional neural network algorithm. IJCCS **12**(1), 1–10 (2018)
2. Zhang, Y., Wallace, B.: A sensitivity analysis of (and practitioners' guide to) convolutional neural networks for sentence classification (2015). arXiv preprint arXiv:1510.03820
3. Liu, B.: Sentiment analysis and subjectivity. Handb. Nat. Lang. Process. **2**(2010), 627–666 (2010)
4. Sattikar, A.A., Kulkarni, R.V.: Natural language processing for content analysis in social networking. Int. J. Eng. Invent. **1**(4), 6–9 (2012)
5. LeCun, Y., Bengio, Y., Hinton, G.: Deep learning. Nature **521**(7553), 436–444 (2015)

6. Bui, V., Chang, L.C.: Deep learning architectures for hard character classification. In: Proceedings on the International Conference on Artificial Intelligence (ICAI), p. 108. The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp) (2016)
7. Devikar, P.: Transfer learning for image classification of various dog breeds. Int. J. Adv. Res. Comput. Eng. Technol. (IJARCET) **5**(12), 2707–2715 (2016)
8. Refianti, R., Mutiara, A.B., Priyandini, R.P.: Classification of melanoma skin cancer using convolutional neural network. Int. J. Adv. Comput. Sci. Appl. **10**(3), 5 (2019). https://doi.org/10.14569/IJACSA.2019.0100353
9. Esteva, A., et al.: Dermatologist-level classification of skin cancer with deep neural networks. Nature **542**(7639), 115–118 (2017)
10. Brinker, T.J., et al.: Skin cancer classification using convolutional neural networks: systematic review. J. Med. Internet Res. **20**(10), e11936 (2018)
11. Mohan, S., Mullapudi, S., Sammeta, S., Vijayvergia, P., Anastasiu, D.C.: Stock price prediction using news sentiment analysis. In: 2019 IEEE fifth international conference on big data computing service and applications (BigDataService), pp. 205–208. IEEE (2019)
12. Gupta, S., Agarwal, M., Jain, S.: Automated genre classification of books using machine learning and natural language processing. In: 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 269–272. IEEE (2019)

Global IoMT Data Analysis Through AI-Driven Governance Framework

Souvik Pal[1,2(✉)], B. Srividhya[3], Saikat Maity[2], A. Thilaka[4], A. Poongodi[5], and N. Madhumitha[6]

[1] Department of Management Information Systems, Saveetha College of Liberal Arts and Sciences, Saveetha Institute of Medical and Technical Sciences, Chennai, India
Souvikpal22@gmail.com

[2] Department of Computer Science and Engineering, Sister Nivedita University (Techno India Group), Kolkata, India
saikat.ma@snuniv.ac.in

[3] Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu 603203, India
srividhb@srmist.edu.in

[4] Department of Computer Applications, SRMIST, Kattankulathur, India
thilakaa@srmist.edu.in

[5] Department of Computer Applications, Vels Institute of Science, Technology and Advanced Studies, Chennai, India
apoongodi.scs@velsuniv.ac.in

[6] Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, India

Abstract. The pharmaceutical industry strives for the shortest feasible speed to market for novel pharmaceuticals because of the finite monopolistic period granted by the protection of patents, which is utilized to recover the expenditures for research and development. Yet, the result of investigations is unpredictable, and talks with regulators are growing tougher, rendering entering the market a more significant challenge; hence, this procedure is becoming increasingly volatile. Hence, this paper proposes International Market Entry and Expansion using the Artificial intelligence assisted Governance Framework (AI-GV) for Pharmaceutical Products (GV-PP). Improving approaches utilized to prepare for this critical operation is the main focus of the dissertation. After thoroughly analysing the procedure in an empirical investigation, multiple flaws in the industry's present planning methodologies are discovered. The next step is to build a model that will support the important operational decisions that will be made before the market launch. The approach considers a number of crucial industry parameters as well as the possibility of volatility. Several discoveries on risk bundling and maintaining a rapid time-to-market are derived from the model. Additionally, an inventory management approach for a novel medication delivery method is created, as the capability for secondary pharmaceutical manufacturing is crucial for the product's availability. Considering the accumulation of inventory, facility confirmation, and restricted longevity, it more accurately represents the ramp-up period. They provide a few perspectives on ramp-up administration and evaluate the operation of multiple start-up procedures. Completing the prior sections and describing

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 247–257, 2025.
https://doi.org/10.1007/978-3-031-91008-1_23

future study options, the doctoral dissertation concludes by displaying the latest recommended organizational framework.

Keywords: International Market Entry · Artificial intelligence assisted Governance Framework (AI-GV) · Pharmaceutical Product (PP) · Pharmaceutical manufacturing

1 Introduction

One way to measure an organization's growth in innovation is to look at its manufacturing life cycles. Development, launch, growth, maturity, and reduction are the traditional stages of a product's life cycle. The organization's competitiveness determines the usual elements in these phases. In keeping with protection, ecological, and environmental requirements, and the quality of the goods created, different functional departments within the organization will carry out the processes, covering research and development, production, and marketing associations, regardless of the domain [1, 2]. In this setting, a supply chain—which encompasses all the administrative, functional, and value-adding tasks involved in producing goods and delivering them to consumers—plays a crucial role. Every step of the process, from initial ideation to final transportation to the patient, retail medicine, or hospital, is included in a pharmaceutical supply chain [3, 4].

Options about supply chain design, such as manufacturing and distribution network organization, financial revenue, advertising approaches, goods and technological advances, portfolio oversight, and the distribution of investment dollars and financial viability, inform these entities' choices [5]. Strategic choices in this context must include the operational and tactical tiers of the whole product range, engage many functional units, and deal with the different stakeholders [6, 7]. Drug producers, wholesalers, retailers, hospitals, MCOs, and insurance organizations are just a few of the essential parties involved in the pharmaceutical industry that make the situation more complicated [8–10]. Pharmaceutical companies design and manufacture disease-fighting drugs. Creating novel drugs, making active ingredients, and making distribution methods are three of the most essential things in the pharmaceutical industry. Complex alliances and cooperation have increased. Most small businesses in this area concentrate on innovative therapy development or generic drug manufacturing. Big pharms develop innovative pharmacological remedies. Thus, the article concentrates on them [11, 12].

- The process of identifying the relevant hazards.
- A two-stage stochastic AI-GV-PP model is being proposed to address market launch planning and the recognized risks in the pharmaceutical business. To keep the model manageable, it will include all essential levels of the supply chain and take advantage of the model's structure.
- To validate our modelling approach, they are conducting a numerical analysis using a real-world industry case.

Section 3.3 analyses the relevant literature, Sect. 3.4 analyses the suggested approach, Sect. 3.5 delves into the numerical analysis, and Sect. 3.6 wraps up the accompanying documentation.

2 Literature Survey

This study uses the ARIMA model, which was introduced by to try to forecast the stock values of a few Indian pharmaceutical businesses included under the NIFTY100 index. The findings might inform further in-depth analyses of stock values and their forecasts in future studies.

In their study, [13] suggested that we cover the important medical device programs outlined in the Regulatory Science Action Plan (RSAP) of the National Medical Products Administration of China (NMPA) and the most recent regulations that try to keep individuals secure and promote creativity in the field of medical devices. Here we outline the key points of the new rules before diving into the potential avenues for translational studies, such as those involving technologically tailored gadgets, drug-device combination goods, software powered by artificial intelligence, surgical robots, and nanomaterials used in medical devices. Lastly, researchers planning to enter the Chinese medical device industry with their inventions are given a regulatory viewpoint.

The goal of the study by [15]. To reach this aim, pharmaceutical companies must determine how AI affects their main and supplementary business activities. The pharmaceutical companies in our qualitative interview study were large, medium, and small. They examined the scant literature on AI's influence on the pharmaceutical industry to discover which business processes are changing and how. AI strongly affects HR business operations, research and development, IoMT data analysis and reporting, and master IoMT data preservation in small pharmaceutical companies, according to the study. Major pharmaceutical companies are transforming their analytical, sales, marketing, and manufacturing processes using AI. Medium-sized enterprises tailor process transformation to their strengths.

The idea of Pharma 4.0 is supported by the ideas of process analytical technology and quality by design, according to [16]. Strong, efficient, and fast manufacturing may be possible with them. Biopharmaceutical production, healthcare infrastructure, and medical technology all make use of Industry 4.0. A significant part is played by digital transformation. Improved tools for enforcing product safety and supply chain security are provided by Pharma 4.0. Analysis of AI-driven Internet of Medical Things data Related ideas [17–22] have been delineated, facilitating the preparation of performance analysis in the healthcare industry.

3 Proposed Framework

Miniature plants that produce a single chemical are one kind of facility that might be utilized to make pharmaceuticals. A second kind of facility is a massive integrated complex that uses many processes to create multiple compounds. Smaller facilities tend to make up the bulk of pharmaceutical manufacturing facilities. An organic compound is the building block of raw materials on top of their utility as solvents. Batch activities are used in the manufacturing of almost all products. On top of that, different goods or intermediates may be produced using the same equipment at different times throughout the year. Unless the object in issue is mass-produced, it is unusual to come across equipment that is tailored to make a single item.

The biological mechanism comprising pharmaceuticals includes active pharmaceutical ingredients (APIs) and additional synthetic active components, intermediates, and basic elements (See Fig. 3.1).

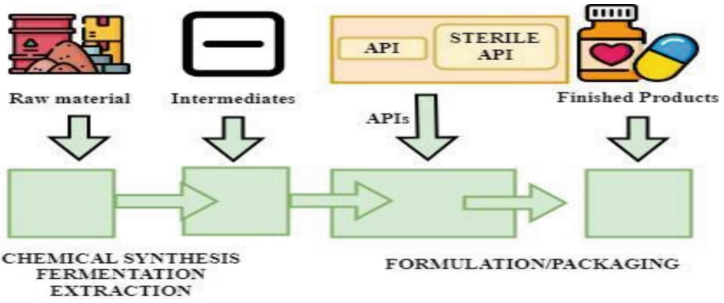


Fig. 1. Process flow diagram for the pharmaceutical sector

- At all times, in every nation, and maybe even inside any particular plant, a minimum of a single production procedure shown in the flow diagram in Fig. 1 is being carried out.
- Several firms are "outsourced" to handle the manufacturing in the pharmaceutical sector. All the building components seen in Fig. 1, top level, are part of this.

The production of an active pharmaceutical ingredient (API) begins with the creation of an intermediate, which must undergo further chemical processing or purification before it can be considered an API. An API is a physiologically active component or compound used in medication formulations to provide a therapeutic effect.

3.1 AI Assisted Hazard Model

Assume a scenario where periods $(p_{l-1}, p_l), l = 1,2, \ldots, n+1, p_o = ()\, and\, p_{n+1} = \propto$ are used for organizing the time to market entrance and the moment the entry in the interval p_{l-1}, p_l is documented as p_l. It follows that firm $j, j-1,2, \ldots, O$, joined the market in the time $l_j \in 1,2, \ldots, n+1$. as these times are consistent across all firms. Furthermore, IoMT data is accessible on a $1 \times m$ matrix of variables $Y_j(l), j = 1,2, \ldots, O, l = 1,2, .., n+1$, for every company at every time period. These variables, which include company and market dynamics, are believed to be consistent throughout all time periods; nonetheless, may fluctuate over periods. With regard to regresses Y_j, let $g(p, Y_j, \theta)$. denote the fundamental quantity of periods.

The chance of entering a market may thus be described by the following Eq. (3.1):

$$\lambda\left(p, Y_j, \theta\right) = \frac{g\left(p, Y_j, \theta\right)}{\int_p^{\infty} g\left(v, Y_j, \theta\right) ev} = \frac{g\left(p, Y_j, \theta\right)}{T\left(p, Y_j, \theta\right)}. \tag{3.1}$$

The longevity operation, shown as $T\left(p, Y_j\right)$ above, stands for the nonentry possibility. Since company j failed to complete the initial $(l-1)$ periods, the likelihood that it will skip the *lth* periods is indicated by following Eq. (3.2).

$$\begin{aligned} Qs(p \geq \backslash\backslash p \geq p_{l-1}; Y_j, \theta &= \frac{T\left(p_l, Y_j, \theta\right)}{T\left(p_{l-1}; Y_j, \theta\right)} \\ &= exp\left[\left| - \int_{p_{l-1}}^{p_l} \lambda\left(v, Y_j, \theta\right) ev\right|\right] = b_l\left(Y_j, \theta\right). \end{aligned} \tag{3.2}$$

In this instance, the parameters of the vector θ are unknown. The probability contribution for entrance in the interval is $[p_{l,-1}, p_l]$ for a completed observation, meaning a business that joins the market during the observation period follows Eq. (3.3).

$$\left[1 - \frac{T\left(p_l, Y_j, \theta\right)}{T\left(p_{l-1}; Y_j, \theta\right)}\right] \prod_{k=1}^{l-1} \left[\frac{T\left(p_k, Y_j, \theta\right)}{T\left(p_{k-1}, Y_j, \theta\right)}\right] = \left[1 - b_l(Y_j, \theta)\right] \prod_{k=1}^{l-1} \left[b_k(Y_j, \theta)\right] \tag{3.3}$$

The likelihood of the j th company entering the interval p_{l-1}, p_l is represented by the first term in the bracket above, while the chance that the identical business wasn't part of each of the preceding $l-1$ periods is represented by the second equation. The probability for a sample of O businesses may be calculated by multiplying the variables in Eq. (3.3) by j. A value for variable δ_j may be readily introduced to manage information restricting. It should be set to 1 for fulfilled observes (firms that joined the market by the conclusion of each observe phase) and a value of 0.

It also assumes, for the sake of convenience, that restricting, if it happens, starts at the start of the final measurement interval and that the filtering process exists independently of the variables θ that are of interest. According to Eq. (3.3), the log-likelihood of the information $\left(p_j, \delta, Y_j\right), j = 1,2, \ldots, O$ is following Eq. (3.4)

$$M(\theta) = \sum_{j=1}^{O} \left\{ \delta_j Io\left[1 - b_{kj}\left(Y_j, \theta\right)\right] + \sum_{k=1}^{l_j - 1} Io\left[b_k\left(Y_j, \theta\right)\right] \right\} \tag{3.4}$$

Parameterizing the -operate in the probability Eq. (3.4) is necessary to finish the model definition. To a certain extent, the inverse AI assisted Hazard model provides a generic approach. The model specifies the hazard rate as follows Eq. (3.5) based around dependent variables:

$$\lambda(p, Y, \theta) = \lambda_0(p) exp(Y, \beta) \tag{3.5}$$

In when $\lambda_0(p)$ denotes the baseline danger and θ contains β and the variables for $\lambda_0(p)$. The framework breaks down the correlate conditional hazard into two parts: the first part shows the effect of time dependency alone, and the second part demonstrates the way variables affect the hazard rate. The probabilities parameters given in Eq. (3.5)

for Cox's AI assisted Hazard model have parameters as follows: Eq. (3.6).

$$\begin{aligned} b_j(Y_j, \theta) &= exp\left[| - \int_{p_{l-1}}^{p_l} \lambda(v, Y_j, \theta) ev | \right] \\ &= exp\left[| - \exp(Y_j, \beta) \int_{p_l - 1}^{p_l} \lambda_0(v) ev | \right] \\ &= exp\left[| - \exp(Y_j, \beta) + Io \int_{p_l - 1}^{p_l} \lambda_0(v) ev | \right] \\ &= exp\left[| - \exp(Y_j, \beta + \gamma_l) \right] \end{aligned} \tag{3.6}$$

The $1 \times (l + n + 1)$ variable vector is (γ, β), while $\gamma_l = lo \int_{p_l - 1}^{p_l} \lambda_0(v) ev$ and θ are the values. This IoMT data grouping in log-likelihood Eq. (3.7) results from the aforementioned description.

$$M(\theta) = \sum_{j=1}^{O} \left\{ \delta_j Io\left[1 - \exp\left\{-\exp(Y_j, \beta + \gamma_l)\right\}\right] - \sum_{k=1}^{l_j - 1} exp(Y_j, \beta + \gamma_l) \right\}. \tag{3.7}$$

Bear in mind that the log-likelihood in Eq. (3.7) is built using variations in the Marketing function. Reason being, although the exact time of admission is a mystery, the intervals in which it occurs are known. For the purpose of marketing the likelihood, researchers often use density functions, carrying on as if the durations were continually watched. In light of what has already been said, this could cause to biased estimations and perhaps faulty qualitative predictions. Second, consistent parameter estimation is still feasible even without a known baseline hazard due to the nonparametric nature of the baseline hazard definition. However, if the assumed parameterization turns out to be incorrect, the estimates provided by the conventional method—which assumes a parametric form for the baseline hazard—would be inconsistent. As grouping intervals approach 0, the "proportional-hazard" Cox model with time-varying variables is best. It estimates baseline hazard using nonparametric criteria, but it uses a special functional form to indicate variable effect, making it semi-parametric. In summary, this is the most crucial step. This suggests that IoMT data-driven factors significantly affect model estimation. Baseline hazard should cover variable mean changes over time.

4 Results and Discussions

The research found that governance structure improves entrance modalities, which impacts strategic alliances and joint ventures. Effective worldwide growth requires market adaptation and risk management. The IoMT data demonstrate the need of linking governance initiatives to global pharmaceutical industry changes as a starting point for discussion. Working together and following industry standards may help companies overcome difficulties, penetrate markets, and develop a permanent presence outside.

IoMT Dataset Description. APIs provide communication and integration across healthcare applications, services, and platforms [17]. API administration requires common protocols, security measures, and documentation to ensure IoMT data flow is secure and efficient while meeting privacy and industry requirements. API management in healthcare increases cooperation, streamlines procedures, and helps establish innovative healthcare solutions and services by facilitating IoMT data interchange and interoperability.

4.1 Time Authorization and Best Case Demand

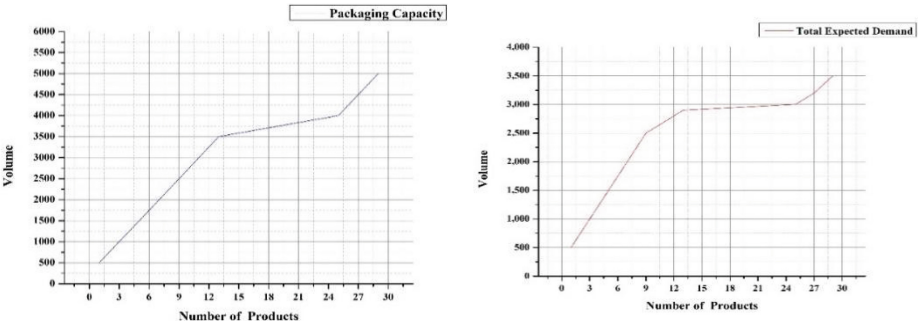


Fig. 2. (a): Increase in packaging capacity. (b): Aggregated expected demand

The conditions and market statistics are determined by the company, the new pharmaceutical type, and other factors. In order to accommodate this variability, a great deal of problematic scenarios had to be developed. They have been able to construct IoMT data intervals for particular markets across many Asian market areas; this was made possible by scaling the IoMT data. The approval process is common (via the Asian Medicines Agency), but authorization procedures are autonomous, which distinguishes Asian Markets from other markets. The aggregated expected demand with on-time authorization is shown in Fig. 2(a) and 2(b), respectively, along with the practical case demand for all markets, as well the increase in packing capacity.

Figure 3(b) shows a substantial association between the number of operational guidelines issued and the number of pharmacies that opened. This shows that standardized practices are necessary for efficiency and consistency in an increasing pharmacy network. Pharmaceutical companies must create efficient and scalable inventory management methods as drugstore outlets proliferate. Figure 3(a) suggests that hospital population expansion improves patient satisfaction. If the hospital wishes to satisfy everyone, it must expand its facilities and improve its services. The graph illustrates if healthcare facility expansion is linked to patient satisfaction.

The legal distribution of these medications is becoming more challenging due to the increasing number of pharmaceuticals. Figure 4 is a result of the rising complexity and conformance demands of regulations. This shows how important it is for pharmaceutical companies to have solid legal procedures to manage their various products. As the number

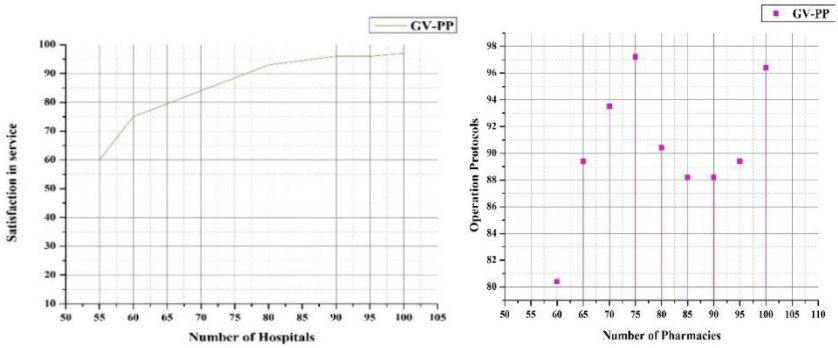


Fig. 3. (a): Hospital service satisfaction. (b): Operation protocols in Pharmacies.

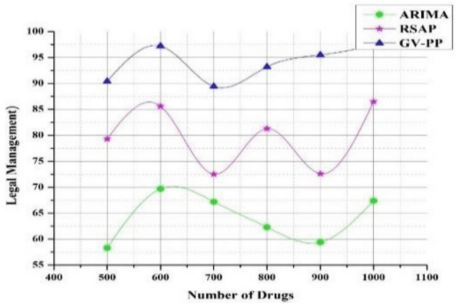


Fig. 4. Legal Restrictions

of pharmaceuticals in a portfolio rises, it becomes more important to actively handle legal matters in order to effectively navigate the legal environment.

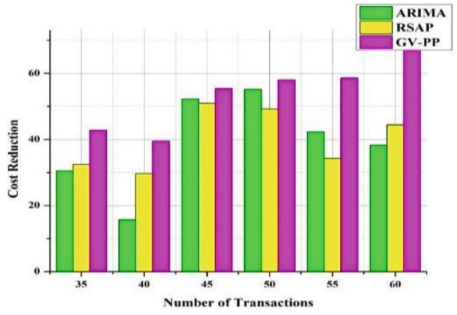


Fig. 5. Transaction costs

Costs fall in direct proportion to the number of transactions, suggesting an inverse link between the two. Figure 5 shows that as transaction volume increases, economies

of scale kick in, leading to a more cost-effective company strategy. Organizations may use the graph to increase expenditure and transaction volume.

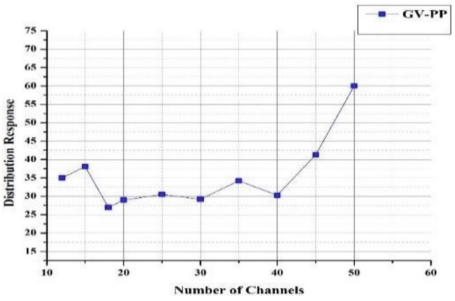


Fig. 6. Distribution through Integrated Channels

Figure 6 shows the number of channels increases, the distribution response improves when the slope is positive and decreases when the gradient is negative. Pharmaceutical distribution may be more responsive and efficient with more outlets. The best graph's optimal point maximizes distribution response relative to channel count. More channels probably won't work when complexity and resource allocation climb over this level. The graph shows that pharmaceutical distribution must balance efficiency and reactivity.

5 Conclusion

This chapter has covered all the bases, including topics such as the many difficulties encountered by the pharmaceutical industry's supply chain and the methodologies and technologies that make supply chain modelling possible. Building a worldwide supply network is difficult. Many "multilevel" components need to be examined, but we are moving toward a more efficient, agile, and responsive supply chain. Optimization might be based on variables, states, objectives, or uncertainties. Recently advanced stem cell research, nanotechnology, and tissue regeneration have increased the availability of these commodities, raising their prices. Novel treatments and equipment will be harder to build and transport than typical chemical units. Despite tighter controls, the digital revolution has increased demand for tailored care. Other industrial processes must be modified to reduce environmental effect. Physical activity and hydration are required before these therapies. Digital engineering is critical for these components because it validates procedures and restructures production infrastructure quickly. Processing must be sturdy and adaptable, and components must be small, modular, and easy to install or remove. Pharmaceutical businesses would likely manage commodities and marketplace supply chains, adjust to demand changes, and cut manufacturing costs. As healthcare digitizes, electronic health IoMT data, prescriptions, and remote monitoring will become more important in the supply chain. This lets us transmit more goods more places. Market relevance is rising, making these difficulties harder to solve. Risk management and compliance will grow with the supply chain.

References

1. Ryan, P., Buciuni, G., Giblin, M., Andersson, U.: Subsidiary upgrading and global value chain governance in the multinational enterprise. Glob. Strateg. J. **10**(3), 496–519 (2020)
2. Atrizka, D., Lubis, H., Simanjuntak, C.W., Pratama, I.: Ensuring better affective commitment and organizational citizenship behavior through talent management and psychological contract fulfillment: an empirical study of Indonesia pharmaceutical sector. Syst. Rev. Pharm. **11**(1), 545 (2020)
3. Reddy, S., Allan, S., Coghlan, S., Cooper, P.: A governance model for the application of AI in health care. J. Am. Med. Inform. Assoc. **27**(3), 491–497 (2020)
4. Gereffi, G.: What does the COVID-19 pandemic teach us about global value chains? The case of medical supplies. J. Int. Bus. Policy **3**, 287–301 (2020)
5. Abbas, K., Afaq, M., Ahmed Khan, T., Song, W.C.: A blockchain and machine learning-based drug supply chain management and recommendation system for smart pharmaceutical industry. Electronics **9**(5), 852 (2020)
6. Aruru, M., Truong, H.A., Clark, S.: Pharmacy Emergency Preparedness and Response (PEPR): a proposed framework for expanding pharmacy professionals' roles and contributions to emergency preparedness and response during the COVID-19 pandemic and beyond. Res. Social Adm. Pharm. **17**(1), 1967–1977 (2021)
7. Tobin, J.J., Walsh, G.: Medical Product Regulatory Affairs: Pharmaceuticals, Diagnostics, Medical Devices. John Wiley & Sons (2023)
8. Shahbahrami, E., Mahdiraji, H.A., Hosseinzadeh, M.: Prioritizing determinants of drug sustainable supply chain management in hospital pharmacies. J. Health Admin. **23**, 89 (2020)
9. Jamil, F., Hang, L., Kim, K., Kim, D.: A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics **8**(5), 505 (2019)
10. Cuypers, I.R., Hennart, J.F., Silverman, B.S., Ertug, G.: Transaction cost theory: past progress, current challenges, and suggestions for the future. Acad. Manag. Ann. **15**(1), 111–150 (2021)
11. Bel, G., Sebő, M.: Does inter-municipal cooperation really reduce delivery costs? An empirical evaluation of the role of scale economies, transaction costs, and governance arrangements. Urban Affairs Rev. **57**(1), 153–188 (2021)
12. Ketokivi, M., Mahoney, J.T.: Transaction cost economics as a theory of supply chain efficiency. Prod. Oper. Manag. **29**(4), 1011–1031 (2020)
13. Papalexi, M., Bamford, D., Breen, L.: Key sources of operational inefficiency in the pharmaceutical supply chain. Supply Chain Manag. Int. J. **25**(6), 617–635 (2020)
14. Song, X., Hu, M., Li, B., Zhang, K., Zhang, X., Wang, L.: Advancing medical device regulatory reforms for innovation, translation and industry development in China. J. Orthop. Transl. **37**, 89–93 (2022)
15. Hulstaert, F., Pouppez, C., Primus-de Jong, C., Harkin, K., Neyt, M.: Gaps in the evidence underpinning high-risk medical devices in Europe at market entry, and potential solutions. Orphanet J. Rare Dis. **18**(1), 212 (2023)
16. https://www.kaggle.com/IoMTdatasets/dinocojagadeeshr/analytics-for-hospitals-healthcare-IoMTdata
17. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2022)
18. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4
19. Balas, V.E., Pal, S. (eds.): Healthcare Paradigm in The Internet of Things Ecosystems. Elsevier (2020). https://doi.org/10.1016/C2019-0-00358-5

20. Rakshit, P., Nath, I., Pal, S.: Application of IoT in healthcare. In: Peng, S.L., Pal, S., Huang, L. (eds.) Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Intelligent Systems Reference Library, vol. 174. Springer, Cham (2020)
21. Pal, S.: Artificial intelligence-based IoT-edge environment for industry 5.0. In: Pal, S., Savaglio, C., Minerva, R., Delicato, F.C. (eds.) IoT Edge Intelligence. Internet of Things. Springer, Cham (2024)
22. Mukhopadhyay, K., Chattopadhyay, S., Dutta, S.P., Bhattacharyya, S., Pal, S., Alzeyadi, A.K.: Recent advancement of block chain in health care. In: AIP Conference Proceedings, vol. 2845, no. 1. AIP Publishing (2023). https://doi.org/10.1063/5.0156992

About Fuzzy Ideal of Unit Regular La-Semi Groups

Alaa F. Hameed and Akram S. Mohammed(✉)

Department of Mathematics, College of Computer Science and Mathematics, Tikrit University, Salahaddin, Iraq
akr_tel@tu.edu.iq

Abstract. The article aims to unit regular LA-semi-group, with the spot over a brands and application for fuzzy ideal with this algebraic mason. On unique kinds for fuzzy ideal ready in these semi-group. A core aims for our work are to given Fu. Le.id., Fu. Ri.id, and Fu. Qu. Id. With a realm for UR- LA-semi-group and we obtains for η is a Fu. (1,2) Id. In δ of the U- reg.LA-semi group δ with a Left Identity, then it is also a Fu. Qu.-Id. in δ., underscoring their importance in the expansive theory of LA-semi-group. A study deals with a attributes with connections between Fu. Id., such as Fu. Int. Id., Fu. Id., Fu. bi-Id., and Fu. (1,2) Id., UR- LA-semi-group and A fuzzy (1,2) ideal in δ is η iff it exists in a U-reg. LA-semi group δ with left identity. Using employing rigorous theoretical analysis and mathematical proof, the work given relation among diverse Fu. Id. With reveal their implication of algebraic structure for UR- LA-semi-group. This analysis given a behavior and nature for fuzzy structure in the field of the algebra. The results holds deep theoretical significance, sang our understanding for a field in Fu. Id. Plays in a algebraic scape for UR- LA-semi-group. This study is not only sustains the theoretical for fuzzy algebra but also opens new results tract of future work in the related field such as If η is fu.-$\mathcal{B}$ -id. of δ, then it is equivalent to being a fu. (1, 2) ideal in δ. Additionally, the study discuss and reforms the characteristics and connections between the fuzzy (1,2), fuzzy-ε, fuzzy-ideal, and fuzzy-$\mathcal{B}$-ideal.

Keywords: Semi Group · Regular · Unit · Group · Ideal · Fuzzy Set

1 Introduction

An LA-semi-group notion have been given in 1964 Nobusawa [13]. It is denoted by δ. An LA-semi-group, as defined in [14], is a groupoid where the element follows the left invertive law (u,v)w = (wv)u. In LA-semi-group, A medial law (uv)(wz) = (uw)(vz) hold for all u, v, w, z in δ. Also, LA-semi group satisfies (uv)(wz) = (zw)(vu) for all u, v, w, z in δ. A unit regular semigroup is a nonempty set where every element is unit regular. An element "a" is unit regular if there exists a unit element "u" such that a = aua [20]. A fuzzy subset of η ∘δ is a fuzzy LA-semi group of δ if η $(k_1, k_2) \geq$ η (k_1) ∧ η (k_2) whenever k_1, k ∈ δ [7]. A fuzzy subset η of δ is a fuzzy left (right) ideal if

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 258–268, 2025.
https://doi.org/10.1007/978-3-031-91008-1_24

$\eta(k_1, k_2) \geq \eta\ (k_2)$ $(\eta(k_1, k_2) \geq \eta\ (k_1))$, $k_1, k_2 \in \delta$ [7]. A fuzzy 2-side ideal in δ if it satisfies both fuzzy (left & right) ideal [7]. A fuzzy generalized bi-ideal in δ is η [7]. A fuzzy bi-ideal is a fuzzy LA-semi-group η that $((k_1, k_2)k_3) \geq \eta\ (k_1) \wedge \eta\ (k_3)$, k, k_2, $k_3 \in \delta$ [15]. A fuzzy interior-ideal is η satisfies $\eta\ ((k_1, k_2)k_3) \geq \eta\ (k_2)$ whenever k, k_2, k_3 are elements of δ [7]. The characteristic function of δ, denoted by $\eta_F\ (q_1)$, equals 1 whenever belongs to δ. For two fuzzy subsets of η of δ, $\eta \subseteq \delta$, means that $\eta\ (k_1) \leq \eta_F\ (k_1)$, for any k_1 in δ [7]. A fuzzy subset η of δ is considered a fuzzy quasi-ideal of δ if $(f \circ \eta_F\ (k_1)) \cap (\eta_F\ (k_1) \circ \eta$ [7]. A fuzzy subsemigroup η of δ is termed a fuzzy (1,2) ideal of δ if $\eta\ ((p_1 r)\ (p_2, p_3)) \geq \eta\ (p_1) \wedge \eta\ (p_2) \wedge \eta\ (p_3)$, whenever p_1, p_2, p_3 and $r \in \delta$, [16]. If η and φ are any two fuzzy subsets of δ, their product $\eta \circ \varphi$ is defined by $(\eta \circ \varphi)_{k_1}) =$ max $\eta(k_2)$,$\varphi(k_3) = \eta(k_2) \vee \varphi(k_3)$ or min $\eta(k_2)$,$\varphi(k_3) = \eta\ (k_2) \wedge \varphi(k_3)$ whenever $k_1, k_2, k_3 \in \delta$ [17]. If LA-semi-group δ contains a left identity e, then $\delta = e\ \delta \subseteq \delta^2$, therefore $\delta = \delta^2$ [18].

1.1. Objective of this paper embarks on an in-depth exploration of unit regular LA-semigroups, with a spotlight on the traits and applications of fuzzy ideals within these algebraic constructs.

2 Related Works

Definition 1 [1] Let be a semi-group and be a nonempty subset of then. This is called the sub-semi group of if $F^2 \subseteq F$.

Definition 2 [1] A nonempty subset of a semigroup is called the left (right) ideal of δ if $\delta F \subseteq F$ ($F\delta \subseteq F$), It is denoted $\ell(\mathcal{R})$-ideal.

Definition 3 [1] An ideal in a semigroup δ is a non-empty subset F that functions as a 2-sided ideal by being both a ℓ and $\mathcal{R}$- ideal of δ.

Definition 4 [1] A sub-semigroup is called the bi-ideal of if $F\delta F \subseteq F$, It is denoted ($\mathcal{B}$-ideal).

Definition 5 [10] If there is a unit element u in a semi-group δ such that $q_1 = q_1 u q_1$, $\forall q_1$ in δ then the semi-group is called the **unit regular**, it is denoted (U- reg.).

Definition 6 [1] An interior ideal of a semigroup, denoted as an ε-ideal, is a non-empty subset where the elements of the semigroup are contained within the subset, (δF) $\delta \subseteq F$.

Definition 7 [1] A subset of a semigroup, not void, is termed the quasi-ideal of δ if $\delta F \cap F\delta \subseteq F$.

Definition 8 [1] A non-empty subset within a sub-semigroup of earns the title of (1,2) ideal of δ if… $(F\delta)F^2 \subseteq F$.

Definition 9 [2] A semigroup is called the right (left) identity $eq_1 = q_1(q_1 e = q_1)$, whenever $q_1 \in \delta$.

Definition 10 [3] Let δ be a semigroup; at that point δ is called the **LA-semi group** in the event that $(q_1q_2)q_3 = (q_3q_2)q_1$; whenever $q_1,q_2,q_3 \in \delta$.

The medial law of a LA-semi group is $(q_1q_2)(q_3q_4) = (q_1q_3)(q_2q_4)$; at whatever point q_1,q_2,q_3 and $q_4 \in \delta$.

In addition, on the off chance that δ contains a left identity.

the paramedical law is cruel: $(q_1q_2)(q_3q_4) = (q_4q_3)(q_2q_1$; at whatever point q_1,q_2,q_3 and $q_4 \in \delta$.

Should LA-semi-group possess a neutral element, the law of succession comes into play. $q_1(q_2q_3) = q_2\ (q_1q_3)$; at whatever point $q_1,q_2,q_3 \in \delta$.

Definition 11 [4] Consider an ordered semi-group (δ, ≤), where F is a subset of δ. The Characteristic Function η_F of F It can be described as follows:

$$\eta_F\colon \delta \to [0,1] \lfloor x \to \eta_F = \begin{cases} 1, \ if\ x \in F \\ 0, \ if\ x \notin F \end{cases}$$

This function is known as the fuzzy subset of δ. A subset F is referred to as a sub-semi-group of δ if the square of F, denoted as $F^2 \subseteq F$.

Definition 12 [11] It is stated that a semigroup δ is regular if, for any q_1 of δ, ∃ q_2 in δ such that $q_1 = q_1q_2q_1$.

Example 1 $(z_6,.)$ is a regular semi group, since $z_6 = \{0, 1, 2, 3, 4, 5\}$, where $1 = 1.1.1$, $2 = 2.5.2$, $3 = 3.3.3$, $4 = 4.4.4$, $5 = 5.5.5$.

Definition 13 [5] The fuzzy sub-semigroup of δ is defined as the fuzzy subset η in a semigroup δ such that, whenever $q_1, q_2 \in \delta$.

$$\eta(q_1q_2) \geq min\{\eta(q_1), \eta(q_2)\},$$

Definition 14 [1] The Fuzzy- ℓ ($\mathcal{R}$)- ideal of δ is defined as a fuzzy subset η of a semi group δ such that, whenever $q_1, q_2 \in \delta$.

$$\eta(q_1q_2) \geq \eta(q_2),\ (\eta(q_1q_2) \geq \eta(q_1)).$$

Definition 15 [6] η is referred to as the **Fuzzy 2-Sided Ideal** in δ.

if it is both fu- ℓ - id & fu- $\mathcal{R}$ - id in δ.

Definition 16 [5] A fu- ε-ideal in δ occurs when a fuzzy sub-semi group η exists within a semi group δ. If $\eta(q_1rq_2) \geq \eta(r)$, $q_1, r,q_2 \in \delta$**.**

Definition 17 [7] η in LA-semi group δ exists (1,2) When, q_2, q_3 and r ∈ δ, the ideal of δ is if $\eta((q_1\ r)\ (q_2q_3)) \geq \eta\ (q_1) \wedge \eta(q_2) \wedge \eta(q_3)$.

Definition 18 [7] A η in LA-semi -group δ is **Fuzzy Quasi-Ideal** for δ if $(\eta \circ F_\delta(r)) \cap (F_\delta(r) \circ \eta) \subseteq \eta$.

Remark 1 [12] In the case where F is a nonempty for semi-group δ & η_F is δ's characteristic function, F is a sub-semigroup of δ if and only if η_F is a fuzzy sub-semigroup of η Only when η_F is a fuzzy- $\ell(\mathcal{R})$-ideal. of δ is a $\ell(\mathcal{R})$-ideal.

of δ If η_F is a Fu. Id. For δ, so F is ideal for δ.

Lemma 1 [8] Each fuzzy -ℓ - ideal of a left identity LA-semigroup δ becomes a fuzzy -$\mathcal{R}$ - ideal of δ.

Lemma 2 [8] The following requirements apply to η in LA-semi-group δ, The fu-$\ell(\mathcal{R})$-id.

(i) of δ is represented by η if f $F_\delta(x) \circ \eta \subseteq \eta(\eta \circ F_\delta(x) \subseteq \eta)$.
(ii) η is a fuzzy LA-Sub-Semi group of δ if and only if $\eta \circ \eta \subseteq \eta$.

Lemma 3 [8] The following holds for each subset M and N that is not empty within a LA-semi group δ.

(i) $F_M \circ F_N = F_{MN}$
(i) $F_M \cap F_N = F_{M \cap N}$

Definition 19 [8] If a subset of a LA-semi group δ is non-empty, then.

(i) Provided that η_F is a Fu. LA-Sub-Semi-group in δ, then F is a LA-Sub-Semi-group of δ.
(ii) Provided and only provided that η_F is a Fuzzy- ℓ ($\mathcal{R}$,2-sided) ideal, then F is a ℓ ($\mathcal{R}$,2-sided) ideal of δ. δ's ideal.

Lemma 4 [2] Every Fuzzy- ℓ - ideal (fuzzy -$\mathcal{R}$ - ideal)is a fuzzy $\mathcal{B}$-ideal of δ.

Definition 20 [3] A fuzzy -ℓ - ideal η is **Idempotent** where $\eta \circ \eta = \eta$.

Definition 21 [9] Given any fuzzy subsets η and φ of a semigroup δ, the product $\eta \circ \varphi$ is defined as $(\eta \circ \varphi)_{(q_1)} = \begin{cases} \bigvee\limits_{q_1 = q_2 q_3} \{\eta(q_2) \wedge \varphi(q_3)\}; \textit{for some } q_1, q_2 \textit{and } q_3 \in \delta \\ 0; \quad \textit{otherwise}. \end{cases}$

Definition 22 [7] η is **Fuzzy-$\mathcal{B}$-ideal** if $\eta((p_1 r)p_2) \geq \eta(p_1) \wedge \eta(p_2)$ whenever p_1, r, $p_2 \in \delta$.

3 The Results

Theorem 1 If the fu -ε- ideal η exists in the ℓ - identity of the U- reg. LA-semi group δ, then $\eta(q_1 q_2) = \eta(q_2 q_1)$ whenever $q_1, q_2 \in \delta$.

Proof. Suppose that η is a fuzzy -ε- idealof a U- reg.LA-semi group δ with left identity, and let $q_1 \in \delta$, then $\exists u \in \delta$ s.t $q_1 = q_1 u q_1$,

$\eta(q_1) = \eta\ (q_1 \mathrm{u} q_1)$ … by Defined (10) (4)
$= \eta\ (u(q_1 q_1)e) = \eta\ ((u(q_1^2) \geq \eta\ (q_1^2)$ (since the ideal fuzzy -ε of η)
$\eta(q_1) \geq \eta(q_1^2)$… (1)
$\eta\ (q_1^2) = \eta\ (q_1 q_1) = \eta\ (q_1(q_1 \mathrm{u} q_1)) = \zeta(q_1^2 u^2 q_1) = \eta\ (q_1^2 \mathrm{u} q_1)\ \eta((q_1^2 \mathrm{u}) q_1 e) \geq \eta\ (q_1)$
$\eta(q_1) \leq \eta(q_1^2)$… (2)
Then from (1) and (2) we get $\eta\ (q_1) = \eta\ (q_1^2)$.
Now, $\eta\ (q_1 q_2) = \eta\ ((q_1 q_2)^2)$.
$= \eta\ ((q_1 q_2)(q_1 q_2))$.
$= \eta\ ((q_2 q_1)(q_2 q_1))$.
$= \eta\ (e(q_2 q_1)(q_2 q_1))$
$\geq \eta(q_2 q_1)$ (given that η is a fu -ε)
Hence $\eta\ (q_1 q_2) \geq \eta\ (q_2 q_1)$… (1)
now $\eta\ (q_2 q_1) = \eta\ (q_2 q_1 \mathrm{u} q_1) = \eta\ (q_2 (q_1) \mathrm{u} q_1)$
$= \eta\ (q_1 (q_2 u q_1))$
$= \eta\ (q_1 q_2 \mathrm{u} q_1)) = \eta\ (e(q_1 q_2)(u q_1)))$
$\geq \eta(q_2 q_1)$ (since the fu-ε-ideal of η)
Hence $\eta\ (q_2 q_1) \geq \eta\ (q_1 q_2)$… (2), then from (1) and (2) we get $\eta\ (q_1 q_2) = \eta\ (q_2 q_1)$.

Theorem 2 Given δ as a subset of δ and η as a fuzzy subset of the U- reg. LA-semi group δ, one can deduce $(\mathrm{F}_\delta \circ \eta) = \eta$.

Proof. Given that δ is a U- reg.LA-semi group, whenever $q_1 \in \delta$, $\exists\, u \in \delta$, s.t $q_1 = q_1 \mathrm{u}\ q_1$.

Now using Left Inverse law $q_1 = (q_1 \mathrm{u}) q_1$ then

$$(\mathrm{F}_\delta(u) \circ \eta)_{(q_1)} = \vee_{q_1 = (q_1 \mathrm{u}) q_1} \{\mathrm{F}_\delta(u)(q_1 \mathrm{u}) \wedge \eta(q_1)\}$$

$= \vee_{q_1 = (q_1 \mathrm{u}) q_1} \{1 \wedge \eta(q_1)\} = \eta(q_1)$.
Hence $\eta = \mathrm{F}_\delta(u) \circ \eta$.

Theorem 3 In a $\mho$- reg. LA-semi group δ, $(\eta \circ \mathrm{F}_\delta = \eta)$ and $(\mathrm{F}_\delta(u) \circ \eta = \eta)$ holds for any fuzzy 2-sided ideal (η) of δ.

Proof. Since δ is $\mho$- reg.LA-semi group, then, whenever $q_1 \in \delta$, $\exists u \in \delta$,s.t $q_1 = q_1 \mathrm{u} q_1$, $q_1 = q_1 \mathrm{u} q_1$ Definition (10) (4)
$= (\mathrm{u} q_1) q_1$.

Then $(\eta \circ \mathrm{F}_\delta)_{(q_1)} = \vee_{q_1 = (\mathrm{u} q_1) q_1} \{\eta(\mathrm{u} q_1) \wedge \mathrm{F}_\delta(u)(q_1)\}$

$$\geq \eta(q_1) \wedge \mathrm{F}_\delta(u)(q_1)$$

$\geq \eta(q_1) \wedge 1$.
$= \eta\ (q_1)$.then $\eta = (\eta \circ \mathrm{F}_\delta)$, and from Theorem (5) we get $\eta = \mathrm{F}_\delta(u) \circ \eta$, for every Fuzzy 2-Sided ideal.

Corollary 1 In a U- reg.LA-semi group δ, $(\mathrm{F}_\delta(u) \circ \mathrm{F}_\delta(u) = \mathrm{F}_\delta(u))$.

Theorem 4 For η Fuzzy -ℓ - Ideal in U- reg.LA-semi group δ, it must also be the Fu -$\mathcal{R}$ - Id. in δ.

Proof. $\Rightarrow$ suppose η has L- identity and is a Fuzzy -ℓ - ideal of U- reg. LA-semi group δ., and let $q_1, q_2 \in \delta$, for some u, $s \in \delta$, s.t $q_1 = q_1 u q_1$ and $q_2 = q_2 s q_2$,

Now $\eta(q_1 q_2) \geq \eta(q_1)$.

This demonstrates that η qualifies as a fuzzy - $\mathcal{R}$ - Ideal of δ.

$\Longleftarrow$ Assuming that η represents a fuzzy - $\mathcal{R}$ - ideal within the U- reg.LA-semigroup δ featuring a left Identity, and considering $q_1, q_2 \in \delta$ such that $q_1 = q_1 u q_1$ for some u, s $\in \delta$ and $q_2 = q_2 s q_2$,

Now $\eta\ (q_1 q_2) \geq \eta(q_2)$.

This confirms that η is Fu - ℓ - Id. in δ.

Theorem 5 If η stands as a fuzzy (1,2) Ideal of δ within the fuzzy subset η of the U-reg.LA-semigroup δ equipped with a left identity, then it also holds the status of being a fuzzy 2-Sided Ideal of δ.

Proof. $\Longrightarrow$Since η is the fuzzy (1,2) ideal of δ of the ℧- reg.LA-semi group δ with left identity, and if $q_1 \in \delta$, thus $\exists\ u \in \delta$, such that $q_1 = q_1 u q_1 = q_1 u q_1$.

Now $\eta\ (s\ q_1) = \eta\ (s\ (q_1 u q_{1)})$

$= \eta\ (s\ (q_1(u)(q_1\big[(u)q_1\big])))$

$= \eta\ (s\ (q_1(u)(u)q_1 q_1))$

$= \eta\ (s\ (\big[q_1(u)(u)\big]q_1 q_1))$

$= \eta\ (q_1[s(u)(u)])(q_1 q_1))$

$\geq \eta(q_1) \wedge \eta\ (q_1) \wedge \eta\ (q_1)$

$= \eta\ (q_1)$

As a result, η is a fuzzy - ℓ - ideal of δ, and according to theorem (4), η is also a $\mathcal{R}$ - ideal of δ. Ideal of δ with Two Sides.

$\Longleftarrow$ if η is fuzzy Using the left identity and letting q_1, q_2, q_3, and r $\in \delta$, we obtain the 2-sided ideal of δ of U- reg.LA-semi group δ. Then, $\exists$ u $\in \delta$, $q_1 = q_1 u q_1$.

Subsequently, $\eta\ ((q_1 r)(q_2 q_3)) \geq \eta(q_1) \wedge \eta\ (q_2) \wedge \eta\ (q_3)$.

illustrates that η qualifies as a fuzzy (1, 2) Ideal of δ.

Theorem 6 η is fu (1,2) Id in δ of the U- reg.LA-semi-group δ with a Left Identity, then it is also a Fuzzy Quasi-Ideal of δ.

Proof. $\Longrightarrow$ directlyby Theorems (5) and (3).

$\Longleftarrow$ if η is fuzzy Qu-Id for U-reg.LA-semi group δ with a left identity. If $q_1 \in \delta$ then there exists u $\in \delta$ such that $q_1 = q_1 u q_1$, based on the definition of a fuzzy Quasi-Ideal.

Now, $q_1 = q_1 u q_1 = (q_1 u)(q_1 e)$…by Definition (10) (3)

$= (e q_1)(u q_1) = (e[(q_1)(u q_1)]\ldots$ by Defined (10) (4)

$= (q_1[(e)(u q_1)])$.

Therefore

$(\eta \circ F_\delta)_{(q_1)} = \vee_{q_1 = (q_1[(e)(u q_1)])}\{\eta(q_1) \wedge F_\delta(e(u q_1))\}$

$\geq \eta(q_1) \wedge F_\delta(e(u q_1))$

$\geq \eta(q_1) \wedge 1$(by theorem (2))

$= \eta\ (q_1)$,

Now, by using Theorem (3.2 we get $(F_\delta \circ \eta) = \eta$ and Corollary (1) we get $(F_\delta(u) \circ F_\delta(u) = F_\delta(u))$. Therefore

$(\eta \circ F_\delta(u)) = (F_\delta(u) \circ \eta) \circ (F_\delta(u) \circ F_\delta(u))\ldots$ Definition(10) (2)
$= (F_\delta(u) \circ F_\delta(u)(\eta \circ F_\delta(u))$
$= F_\delta(u) \circ (\eta \circ F_\delta) \supseteq (F_\delta(u) \circ \eta)$.
which shows that $(F_\delta(u) \circ \eta) \subseteq (\eta \circ F_\delta(u)) \cap (F_\delta(u) \circ \eta)$.

As η is a fuzzy Quasi-Ideal of δ, $(F_\delta(u) \circ \eta) \subseteq \eta$. By theorem (4), η is Fu. 2-side Id. From theorem (5), it Fu. (1, 2) Id. in δ.

Theorem 7 If η is fu.-$\mathcal{B}$ -id. of δ, then it is equivalent to being a fuzzy (1, 2) ideal of δ., where δ is a LA-semi-group that hold left-identity and is U-regular.

Proof. $\Longrightarrow$ Using Left -Identity, let η be a fuzzy $\mathcal{B}$ -ideal of U- reg.LA-semi group δ, and let $q_1, r, q_2, q_3 \in \delta$, then $\exists\ u \in \delta$ s.t $q_1 = q_1 u q_1 = q_1 u q_1$,
$\eta((q_1 r)(q_2 q_3))$ …by Definition (2.10) (3)
$= \eta\ ((q_3 q_2)(r q_1))$ …by Definition (10) (1) $= \eta(((r q_1) q_2) q_3))$.
$= \eta(((r q_1) q_2) e q_3))$
$\geq \eta\ (((r q_1) q_2)) \wedge \eta\ (q_3)$ (because η is a Fuzzy $\mathcal{B}$-ideal)
$= \eta\ (((r q_1) e q_2)) \wedge \eta\ (q_3)$
$\geq \eta\ (r q_1) \wedge \eta\ (q_2) \wedge \eta\ (q_3)$ (because η is a Fuzzy $\mathcal{B}$-ideal)
$= \eta\ ((r\big[(q_1)(u q_1)\big]) \wedge \eta\ (q_2) \wedge \eta\ (q_3)$…by Definition (10) (4)
$= \eta\ (((q_1)\big[r(u q_1)\big]) \wedge \eta\ (q_2) \wedge \eta\ (q_3)$
$= \eta((q_1)[r u] q_1) \wedge \eta(q_2) \wedge \eta(q_3)$
$\geq \eta(q_1) \wedge \eta(q_1) \wedge \eta(q_2) \wedge \eta(q_3)$
$= \eta(q_1) \wedge \eta(q_2) \wedge \eta(q_3)$ (because η is a Fuzzy $\mathcal{B}$-ideal),
which shows that η is a Fuzzy (1, 2) Ideal of δ.

$\Leftarrow$ Let η be a fuzzy (1,2) Ideal of U- reg.LA-semi group δ with Left Identity then whenever r, q_1 and $q_2 \in \delta$, then $\exists\ s \in \delta$ s.t $q_2 = q_2 s q_2 = q_2 s q_2$,.
$\eta\ ((q_1 r) q_2) = \eta\ ((q_1 r)[q_2(s q_2)])$ …by Definition (10) (4)
$= \eta\ ((q_1 r)[s(q_2 q_2)])$
$= \eta\ ([(q_1 r)(s)](q_2 q_2))$ …by Definition (10) (2)
$= \eta\big(\big[(q_1 r)(s)\big](q_2 q_2)\big)$
$= \eta\big((q_1[(rs))\big](q_2 q_2)\big)$
$\geq \eta(q_1) \wedge \eta(q_2) \wedge \eta(q_2)$(because η is a fuzzy (1, 2) Ideal)
$= \eta\ (q_1) \wedge \eta\ (q_2)$,
It shows that the fuzzy $\mathcal{B}$-ideal of δ is η.

Theorem 8 A fuzzy (1,2) ideal of δ is η iff it exists in a U- reg. LA-semi group δ with left identity.

Proof. assume η is fu-$\mathcal{B}$ -id in δ, so it is the same as being a fuzzy (1, 2) ideal of the U-reg.LA-semi group δ., such as Left Identity, and let $q_1, a, q_2 \in \delta$, then $\exists\ u \in \delta$ s.t $a = aua = aua$,

$(q_1 a) q_2 = [(q_1(aua)\big] q_2$ …by Definition (10) (1)
$= [q_2(aua)] q_1 = [q_2(a(ua))] q_1 \ldots$ by Definition (10) (4)
$= (a(q_2 ua))] q_1 = [(a(q_2 ua)) q_1]$ …by Definition(10) (1)
$= [(q_1(q_2 ua))a]$
$= [(q_1(q_2 ua))(aua))]$ … by Definition (10) (4)
$= a(q_1(q_2 ua))(ua)$.

$= a[\ (q_1q_2\mathrm{u}a)(\mathrm{u}a)]$…by Definition (10) (2)
$= a[\ (q_1q_2\mathrm{uu})(aa)]$.
Therefore $\eta\ ((q_1a)q_2) = \eta\ (a[\ (q_1q_2\mathrm{uu})(aa)])$
$= \eta\ (ah(aa))$ where $h = (q_1q_2\mathrm{uu})$
$\geq \eta(a)\wedge\eta\ (a)\wedge\eta\ (a)$
$= \eta\ (a)$.
so η is Fu- ε-ideal of δ.
⇐ Let η be a Fuzzy- ε-ideal of U- reg.LA-semi group δ, with Left Identity and let $q_1, a, q_2, q_3 \in \delta$, then $\exists\ u \in \delta$ s.t $q_3 = q_3\mathrm{u}q_3 = q_3\mathrm{u}q_3$,
$\eta\ ([(q_1a)(q_2q_3)])$ … by Definition (10) (3)
$= \eta\ ((q_3q_2)(aq_1)\geq \eta\ (q_2)$ (because η is a fuzzy -ε- ideal).
Now, $\eta\ ([(q_1a)(q_2q_3)]) = \eta\ [(q_1((a)(q_2q_3))]$ … by Definition (10) (4).
$= \eta\ (a(q_1q_2q_3) = \eta\ (a((q_1)q_2q_3)$.
$\geq \eta(q_1)$ (because η is a fuzzy -ε- ideal).
and,
$\eta[(q_1a)((q_2)(q_3))] = \eta\ [(q_1a)((q_2)(q_3\mathrm{u}q_3))]$…by Definition (10) (3).
$= \eta\ [(q_3\mathrm{u}q_3q_2)(aq_1)]$ …by Definition (10) (1).
$= \eta\ ((aq_1q_2)q_3\mathrm{u}q_3)$.
$= \eta\ ((aq_1q_2)q_3(\mathrm{u}q_3)$.
$\geq \eta(q_3)$ (because η is a fuzzy -ε- ideal).
Therefore,
$\eta((q_1a)(q_2q_3)) \geq \eta(q_1)\wedge\eta\ (q_2)\wedge\eta\ (q_3)$.
Thus η is a Fuzzy (1, 2) Ideal.

Corollary 2 There is a U-reg- LA-semigroup δ with a left identity that coincides with fuzzy 2-sided ideals, fuzzy-$\mathcal{B}$ -ideals, fuzzy (1, 2) ideals, fuzzy-ε-ideals, and fuzzy quasi-ideals.

Theorem 9 Assume δ is a left-identity U- reg. LA-semigroup. If and only if η is equal to the intersection of $(\eta \circ \mathrm{F}_\delta)$ and $(\mathrm{F}_\delta \circ \eta)$ equals η. Then η is regarded as a fuzzy quasi-ideal of δ.

Proof. ⇒ follows by Theorem (3) and Theorem (6)**.**
⇐ obvious.

Theorem 10 This is a fu $\mathcal{B}$ -id for δ in the U- reg.LA-semi-group δ, employing left identity, iff $(\eta \circ \mathrm{F}_\delta(u))\circ\eta) = \eta$ and $\eta \circ \eta = \eta$.

Proof. ⇒ Suppose that η is fu $\mathcal{B}$-ideal in U- reg.LA-semi group δ, with left Identity and let $q_1 \in \delta$, then $\exists u \in \delta$ s.t $q_1 = q_1\mathrm{u}q_1$.
$q_1 = q_1\mathrm{u}q_1 = (q_1\mathrm{u})[(q_1(u)]q_1\ldots$ by Definition (10) (4)
$= (q_1\mathrm{u})[(q_1u)]q_1 = q_1uu(q_1u)q_1 = (q_1uuq_1u)q_1$.

Therefore,
$((\eta \circ \mathrm{F}_\delta(u)) \circ \eta)_{(q_1)}$
$=\vee_{q_1=(q_1uuq_1u)q_1}\{(\eta \circ \mathrm{F}_\delta(u))(q_1uuq_1u) \wedge \eta(q_1)\}$.
$\geq \vee_{(q_1uuq_1u)q_1=(q_1uuq_1u)q_1}\{(\eta(q_1uuq_1) \wedge \mathrm{F}_\delta(u)(u)))\} \wedge \eta(q_1)\}$
$\geq \eta(q_1(uu)q_1)\wedge 1 \wedge\eta(q_1)$
$\geq\eta(q_1) \wedge \eta(q_1)\wedge 1 \wedge \eta(q_1)$(because η is a fuzzy $\mathcal{B}$-ideal)

$= \eta(q_1)$

Now, $q_1 = q_1 \mathrm{u} q_1 = (q_1(\mathrm{u}q_1\mathrm{u}))q_1$.

Therefore,

$((\eta \circ \mathrm{F}_\delta(u)) \circ \eta)_{(q_1)} = \vee_{q_1=(q_1(uq_1u))q_1}\{(\eta \circ \mathrm{F}_\delta(u))(q_1(uq_1u) \wedge \eta(q_1)\}$.

$= \vee_{q_1=(q_1(uq_1u))q_1}\{(\eta(q_1) \wedge \mathrm{F}_\delta(u)(uq_1u)))\} \wedge \eta(q_1)\}$

$= \vee_{(q_1(uq_1u)q_1}\{\vee_{q_1(uq_1u)}\{(\eta(q_1) \wedge \mathrm{F}_\delta(u)(uq_1u)))\} \wedge \eta(q_1))).$

$= \vee_{(q_1(uq_1u))q_1}\{\vee_{q_1(uq_1u)}\{(\eta(q_1) \wedge 1))\} \wedge \eta(q_1))).$

$= \vee_{(q_1(uq_1u))q_1}\{\vee_{q_1(uq_1u)}\{\eta(q_1))\} \wedge \eta(q_1))).$

$= \vee_{(q_1(uq_1u))q_1}\{\eta(q_1) \wedge \eta(q_1)\}.$

$= \eta(q_1).$

Thus $(\eta \circ \mathrm{F}_\delta(u)) \circ \eta = \eta$.

$q_1 = q_1 \mathrm{u} q_1 = \big[(q_1\mathrm{u})(q_1\mathrm{u})\big]q_1 \ldots$ by Definition (10) (3)

$= \big[(q_1q_1)(\mathrm{uu})\big]q_1 \ldots$ by Definition (10) (1)

$= \big[((\mathrm{uu})q_1)q_1\big]q_1.$

$= \big[\big(((\mathrm{uu})q_1\mathrm{u}q_1\big]\big)q_1\big)q_1.$

$= \big[\big(((\mathrm{uu})\{(q_1)\mathrm{u}q_1\}\big]\big)q_1\big)q_1 \ldots$ by Definition (10) (4)

$= q_1\big[(\mathrm{uu})(\mathrm{u}q_1)\big]q_1)q_1.$

Therefore $(\eta \circ \eta)_{(q_1)}$.

$\Leftarrow$ let η be a fuzzy subset of U- reg.LA-semi group δ, with left identity, and let q_1, a, $q_3 \in \delta$.$\eta((q_1a)q_2) = ((\eta \circ \mathrm{F}_\delta(a)) \circ \eta)(q_1a)q_2$.

$= \vee_{(q_1a)q_2=(q_1a)q_2}\{(\eta \circ \mathrm{F}_\delta(a)(q_1a)) \wedge \eta(q_2)\}$

$$\geq \vee_{(q_1a)q_2=(q_1a)q_2}\{(\eta \circ \mathrm{F}_\delta(a)(q_1a)) \wedge \eta(q_2)\}$$

$\geq \vee_{(q_1a)q_2=(q_1a)q_2}\{(\eta(q_1) \circ \mathrm{F}_\delta(a)(a)) \wedge \eta(q_2)\}$

$\geq \eta(q_1) \wedge 1 \wedge \eta(q_1)$

$\geq \eta(q_1) \wedge \eta(q_1).$

Since $\eta \circ \eta = \eta$, therefore by theorem (3.3), η denotes A fuzzy LA-sub semigroup of δ implies that η serves as the fuzzy-$\mathcal{B}$ -ideal of δ.

Theorem 11 If and only if $(\mathrm{F}_\delta(u) \circ \eta) \circ \mathrm{F}_\delta(u) = \eta$, then for any U- reg.LA-semi group δ with left identity, η is a fuzzy -ε- ideal of δ.

Proof. $\Longrightarrow$ Given η as a fuzzy -ε- ideal of U- reg.LA-semi group δ with left identity, and letting $q_1 \in \delta$, we find that $\exists u \in \delta$ s.t $q_1 = q_1 \mathrm{u} q_1$,

$q_1 = q_1 \mathrm{u} q_1 = \big[q_1(u)\big]q_1 \ldots$ by Definition (2.10) (3).

$= [(u)q_1]q_1 = (u)[q_1uq_1]q_1 \ldots$ by Definition (10) (2).

$= (u)[(q_1q_1(\mathrm{u}))]q_1 = (u)[((q_1q_1\mathrm{u})q_1] \ldots$ by Definition (10) (1).

$= (u)[(q_1\mathrm{u})q_1q_1] = (u)((q_1\mathrm{u})q_1q_1).$

Therefore

$\eta((q_1uq_2) = (\mathrm{F}_\delta(u) \circ \eta) \circ (\mathrm{F}_\delta(u))((u(q_2u)q_1^2)u)$

$= \vee_{(u)((q_1\mathrm{u})q_1q_1)=u(q_2u)q_1^2)}\big\{(\mathrm{F}_\delta(u) \circ \eta\big((q_2u)q_1^2\big) \wedge \mathrm{F}_\delta(u)(u)\big\}$

$$\geq \vee_{(u)((q_1\mathrm{u})q_1q_1)=u(q_2u)q_1^2)}\Big\{1 \wedge \eta\Big((q_2u)q_1^2\Big) \wedge 1\Big\}$$

$\geq \vee_{(u)((q_1\mathrm{u})q_1q_1)=u(q_2u)q_1^2)}\big\{\eta\big((q_2u)q_1^2\big)\big\}$

$\geq \eta(u)$.

A fuzzy -ε- ideal, therefore, is η. These are the results that follow directly from Corollary (2) and Theorem (10).

Corollary 3 η qualifies as a fuzzy (1, 2) ideal of δ iff $(\eta \circ F_\delta) \circ (\eta \circ \eta) = \eta$ and $\eta \circ \eta = \eta$.

Theorem 12 every fuzzy $\mathcal{R}$-ideal of δ exhibits idempotent properties.

Proof. $\Rightarrow$ Suppose that δ is U- reg.LA-semigroup having a left identity that allows for $q_1 \in \delta$, then $\exists u \in \delta$ s.t $q_1 = q_1 u q_1 = q_1 u q_1$.

Let's assume that η is a fuzzy - $\mathcal{R}$ - ideal of δ. It is evident that (η∘ η) is a subset of η in order to demonstrate that (η ∘η) is a superset of η.

$(\eta \circ \eta)_{(q_1)} = \vee_{q_1=(q_1u)q_1}\{\eta(q_1u) \circ \eta(q_1)\}$

$$\geq \vee_{(q_1u)q_1=(q_1u)q_1}\{\eta(q_1u) \wedge \eta(q_1)\}$$

$\geq \vee_{(q_1u)q_1=(q_1u)q_1}\{\eta(q_1) \wedge \eta(q_1)\}$

$\geq \eta(q_1) \wedge \eta(q_1)$

$= \eta(q_1)$. Hence η is a fuzzy -ε- ideal hence $(\eta \circ \eta) \supseteq \eta$, thus $(\eta \circ \eta) = \eta$. Therefore η is an idempotent.

$\Longleftarrow$ All fuzzy - $\mathcal{R}$ - Ideals of δ with left identity are assumed to be idempotent. Because aδ is a $\mathcal{R}$ - ideal of δ, a fuzzy - $\mathcal{R}$ - ideal of δ is also its characteristic function, $F_{a\delta}$. Additionally, $F_{a\delta}$ (a) = 1 since a ∈ aδ. Using lemma (3) and the given assumption, we now have $F_{a\delta} \circ F_{a\delta} = F_{a\delta}$ and $F_{a\delta} \circ F_{a\delta} = F_{(a\delta)^2}$, so we have $\left(F_{(a\delta)^2}\right)(a) = (F_{a\delta}) = 1$, implying that a ∈ $(a\delta)^2$ and that ∈ $(a\delta)^2 = (a\delta)(a\delta) = (aa)(a\delta) = (aa)\delta^2 = (aa)\left(\delta^2 e\right)$.

4 Conclusion

Within the theory of LA-semi groups, the study concentrates on fuzzy -ℓ ($\mathcal{R}$)ideal and fuzzy Quasi-Ideal in U- reg. Semi groups. Additionally, the study explores and evaluates the characteristics and connections between the fuzzy (1,2), fuzzy-ε, fuzzy-ideal, and fuzzy-$\mathcal{B}$-ideal. A theoretical study and mathematical arguments are used to demonstrate the connections between these different types of fuzzy ideals and their implications for the algebraic structure of U- reg.LA-semi groups.

References

1. Khan, M., Asif, T., Faisal, J.: Intra-regular left almost semigroups characterized by their anti-fuzzy ideals. Journal of Mathematics Research **2**(4), 100–110 (2010)
2. Mohamed, S.A., Asaad, H.S., Ahmad, S.I.: New properties of strongly regular left almost semi-groups. J. Discrete Math. Sci. Cryptogr. **25**(2), 615–622 (2022)
3. Mohamed, S.A.: Some Studies on Injectivity, Flatness Rings, and Fuzzy Ideals of Semigroups. Ph.D. Thesis. University of Mosul, Mosul, Iraq (2013)
4. Muhammad, S., Asghar, K.: Characterizations of ordered semigroups by the properties of their fuzzy ideals. Comput. Math. Appl. **59**, 539–549 (2010)

5. Hong, S.M., Jun, Y.B., Meng, J.: IN Fuzzy Interior Ideals in Semigroups Indian. J. Pure Appl. Math **26**(9), 859–863 (1995)
6. Kehayopulu, N., Tsingelis, M.: Fuzzy sets in ordered groupoids, semigroups. In Forum. Sci. **65**, 128–132 (2002)
7. Mordeson, J.N., Malik, D.S., Kuroki, N.: Fuzzy semigroups. Springer-Verlag, Berlin, Germany (2003)
8. Khan, M., Khan, M.N.: On fuzzy Abel-Grassmann's groupoids. Advances in Fuzzy Mathematics, pp. 349–360 (2010)
9. Shabir, M., Nawaz, Y.: Semi groups characterized by the properties of their anti-fuzzy ideals. J. Adv. Res. Pure Math. **1**(3), 42–59 (2009)
10. McFadden, R.B.: Unit-regular orthodox semigroups. Glasg. Math. J. **25**(2), 229–240 (1984)
11. Von, N.J., Princeton, N.J.: On Regular Rings. Proc. Natl. Acad. Sci. U.S.A. **22**(12), 707–713 (1936)
12. Rosenfeld, A.: Fuzzy Groups. J. Math. Anal. Appl. **35**, 512–517 (1971)
13. Nobusawa, N.: Osaka Journal of Mathematics (1964). https://doi.org/10.18910/12354
14. Samah, H.A., Akram, S.M.: New properties of γ – Regular LA-semi groups and related Concept. The National University of Science and Technology International Conference for Pure and Applied Sciences, 13 (2023)
15. Madad, K., Ahmad, N.: Journal of Advanced Research in Pure Mathematics **2**, 61–73 (2010)
16. Asaad, S., Ahmed, I.S., Mohammed, A.S.: Generalization Fuzzy Completely Intra G-ideals in G-Semi Groups. Journal of Physics: Conference Series, 1664 (2020)
17. Asaad, S.: On Study of Fuzzy Ideals of Semigroups. Thesis, Tikrit University, Msc (2019)
18. Madad, K., Young, B., Farisal, Y.: Hacettepe Journal of Mathematics and Statistics **44**(3), 569–586 (2015)

Enhancing Digital Music Libraries: A Clustering-Based Music Recommendation System

Aditya Prashant Ardak[1(✉)], Shamneesh Sharma[1], Isha Batra[2], Rajeev Sobti[2], and Manzoor Hussain[3]

[1] Delivery and Student Success, upGrad Education Private Limited, Bangalore, India
ardakaditya@gmail.com
[2] School of Computer Science and Engineering, Lovely Professional University, Punjab, India
[3] Indus University, Karachi, Pakistan
manzoor.hussain@indus.edu.pk

Abstract. The growth of digital music libraries shows the importance of having the best music to help users find customized content. This paper presents an integrated approach to music recommendation, as users receive content based on recommendations of songs that other users have already searched for and the content of song recommendations relevant to user's taste. This article tried to use K-Means clustering technology to find similar users by content, used PLSA technology to separate active or most listened to songs by content. To accomplish this task, a set of many documents was collected, assuming that they could be used empirically. To evaluate the usefulness of recommendations generated using the music recommendation method, three parameters, including accuracy, F-1 score, and recall, were calculated. Results of the provided method showed good results by evaluating the parameters of the collected data (e.g., precision, recall, and F1 score). The evaluation can be done from the perspective of users' real data, which will take some time due to the availability of data.

Keywords: Filtering · Recommendations · Music · K-Means · PLSA

1 Introduction

Nowadays, music is an important part people daily life. Music became an inseparable part for people to participate in. Music recommendation systems have become popular research projects. Poor budgeting and tech led to the fast development of music. Today's music giant ensures finding the best music for its customers, so it is important to choose the right music for each customer. In addition, thanks to music recommendations, songs can be easily filtered and found according to the user's taste.

A music Recommendation System; It is discussed under three headings: user model, product analysis and comparison algorithm. Six consensus models are discussed in this study. This article briefly reviews two commonly used methods: content-based techniques and collaborative filtering. The collaboration appears to have been successful. In

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 269–277, 2025.
https://doi.org/10.1007/978-3-031-91008-1_25

this study, motivation-based model, human behavior, music psychology, etc. based on research [1].

In addition, in this article, the thinking-based model, one of the user solutions, is discussed and examined.

A new technique has been introduced, which is recommended to suit users from music collection. Primary purpose of the offer is finding the music that the users listen to the most, that is new to the listener's ear, and that suits his/her ears. This article uses an application to calculate real-world solutions. User reports from volunteers attempt to demonstrate the effectiveness of the plan [2].

A method for detecting social signals from WAV files is discussed. Using optimization techniques, the characteristics of the voice can be matched with social tags collected by the network. Automatic tags are mostly automatic tags that provide information about the music. This will help prevent cold start problems. This common cold start issue occurs during the validation process. Automatic labeling can simplify label positioning and help provide consistency and expression by providing a uniform set of labels for all lines in the body [3].

A Context-based Music Recommendation (COMUS) ontology was introduced. This application is used to model the user's favorite music selections. This approach provides a hierarchical approach that lists specific ontologies such as music, characters, and events, as well as a top-level music space that restricts concepts related to music quality such as title, artist, and genre. The proposed method can use the logical method by analyzing the reliability of the data frame. This ontology system helps define the relationship between music and content, allowing users to search for music suitable for use [4].

This article discusses music recommendations based on user preference analysis. In this study, a new model for the recommendation process was introduced using the hidden Markov model. Each song is modeled with a hidden Markov model, and this model is relied upon to define the measure of similarity between songs. Using similar metrics, the song users have listened to previously are brought together. The environment is controlled by a pseudo user having many options and arrays of system-generated commands [5].

This article proposes a hybrid as the most effective model. This ecosystem passes problems of accuracy of instructions and diversity of the artist's suggestions. The CF method is a method that can only use e-commerce sites, cannot accept work without criticism, and has a very narrow range of artist. The content-based method may not give the correct result due to the expectation of intuitiveness, which means that the user's favorite tracks have the same melodic content. To achieve higher accuracy and precision, the design has the ability to integrate information based on the context used. The results showed that the proposed system provided high-quality customers but added new customers [6]. Machine learning techniques have been applied to various fields such as sentiment analysis [23], e-learning recommendations [24], energy-saving in smartphones [25], and digital governance in smart cities [26].

2 Datasets

2.1 Spotify Dataset

The data is collected with the help of Python library "Spotify" that allows users to access files provided by the API. The archive contains approximately 1 million tracks across 19 features between 2000 and 2023.

This clean data has been prepared and utilized for research purposes. Its significance lies in its potential to unravel patterns and predict song popularity prior to its release. This dataset could be used to create various predictive models with machine-learning/deep-learning techniques.

2.2 Audio Features

The audio properties of the dataset include: Popularity, Vintage, Danceability, Energy, Theme, Loudness, Mood, Speech, Acousticity, Instrumentality, Liveliness, Value, Tempo, Time signature, and Duration_ms.

3 Proposed Methodology

Previous studies have proposed the hybrid K-Means PLSA method for aesthetic visualization. In this way, users will receive recommendations based on song recommendations content listened to by similar groups of users, as well as song recommendations searched by other users similar to existing users [7].

Here in this article, we will try to use K-Means clustering method to find similar users according to content, and the model uses PLSA method to find frequent songs among these users or often listen to content. Show the songs listened to by the user proportionally and then recommend the songs listened to most by other users to the current user [8] (Fig. 1).

A map of the system is provided, the proposed operation is evaluated, and any proposed music is used to implement the network architecture. The language used to use web scripts is PHP (Fig. 2).

Three metrics such as precision, recall, and F-1 score are used to validate the correctness of recommendations generated by music recommendation systems. The F-1 score differs from other scores because it is a measure of test accuracy and takes into account the accuracy of the test and returns it to calculate the final score. Accuracy: The accuracy of the contract refers to the ratio of the agreed content to the total content agreed upon.

$$Precision = \frac{Correctly\ Suggested\ Songs}{Total\ Suggested\ Songs}$$

Below is the ratio of truly suggested songs to total appropriate songs.

$$Recall = \frac{Correctly\ Suggested\ Songs}{Relavant\ Songs}$$

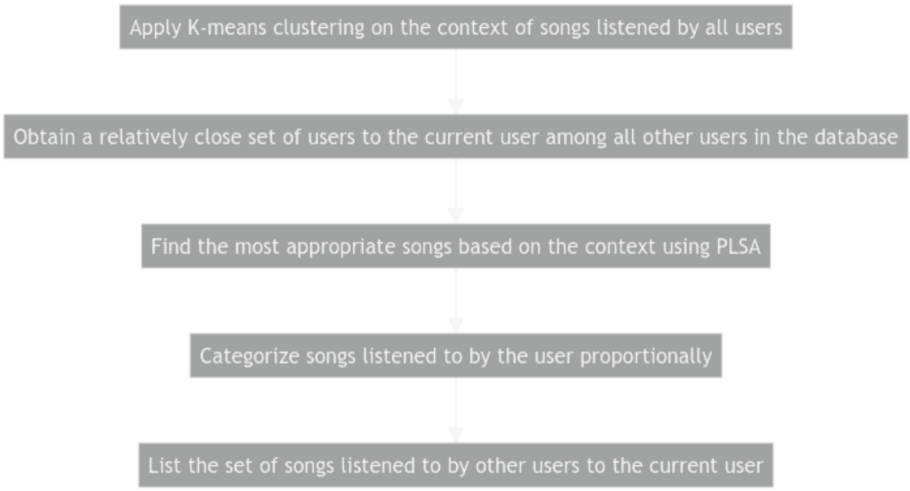


Fig. 1. Application Flowchart

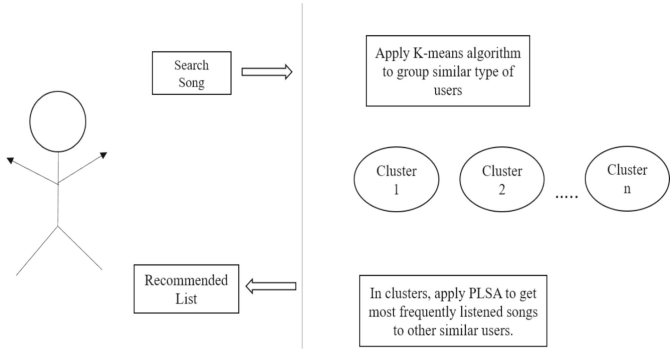


Fig. 2. Abstract System Design

F1-Score tries to integrate recall and precision resulting value by calculating different varieties of averages of metrices. It is seen average of above metrices

$$F_1 = \frac{2 * Precision * Recall}{Precision + Recall}$$

4 Result

It is evident that the key detection task appears relatively straightforward compared to the other tasks. The achieved accuracies are notably higher, with even the simplest technique performing quite well. Several factors contribute to this:

1. The property being determined in the key detection task is inherently "low-level," closely tied to chroma features and their temporal evolution. In contrast, relating genres or artists to these features proves more challenging.

2. For developing the key discovery dataset, we particularly chosen tracks with tall key certainty. This recommends that the calculation utilized to comment on key data within the Spotify tune Dataset seem perceive the key of these data generally effectively, likely contributing to the victory of our models. Shockingly, without manual labeling, it is challenging to confirm this statement (Tables 1 and 2).

Table 1. Experimental Values Proposed

Users	Precision	Recall	F1-Score
4	1	0.47	0.65
12	0.87	0.47	0.62
23	1	0.53	0.7
41	0.69	0.41	0.52
49	0.89	0.53	0.67
70	0.77	0.41	0.54
81	0.77	0.41	0.54

Table 2. Experimental Values of base paper

Users	Precision	Recall	F1-Score
4.00	0.73	0.35	0.50
12.00	0.67	0.23	0.39
23.00	1.00	0.53	0.70
41.00	0.49	0.53	0.38
49.00	0.58	0.34	0.45
70.00	0.45	0.24	0.30
81.00	0.67	0.30	0.40

In contrast, for the other tasks, the K-means exhibits a clear advantage over alternative approaches, resulting in significantly improved classification accuracies.

Although the benefits of pretraining are more modest, it proves advantageous for the artist recognition task, a challenging availability of labeled training data per class, particularly compared to other tasks. It is well-documented that gains from unsupervised pretraining are most pronounced when labeled training data is scarce, as is the case here.

The evaluated performance of the model, we analyze the precision, recall, and F1-score across different user groups. The presented mean, median, and standard deviation for these metrics provides insights into the model's overall performance (Fig. 3).

The plots show the scatter points of Precision, Recall, and F1-Score against the number of users, with regression lines and 95% confidence intervals shaded. These

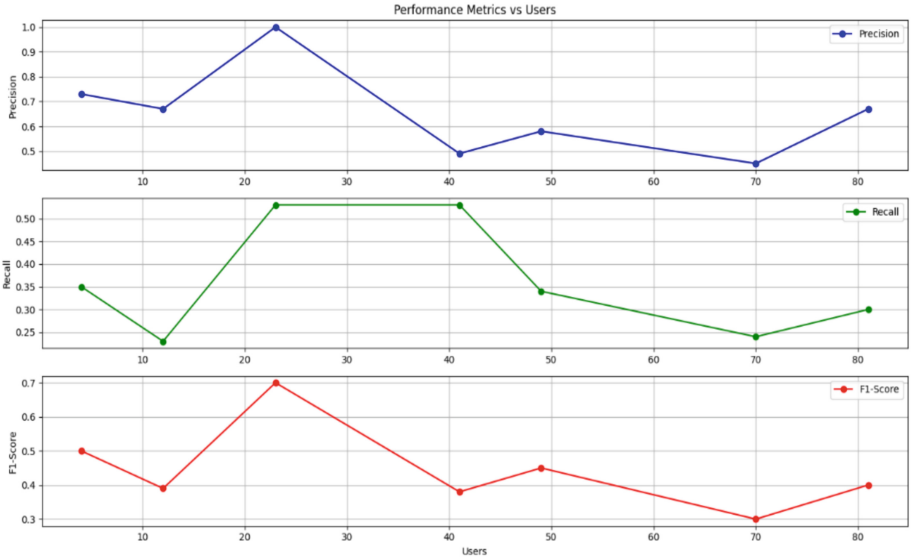


Fig. 3. Performance with respect to Precision, Recall and F1-Score

visualizations help in understanding the trend and variability of the performance metrics as the number of users increases (Table 3).

Table 3. Statistics at various user percentile

Users	Precision	Recall	F1-Score	
Mean	40	0.655714	0.36	0.445714
Median	41	0.67	0.34	0.4
Std. Dev	28.959742	0.182561	0.124633	0.128044

Interests, ideal modifying rate of key location of the K-means contrasts based on whether pretraining is utilized or not. This error emerges since preparing for this assignment without pretraining fizzled to meet after 30 ages employing a learning rate of 0.005. This proposes that pretraining assists meeting. Upon closer examination, comparing classification exactness's after as it was 20 training epochs uncovers that pretraining benefits all assignments, advance affirming its part in upgrading joining speed (Fig. 4).

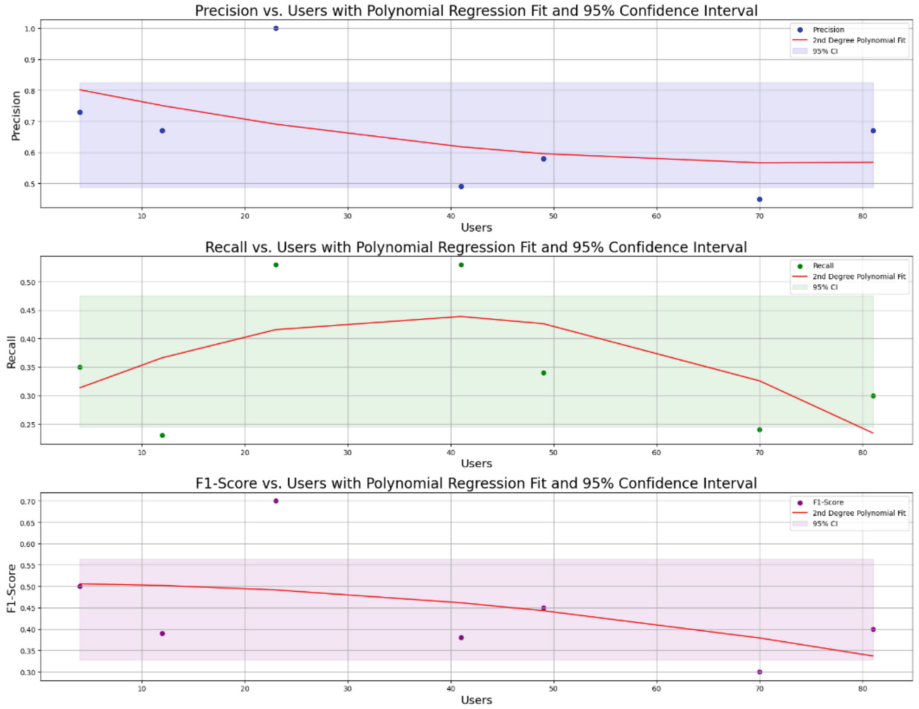


Fig. 4. Performance Metrics: Precision, Recall, and F1-Score Variability with Increasing User Base

5 Conclusion

A song recommender system that combines K-Means clustering and PLSA (Probabilistic Latent Semantic Analysis) is expected to offer a valuable service to users. This system would save users time searching for music by recommending songs based on their interests. It achieves this by identifying similar users based on their listening habits. To make accurate recommendations, the system would require a significant amount of user data.

The paper proposes a recommendation system for clients. It uses a technique called PLSA to analyze client preferences and suggest relevant items. A web application was developed to test the system, and it showed promising results based on accuracy, precision, and F1-score metrics using simulated data. In the future, the system could be applied to real client data, but this would require access to such data, which may not be readily available. Once sufficient client data is collected through the web application, the system can be used to generate real-world recommendations.

In future endeavors, the paper point to refine certain perspectives of the arrange design, especially centering on how input highlights are modeled within the lower layers. Investigating elective sorts of obvious units may surrender moved forward execution. Also, the paper arranges to examine differing techniques to advance the learning of significant highlights by the RBMs, past the sparsity punishment term utilized in these

tests. Analysts have too found a connect between users' music inclinations and their identities. Also, fast-paced music incorporates a stimulative impact, whereas moderate and delicate music contains a calming impact. These discoveries emphasize that music recommendation systems are not only tools for unwinding but too compelling devices for assembly different needs completely different settings. Be that as it may, there's constrained inquire about based on these experimental discoveries.

The evaluated performance of the model, we analyze the precision, recall, and F1-score across different user groups. The presented mean, median, and standard deviation for these metrics provides insights into the model's overall performance. The model achieves the best overall performance for the group with 23 users, as indicated by the highest precision, recall, and F1-score. Planning a personalized music recommender framework could be a complex assignment, requiring a profound understanding of users' needs and inclinations. As examined, future inquire about bearings will essentially center on user-centric music proposal frameworks. A study among competitors uncovered that professionals in sports and work out situations regularly select music subjectively without considering its motivational characteristics completely. Therefore, future music recommenders ought to direct clients to create educated music choices. Eventually, our objective is to bridge disconnected investigate endeavors over different disciplines through this think about.

References

1. Yading, S., Dixon, S., Pearce, M.: A survey of music recommendation systems and future perspectives. 9th International Symposium on Computer Music Modeling and Retrieval, pp. 395–410 (2012)
2. Yajie, H.O.M.: NextOne Player: A music recommendation system based on user behavior. In: ISMIR, pp. 103–108 (2011)
3. Douglas, E., Lamere, P.B.-M.T.G.S.: Automatic generation of social tags for music recommendation. In: Advances in Neural Information Processing Systems, pp. 385–392 (2008)
4. Seungmin, R., Song, S.H.E.K.M.: COMUS: Ontological and rule-based reasoning for music recommendation system. In: Advances in Knowledge Discovery and Data Mining. Springer Berlin Heidelberg, pp. 859–866 (2009)
5. Kunsu, K., Lee, D.Y.T.B.L.J.H.: A music recommendation system based on personal preference analysis. In: IEEE First International Conference on the Applications of Digital Information and Web Technologies, ICADIWT, pp 102–106 (2008)
6. Kazuyoshi, Y., Goto, M.K.K.O.T.O.H.G.: An efficient hybrid music recommender system using an incrementally trainable probabilistic generative model. IEEE Trans Audio Speech Lang Process **16**, 435–447 (2008)
7. Ziwon, H., Lee, K.L.K.: Music recommendation using text analysis on song requests to radio stations. Expert Syst. Appl. **41**, 2608–2618 (2014)
8. Singh, G., Boparai, R.D.S.K.M.: A novel hybrid K-Means PLSA technique for music recommender. Indian J. Sci. Technol. **9**, 1–4 (2016)
9. Sharma, S.N.M.: Analyzing the Potential of Smart Cities: Technologies, Frameworks, Vulnerabilities, Threats, and Information Security Solutions. In: ASU International Conference in Emerging Technologies for Sustainability and Intelligent Systems (ICETSIS) (2024)

10. Sharma, S.N.M.: Original Research Article Anomaly detection in Smart Traffic Light system using blockchain: Securing through proof of stake and machine learning. J. Auton. Intel. (2024)
11. Sharma, S., Manuja, M.P.B.S.B.C.S.: Online education system in the age of pandemics: a statistical analysis of current Covid-19 to the teaching and learning pedagogies in India. In: AIP Conference Proceedings, p. 20066 (2022)
12. Sharma, N.S.M.: Integration of Blockchain Technology into Smart Cities for Information Security: Research Constituents and Need of Research. In: 7th International Joint Conference on Computing Sciences (ICCS-2023) (2023)
13. Bali, S.S.S.: Anticipating Legal Issues Associated with the Cyber Security and Privacy of Automated Driving Systems in India. In: Auton. Driv. Adv. Driver-Assistance Syst. Appl. Dev. Leg. Issues, Test. p. 389 (2021)
14. Sharma Tushar, A., Sharma, S.S.A.K.A.M.A.S.: Asteroid Hazard Prediction Using Machine Learning: A Comparative Analysis of Different Algorithms. In: 3rd International Conference on Advancement in Electronics & Communication Engineering (AECE), pp. 673–677 (2024)
15. Sharma, S.N.M.: Horizoning recent trends in the security of smart cities: Exploratory analysis using latent semantic analysis. J. Intell. Fuzzy Syst. 1–18 (2023)
16. Thakur, A.S., Sharma, T.S.: Design of Semantic Segmentation Algorithm to Classify Forged Pixels. In: 12th International Conference on Communication Systems and Network Technologies (CSNT), pp. 409–413 (2023)
17. Sharma, T.U., Kaur, S.S.: Inclusive and Relative Analysis of Nature Inspired Optimization Algorithms in Reference to Sworn Intelligence. In: 8th International Conference on Signal Processing and Communication (ICSC), pp. 397–403 (2022)
18. Hanlin Goh Nicolas Thome, M.C.: Biasing restricted boltzmann machines to manipulate latent selectivity and sparsity. In: Deep Learning and Unsupervised Feature Learning Workshop — NIPS (2010)
19. Hung-Chen, C.C.A.L.P.: A music recommendation system based on music and user grouping. J. Intell. Inf. Syst. **24**, 113–132 (2005)
20. Yoon, T., Lee, S.Y.K.H.K.D.L.J.H.: A personalized music recommendation system with a time-weighted clustering. In: 4th International IEEE Conference on Intelligent Systems IS'08, pp. 48–52 (2008)
21. Bo, S., Wang, D.L.T.O.M.: Music recommendation based on acoustic features and user access patterns. IEEE Trans Audio Speech Lang Process **17**, 1602–1611 (2009)
22. Cheng-Che, L.T.V.S.: A novel method for personalized music recommendation. Expert Syst. Appl. **36**, 10035–10044 (2009)
23. Wassan, S., Chen, X., Shen, T., Waqar, M., Jhanjhi, N.Z.: Amazon product sentiment analysis using machine learning techniques. Revista Argentina de Clínica Psicológica **30**(1), 695 (2021)
24. Jena, K.K., et al.: E-learning course recommender system using collaborative filtering models. Electronics **12**(1), 157 (2022)
25. Zaman, N., Almusalli, F.A.: Smartphones power consumption & energy saving techniques. In: 2017 international conference on innovations in electrical engineering and computational technologies (ICIEECT), pp. 1–7. IEEE (2017)
26. Humayun, M., Jhanjhi, N.Z., Alamri, M.Z., Khan, A.: Smart cities and digital governance. In: Employing recent technologies for improved digital governance, pp. 87–106. IGI Global (2020)



Breast Cancer Diagnosis Using Machine Learning and Knowledge Discovery in Data

Mayank Arora(✉), Poonam Saini, and Kanu Goel

Punjab Engineering College (Deemed to Be University), Chandigarh, India
mayankarora.mt22cse@pec.edu.in

Abstract. Breast cancer, a condition characterized by the uncontrolled growth of damaged cells in the tissues of the breast is a major concern to societies in the world today. For this study, we selected Wisconsin Breast Cancer dataset analyzing patterns and risk factors using Decision Tree, Random Forest, AdaBoost, XGBoost and Gradient Boosting techniques. Through examination of the measures such as size, shape, margin and cellular attributes of tumors, it becomes the focal point to enhance the diagnostic accuracy, early detection and subsequent treatment. As suggested in this approach, it offers fundamental instruments to help clinical personnel in expanding diagnoses of illnesses and determinations of the most pertinent remedy plans. Through these supervised machine learning methods, it is aimed to increase the understanding of breast cancer, and therefore, contribute to the extension of diagnostic procedures and therapeutic approaches in clinical practice. However, the XGBoost Algorithm had a better accuracy of 93.20%. It furthers clinical practice by offering reliable prediction models to aid in predicting breast cancer diagnosis and the knowledge gathered on the disease.

Keywords: Breast Cancer · Machine Learning · Resampling · Classification · Healthcare

1 Introduction and Related Works

Breast cancer is still in focus of attention all over the world as it is among the most common cancer types and still is the leading cause of cancer related deaths among women. An accurate diagnosis of the disease is the key to increasing the survival rate of patients, as well as starting treatment as early as possible [13]. However, modalities like mammography, ultrasound and biopsy provide hurdles in diagnosis owing to their aspects like sensitivity or specificity and most often these are invasive procedures [1].

The implementation of artificial ML into the healthcare framework is shown to have a possibly positive impact on diagnosing diseases more accurately [12]. Cardiac disease causes 17.3 million deaths annually and this is why early pre- diction is important. This paper employs data-mining on the AHA dataset and utilizes Weka to analyze the results and deduces that random tree method out- performs in accuracy [7].

This paper presents an elaborate ML model for the classification of breast cancer based on the Breast Cancer Wisconsin (Diagnostic) data set [4]. Our selected

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 278–286, 2025.
https://doi.org/10.1007/978-3-031-91008-1_26

ML classifiers are Decision Tree, Random Forest, Gradient Boosting, AdaBoost, and XGBoost.

Furthermore, this study also includes a comprehensive use of exploratory data analysis (EDA) that employs density plots to give a visual description and density of the given dataset features [9]. It can be stated that these visual plots are useful for understanding the potential dependencies between features and the target variable.

Section 2 the related work done in the application of ML for breast cancer prediction has been discussed. In Sect. 3, details about the data set is provided and the process of data pre-processing is explained followed by the experimental methodology in terms of the ML models used and the evaluation metrics. Section 4 is about the future works. Section 5 shows conclusion of the study findings of the research conducted.

Khandaker Mohammad Moji Uddin et al. [11] while conducting a survey using a large number of datasets including the Wisconsin Breast Cancer Dataset, used classifiers including the KNN, SVM, LR, NB, Gradient Boosting, Neural Network Classifier and others. This research supports the use of ensemble methods and neural networks, as the above analyses demonstrate high accuracy, precision, recall, and F1-score.

In a similar context, Varsha Nemade et al. [5] have stressed upon the conventional ML classifiers including NB, LR, SVM, KNN, DTs, and some ensemble methods including AB, XGB, and AB for the problems of breast cancer classification. They emphasized accuracy but along with it emphasized on precision, recall, F1 score and area under the curve in their work and justified how the ensemble method enhances the predictive accuracy.

Moreover, Souvik Pal et al. [6] proposed a new segmentation method based on the integration of FOA and FCM for enhancing the performance of cancerous area identification in MRI images. Their approach yielded an accuracy of 96%, which is satisfactory for the problem formulation of the project.

Also, Abdur Rasool [8] provided some ideas about the implementations of SVM that are LR, KNN, Evolutionary Algorithm with benchmark sets like WBCD& BCCD. In their study, they used accuracy, precision, recall, and F1-score where they demonstrated the importance of the dataset and adjustment of the algorithm to improve diagnostic accuracy.

A hybrid CNN was developed by Angayarkanni et al. [10] in the area of deep learning where the preprocessing techniques such as median filtering and Otsu-based segmentation were the components of the proposed model for analyzing the mammography images.

1.1 Objectives of Current Research

The present investigation enhances the breast cancer diagnosis by applying KDD with ensemble methods to enhance the prediction accuracy. Unlike the previous studies that have investigated the performance of a single or a couple of algorithms, we compared more than one classifier, while handling imbalanced dataset. Consequently, to achieve a higher efficiency, we utilize certain sophisticated methods of machine learning for the analysis of the Breast Cancer Wisconsin (Diagnostic) dataset. Table 1 illustrates a summary of related works.

Table 1. A Table of Related Literature.

Sr. No.	Authors	Method Used	Type of Learning	Disease/Dataset	Performance Metrics Used
1	Khandaker Mohammad Moji Uddin et al. [11]	KNN, SVM, LR, NB, GB, NCC, VC, AB, MLP	Machine Learning, Deep Learning	Wisconsin Breast Cancer Dataset	Accuracy, Precision, Recall, F1-Score, Specificity
2	Varsha Nemade et al. [5]	NB, LR, SVM, KNN, DT, XGB, AB	Machine Learning	Breast Cancer Dataset	Accuracy, Precision, Recall, F1-Score, AUC
3	Jiande Wu et al. [13]	LR, KNN, NB, SVM	Machine Learning	Breast Cancer Dataset	Accuracy, Precision, Recall, F1-Score, Specificity
4	Vikas Chaurasia et al. [4]	AB, GBC, RF, ET, XGB	Machine Learning	Wisconsin Breast Cancer Dataset	Accuracy
5	Mohammed Amine Naji [1]	SVM, RF, LR, DT, KNN	Machine Learning	Wisconsin Breast Cancer Dataset	Accuracy, Sensitivity, F1-Score, Precision
6	Abdur Rasool [8]	SVM, LR, KNN, EC	Machine Learning	WBCD, BCCD Datasets	Accuracy, Precision, Recall, F1-Score
7	Vincent Peter C. Magboo [3]	NB, SVM, LR, KNN	Machine Learning	Wisconsin Breast Cancer Dataset	Precision, Recall, F1-Score, AUPRC, Cohen Kappa Score
8	Puja Gupta et al. [2]	KNN, LR, DT, RF, SVM with RBF, ANN	Machine Learning, Deep Learning	Wisconsin Breast Cancer Dataset	Accuracy, Sensitivity, F1-Score, Precision
9	Angayarkanni et al. [10]	CNN with median filter and Otsu-based segmentation	Deep Learning	Mammography images (50,000 images)	Accuracy
10	Besma Senai et al. [9]	CNN + ML Algorithms	Deep Learning, Machine Learning	MIAS and DDSM mammography datasets	Accuracy, Precision, Recall, F1-Score

2 Research Methodology

The focus of the research is to construct a classifier function that would predict the status of a breast Cancer based on clinical measurements. In this model, several categories of algorithms such as Decision Trees, XGBoost, Random Forest, and the Gradient Boosting classifier of the machine learning category will be applied to improve the classification results. The features that are used in the model include several features extracted from images of fine needle aspirate (FNA) of breast masses and other parameters that may be related to the patient's clinical condition.

2.1 Subject and Proposed Approach

Data analysis is performed using supervised and ensemble learning involving employing the principles of KDD that is Knowledge Discovery in Data. The choice of the right algorithm is crucial and entails the assessment of data performance precisely in different models. Some of the techniques used in ensemble learning. This approach is

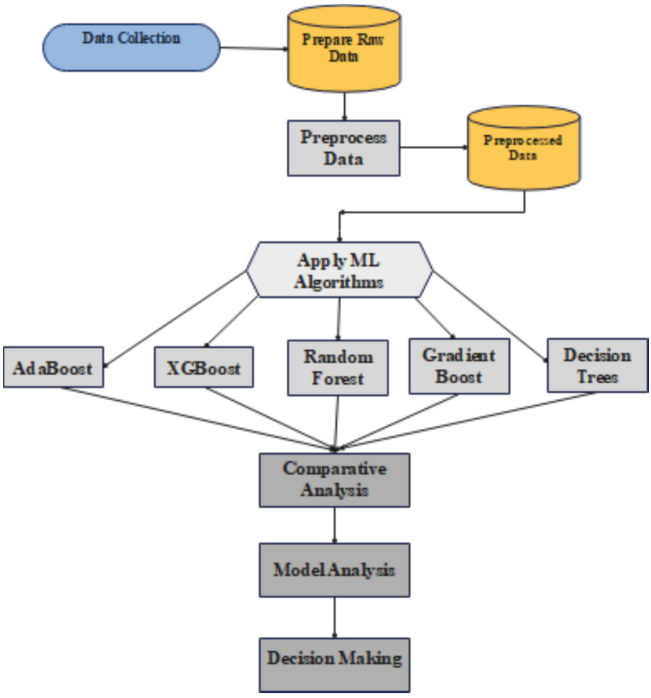


Fig. 1. Architecture of Proposed Methodology

systematically depicted in the flow chart in Fig. 1 which gives a sequential process of the project.

2.2 Dataset Overview

This research uses the Wisconsin Breast Cancer dataset from the UCI Machine Learning Repository with 13 clinical features. In total, the data set has 357 benign and 212 malignant cancer instances.

2.3 Data Imbalance and SMOTE

To deal with class imbalance issue, we synthesize some new samples by using SMOTE method to add new samples for the small class, which can enhance the ability of the model for classifying between the two classes. However, it has been clearly seen that SMOTE may overfit and other problems may occur. ADASYN is best used in conjunction with SMOTE since it provides an approach to the synthesis of new samples for difficult minority class examples improves classifiers' performance and minimizes over-fitting. Hence, these classifiers are assessed by accuracy, precision, recall as well as F1-Score to determine the most appropriate model for predicting breast cancer.

2.4 Data Pre-processing

A thorough pre-processing phase addresses data reliability issues, including handling missing values and ensuring consistent data types. This foundational step involves transforming raw data into a usable format, crucial for subsequent analysis.

2.5 Resampling Techniques

To address the prevalent issue of data imbalance in predictive modeling, the ADASYN technique is employed to generate new samples for the minority class, thereby enhancing dataset balance. This method is particularly crucial for un- evenly distributed data, improving forecast reliability. Additionally, the SMOTE further increases minority class density, demonstrating its efficacy in overcoming class imbalance and enhancing model classification quality. ADASYN differs from traditional methods by generating synthetic samples based on the density estimation of existing data, focusing on underrepresented areas to more accurately capture the true nature of the data.

2.6 Evaluation Metrics

In tasks that involve only two classes like the breast cancer diagnosis problems, we see important parameters like accuracy whereby it quantifies the correctness of the prediction; the precision parameter which quantifies the right proportion of the positive predictions. Recall evaluates the model's capacity to classify all the true positives accurately, very useful for medical diagnosis where false negatives are fatal. The F1-score is the average of precision and recall in one single measure thus most suited for imbalanced datasets. ROC measures the model's efficacy in identifying classes with respect to varying threshold levels and provides a glimpse of the discriminative competence of the model.

3 Results and Discussion

To thoroughly understand the interrelationships among various features, a pairplot is constructed (Fig. 2), also correlation matrix was plotted for features vs features in Fig. 3. Model evaluation is performed using Out-of-Sample Testing or Cross-Validation, specifically employing K-Fold cross-validation with values of 5. This method divides the data into multiple subsets, enhancing model validation without assumptions about model potential. Performance metrics such as accuracy, precision, recall, F1-score, and AUC-ROC are recorded for each algorithm, providing a comprehensive assessment of their efficacy and informing the selection of the most suitable model.

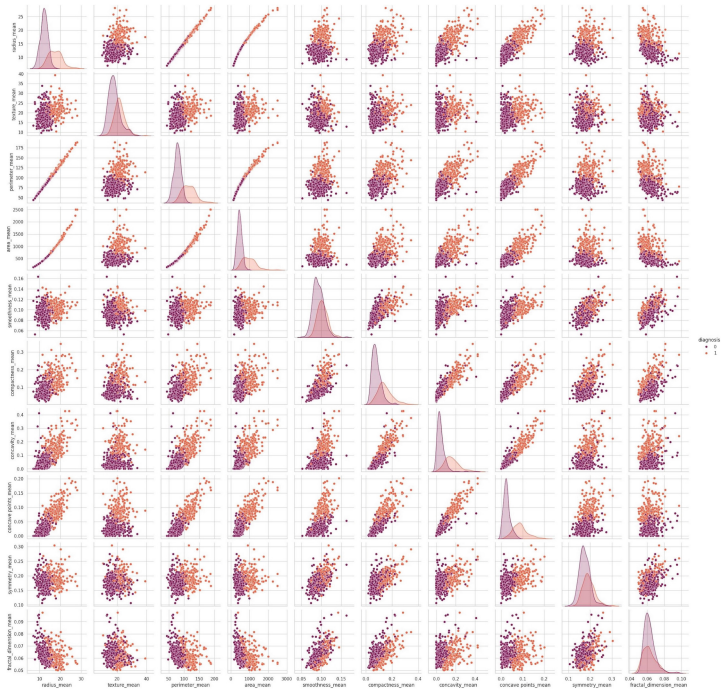


Fig. 2. Pairplots for various features in the dataset

3.1 Descriptive Results

The Decision Tree algorithm provides good results with accuracy of 89% of the total percentage; precision of 89. 4% for Precision and F1-Score of 90.70%. Its ROC value is presented as 89. 53%, Likewise, Random Forest approach produces high accuracy of 90. 8%, while a significant ROC value of 97. 90%. The performance of the XGBoost algorithm is also impressive, it achieves an accuracy of 90. 20%, precision of 81, 40%, recall of 91. 60%, an F1-Score of 86. 27%, as well as the ROC value of 97. 65%. The Table 2 shows the performance comparison of algorithms. The ROC value for AdaBoost algorithm is 97.65 The Gradient Boost Classifier has ROC value of 97. 54%. For comparison of ROC Curves of the above algorithms, please refer to Fig. 4.

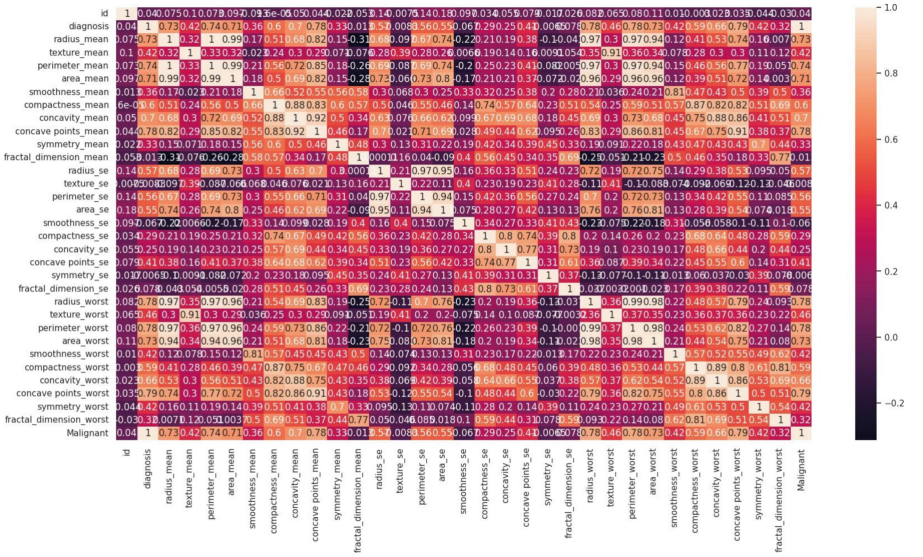


Fig. 3. Correlation Matrix for various features in the dataset

Table 2. Performance metrics of various algorithms

Sr. No.	Algorithm	Accuracy	Precision	Recall	F1-Score	AUC-ROC
1	Decision Tree	89%	89.09%	92.40%	90.70%	89.53%
2	Gradient Boost	90.21%	84%	91.50%	87.54%	95.00%
3	Random Forest	90.90%	84.50%	89.50%	86.80%	91.23%
4	XGBoost	93.20%	91.40%	91.60%	91.50%	97.65%
5	AdaBoost	93.06%	88%	91.60%	89.68%	97.90%

4 Future Work

It is possible to improve the prediction of breast cancer in the future with the help of deep learning and a new relevant data set. CNNs well looks at a medical image for discrimination between the images from data for the progression of the disease. The information derived from genomics analysis would improve on the clinical data that the patients received in regard to treatment plans. Techniques such as transfer learning and model ensemble serves as a way to build a more robust and accurate model to further improve the diagnostic capability and the patients' condition.

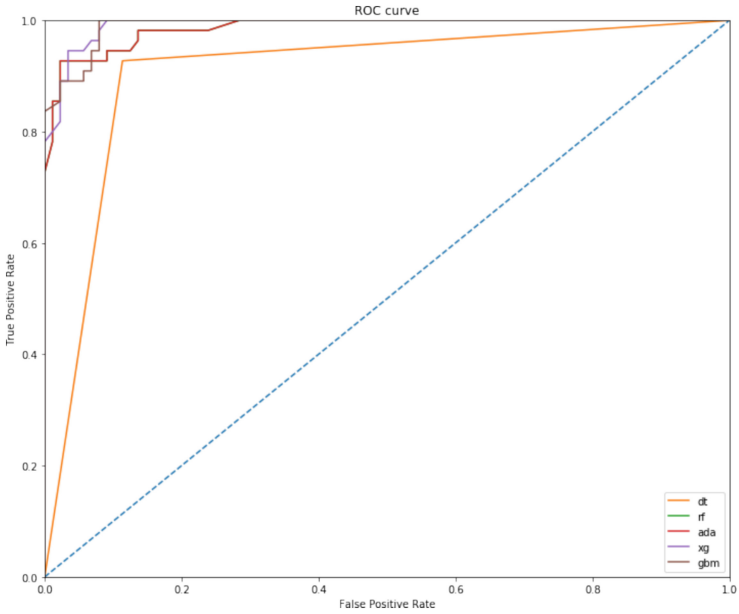


Fig. 4. Comparison of ROC Curves for various Algorithm used in the Study

5 Conclusion

The studies show that the XGBoost algorithm offers the best result for the diagnosis of breast cancer, with the highest accuracy and ROC rates among all the algorithms compared in studies above. Thus, XGBoost is a very good fit for this task; not only does it allow for handling imbalanced data, but it is capable of capturing intricate patterns as well. However, the primary drawback inherent only to the current study is that it uses only one dataset and some synthetic data methods might overfit the models. Expanding datasets and incorporating advanced techniques such as deep learning to further enhance the accuracy and efficiency of breast cancer diagnosis [11].

References

1. Filali, S., Aarika, K., Naji, M., Benlahmar, E.H., Abdelouahid, R.A., Debauche, O.: Machine learning algorithms for breast cancer prediction and diagnosis. Procedia Comput. Sci. **191**, 487–492 (2021). https://doi.org/10.1016/j.procs.2021.07.062
2. Haq, I.U., Hussain, M., Azeem, M.M., Bashir, S.: Breast cancer detection: a comparative study using machine learning models. Int. J. Innov. Sci. Res. Technol. **8**, 759–766 (2023). https://doi.org/10.5281/zenodo.8285931
3. Magboo, V.P.C., Magboo, M.S.A.: Machine learning classifiers on breast cancer recurrences. Procedia Comput. Sci. **192**, 2742–2752 (2021). https://doi.org/10.1016/j.procs.2021.09.044
4. Mustafa, W.A., et al.: Breast cancer detection and classification on mammogram images using morphological approach. In: 2022 5th International Conference on Engineering Technology and its Applications (IICETA), pp. 260–264 (2022). https://doi.org/10.1109/IICETA54559.2022.9888432

5. Nemade, V., Fegade, V.: Machine learning techniques for breast cancer prediction. Procedia Comput. Sci. **218**, 1314–1320 (2023). https://doi.org/10.1016/j.procs.2023.01.110
6. Pal, S., Maity, S., Adhikari, S., Alkhafaji, M., Díaz, V.: Breast cancer detection using hybrid segmentation using FOA and FCM clustering. In: Peng, S., Jhanjhi, N., Pal, S., Amsaad, F. (eds.) Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. ICMMCS 2023. Advances in Intelligent Systems and Computing, vol. 1450, pp. 67–78. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3_6
7. Poornima, V., Gladis, D.: An empirical study of heart disease prediction system using various machine learning classification algorithms. In: Peng, S., Hao, R., Pal, S. (eds.) Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing, vol. 1292, pp. 193–204. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4_13
8. Rasool, D., Bunterngchit, C., Tiejian, L., Islam, M., Qu, Q., Jiang, Q.: Improved machine learning-based predictive models for breast cancer diagnosis. Int. J. Environ. Res. Public Health **19**, 3211 (2022). https://doi.org/10.3390/ijerph19063211
9. Senaï, B., Rahal, S., Khiat, S.: An optimized hybrid model of convolutional neural networks and extreme gradient boosting for enhanced mammographic tumor classification. Ingénierie des Systèmes d'Information **28**(3), 725–736 (2023). https://doi.org/10.18280/isi.280323
10. SP, A.: Hybrid convolution neural network in classification of cancer in histopathology images. J. Digit. Imaging **35**(2), 248–257 (2022). https://doi.org/10.1007/s10278-021-00541-3
11. Uddin, K.M.M., Biswas, N., Rikta, S.T., Dey, S.K.: Machine learning-based diagnosis of breast cancer utilizing feature optimization technique. Comp. Methods Progr. Biomed. Update **3**, 100098 (2023). https://doi.org/10.1016/j.cmpbup.2023.100098
12. Wang, Z., Xu, G., Lin, R., Wang, H., Ren, J.: Energy performance contracting, risk factors, and policy implications: identification and analysis of risks based on the best-worst network method. Energy **170**, 1–13 (2019). https://doi.org/10.1016/j.energy.2018.12.140
13. Wu, J., Hicks, C.: Breast cancer type classification using machine learning. J. Pers. Med. **11**, 61 (2021). https://doi.org/10.3390/jpm11020061

Study of Soft $\beta - \sigma -$ Field

Shangul F. Abdulaziz(✉) and Hassan H. Ebrahim

Department of Mathematics, College of Computer Science and Mathematics, Tikrit University, Tikrit, Iraq

shnkwlbas577@gmail.com, hassan1962pl@tu.edu.iq

Abstract. This paper is concerned with the new space namely soft measurable space over soft $\beta - \sigma -$ field. It is accordingly devoted to the basic properties of this new space as well as characterizations of this concept are shown such as Let $\{\widetilde{\mathcal{H}}_\alpha\}_{\alpha\in I}$ be a family of soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$. Then so is $\widetilde{\bigcap_{\alpha\in I}}\widetilde{\mathcal{H}}_\alpha$, $\widetilde{bs(\widetilde{\mathcal{I}})}$ is the smallest soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contains $\widetilde{\mathcal{I}}$, If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$, then $\widetilde{\mathcal{I}}$ is a soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ iff $\widetilde{\mathcal{I}} = \widetilde{bs(\widetilde{\mathcal{I}})}$, If $\widetilde{\mathcal{I}}_1, \widetilde{\mathcal{I}}_2 \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ such that $\widetilde{\mathcal{I}}_1 \subset \widetilde{\mathcal{I}}_2 \subset \widetilde{bs(\widetilde{\mathcal{I}}_1)}$, then $\widetilde{bs(\widetilde{\mathcal{I}}_1)} = \widetilde{bs(\widetilde{\mathcal{I}}_2)}$, Suppose $\widetilde{\mathcal{H}}$ is a soft $\beta - \sigma -$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$, then a restriction of $\widetilde{\mathcal{H}}$ over $\mathcal{P}_\mathcal{B}$ is defined as:

$\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} = \{\mathcal{P}_N : \mathcal{P}_N = \mathcal{P}_M \widetilde{\bigcap} \mathcal{P}_\mathcal{B}$, where $\mathcal{P}_M \in \widetilde{\mathcal{H}}\}$. Suppose $\widetilde{\mathcal{H}}$is a soft b $-$ s $-$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$, then $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$is a softb $-$ s $-$ field on $\mathcal{U}$ relative to $\mathcal{P}_\mathcal{B}$ and Let $\{\widetilde{\mathcal{H}}_\alpha\}_{\alpha\in I}$ be a family of soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$. Then so is $\widetilde{\bigcap_{\alpha\in I}}\widetilde{\mathcal{H}}_\alpha$. Assume that $\mathcal{U}$ is a universal set and $\mathcal{E}$ is a set of parameters with respect to $\mathcal{U}$. If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$. Then the soft intersection of all soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, that contain $\widetilde{\mathcal{I}}$ is called the soft b $-$ field generated by $\widetilde{\mathcal{I}}$ and denoted by $\widetilde{\beta(\widetilde{\mathcal{I}})}$, that is, $\widetilde{\beta(\widetilde{\mathcal{I}})} = \widetilde{\bigcap}\{\widetilde{\mathcal{H}}_\alpha : \widetilde{\mathcal{H}}_\alpha$is a soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}_\alpha \forall \alpha \in I\}$.

Keywords: Measure · Fuzzy Set · Soft Set · $\sigma -$ field

1 Introduction

The notion of measure is one of significant topics in field of probability theory. Ahmed et al. [1–3] and [4] have been studied many kinds of family of sets as generalizations of $\sigma -$ field such as $\beta -$ field, $\beta - \sigma -$ field and fuzzy s $-$ algebra. The concept of soft set was studied in [5–7] and [8] where $\mathcal{U}$ is a universal set and $\mathcal{E}$ is a set of parameters with respect to $\mathcal{U}$. Let $\mathcal{A}$ be a nonempty subset of $\mathcal{E}$. Then the set of ordered pairs $\mathcal{P}_\mathcal{A} = \{(x, f_\mathcal{A}(\S)) : \S \epsilon \mathcal{E}, f_\mathcal{A}(\S) \epsilon P(\mathcal{U})\}$ is called a soft set on $\mathcal{U}$, where $f_\mathcal{A} : \mathcal{E} \to P(\mathcal{U})$ such that $f_\mathcal{A}(\S) = \Phi$ if $\S \notin \mathcal{A}$. The soft set $\mathcal{P}_\mathcal{A}$ is called null soft set and denoted by $\mathcal{P}_\Phi$ *or* $\widetilde{\Phi}$, if $f_\mathcal{A}(\S) = \Phi \forall \S \epsilon \mathcal{A}$. A soft set $\mathcal{P}_\mathcal{A}$ over $\mathcal{U}$ is called $\mathcal{A}-$ universal soft set and denoted by $\mathcal{P}_{\widetilde{\mathcal{A}}}$ or $\widetilde{\mathcal{A}}$, if $f_\mathcal{A}(\S) = \mathcal{U} \forall \S \epsilon \mathcal{A}$.

If $\mathcal{A} = \mathcal{E}$, then the $\mathcal{A}-$ universal soft set is called a universal soft set and denoted by $\mathcal{P}_{\widetilde{\mathcal{E}}}$ or $\widetilde{\mathcal{E}}$. The soft union of $\mathcal{P}_\mathcal{A}, \mathcal{P}_\mathcal{B}$ is denoted by $\mathcal{P}_\mathcal{A} \widetilde{\cup} \mathcal{P}_\mathcal{B}$ and defined by the approximate

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 287–295, 2025.
https://doi.org/10.1007/978-3-031-91008-1_27

function $f_{\mathcal{A}}(\S) \cup f_{\mathcal{B}}(\S)\ \forall \S \epsilon \mathcal{E}$. The soft intersection of $\mathcal{P}_{\mathcal{A}}, \mathcal{P}_{\mathcal{B}}$ is denoted by $\mathcal{P}_{\mathcal{A}} \widetilde{\bigcap} \mathcal{P}_{\mathcal{B}}$ and defined by the approximate function $f_{\mathcal{A}}(\S) \bigcap f_{\mathcal{B}}(\S)\ \forall \S \epsilon \mathcal{E}$.

Objective in paper to study some concepts in measure theory by using soft sets as well as this article aims to study the relationship between these notions.

2 Related Works and Results

Definition 1:
Let $\widetilde{\mathcal{H}}$ be a class of soft subsets of $\mathcal{P}_{\widetilde{\mathcal{E}}}(\widetilde{\mathcal{H}} \subseteq \widetilde{\mathrm{P}}(\mathcal{P}_{\widetilde{\mathcal{E}}}))$. Then $\widetilde{\mathcal{H}}$ is called soft $\beta - \sigma -$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ for short (soft $\mathrm{b} - \mathrm{s} -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$) if the following statement are holds:

1- $\mathcal{P}_{\Phi}, \mathcal{P}_{\widetilde{\mathcal{E}}} \in \widetilde{\mathcal{H}}$.

2- If $\mathcal{P}_{\mathrm{M}_1}, \mathcal{P}_{\mathrm{M}_2}, \cdots \in \widetilde{\mathcal{H}}$,. Then $\widetilde{\bigcap_{\mathrm{i}=1}^{\infty}} \mathcal{P}_{\mathrm{M}_\mathrm{i}} \in \widetilde{\mathcal{H}}$.

Definition 2:
$(\mathcal{P}_{\widetilde{\mathcal{E}}}, \widetilde{\mathcal{H}})$ is said soft measurable space over soft $\beta - \sigma -$ field and each member in $\widetilde{\mathcal{H}}$ is called soft measurable set.

Example 1:
If $\mathcal{U} = \{\sqcup_1, \sqcup_2\}$ & $\mathcal{E} = \{\rceil_1, \rceil_2\}$. Then all soft subsets of $\mathcal{P}_{\widetilde{\mathcal{E}}}$ is $\widetilde{\mathrm{P}}(\mathcal{P}_{\widetilde{\mathcal{E}}}) = \left\{ \begin{matrix} \mathcal{P}_{\Phi}, \mathcal{P}_{M_1}, \mathcal{P}_{M_2}, \mathcal{P}_{M_3}, \mathcal{P}_{M_4}, \mathcal{P}_{M_5}, \mathcal{P}_{M_6}, \mathcal{P}_{M_7}, \mathcal{P}_{M_8} \\ \mathcal{P}_{M_9}, \mathcal{P}_{M_{10}}, \mathcal{P}_{M_{11}}, \mathcal{P}_{M_{12}}, \mathcal{P}_{M_{13}}, \mathcal{P}_{M_{14}}, \mathcal{P}_{\widetilde{\mathcal{E}}} \end{matrix} \right\}$, where

$\mathcal{P}_{\Phi} = \{(\rceil_1, \Phi), (\rceil_2, \Phi)\}, \mathcal{P}_{M_1} = \{(\rceil_1, \{\sqcup_1\})\}, \mathcal{P}_{M_2} = \{(\rceil_1, \{\sqcup_2\})\},$
$\mathcal{P}_{M_3} = \{(\rceil_1, \mathcal{U})\}, \mathcal{P}_{M_4} = \{(\rceil_2, \{\sqcup_1\})\}, \mathcal{P}_{M_5} = \{(\rceil_2, \{\sqcup_2\})\}$
$\mathcal{P}_{M_6} = \{(\rceil_2, \mathcal{U})\}, \mathcal{P}_{M_7} = \{(\rceil_1, \{\sqcup_1\}), (\rceil_2, \{\sqcup_1\})\}$
$\mathcal{P}_{M_8} = \{(\rceil_1, \{\sqcup_1\}), (\rceil_2, \{\sqcup_2\})\}, \mathcal{P}_{M_9} = \{(\rceil_1, \{\sqcup_2\}), (\rceil_2, \{\sqcup_1\})\}$
$\mathcal{P}_{M_{10}} = \{(\rceil_1, \{\sqcup_2\}), (\rceil_2, \{\sqcup_2\})\}, \mathcal{P}_{M_{11}} = \{(\rceil_1, \mathcal{U}), (\rceil_2, \{\sqcup_1\})\}$
$\mathcal{P}_{M_{12}} = \{(\rceil_1, \mathcal{U}), (\rceil_2, \{\sqcup_2\})\}, \mathcal{P}_{M_{13}} = \{(\rceil_1, \{\sqcup_1\}), (\rceil_2, \mathcal{U})\}$
$\mathcal{P}_{M_{14}} = \{(\rceil_1, \{\sqcup_2\}), (\rceil_2, \mathcal{U})\}, \mathcal{P}_{\widetilde{\mathcal{E}}} = \{(\rceil_1, \mathcal{U}), (\rceil_2, \mathcal{U})\}.$
Let $\widetilde{\mathcal{H}}_1 = \{\mathcal{P}_{\Phi}, \mathcal{P}_{M_8}, \mathcal{P}_{M_{10}}, \mathcal{P}_{M_5}, \mathcal{P}_{\widetilde{\mathcal{E}}}\}$.
$\widetilde{\mathcal{H}}_2 = \{\mathcal{P}_{\Phi}, \mathcal{P}_{M_{10}}, \mathcal{P}_{M_{11}}, \mathcal{P}_{M_2}, \mathcal{P}_{\widetilde{\mathcal{E}}}\}$,
$\widetilde{\mathcal{H}}_3 = \{\mathcal{P}_{\Phi}, \mathcal{P}_{M_{11}}, \mathcal{P}_{M_{12}}, \mathcal{P}_{M_3}, \mathcal{P}_{\widetilde{\mathcal{E}}}\}$,
$\widetilde{\mathcal{H}}_4 = \{\mathcal{P}_{\Phi}, \mathcal{P}_{M_{11}}, \mathcal{P}_{M_{14}}, \mathcal{P}_{M_{10}}, \mathcal{P}_{\widetilde{\mathcal{E}}}\}$ and $\widetilde{\mathcal{H}}_5 = \{\mathcal{P}_{\Phi}, \mathcal{P}_{\widetilde{\mathcal{E}}}\}$.
Then $\widetilde{\mathrm{P}}(\mathcal{P}_{\widetilde{\mathcal{E}}}), \widetilde{\mathcal{H}}_1, \widetilde{\mathcal{H}}_2, \widetilde{\mathcal{H}}_3, \widetilde{\mathcal{H}}_4, \widetilde{\mathcal{H}}_5$ are soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

Proposition 1:
Let $\{\widetilde{\mathcal{H}}_\alpha\}_{\alpha \in \mathrm{I}}$ be a family of soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$. Then so is $\widetilde{\bigcap_{\alpha \in \mathrm{I}}} \widetilde{\mathcal{H}}_\alpha$.

Proof:
Since $\widetilde{\mathcal{H}}_\alpha$ is a soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}\ \forall \alpha \in \mathrm{I}$, then $\mathcal{P}_{\Phi}, \mathcal{P}_{\widetilde{\mathcal{E}}} \in \widetilde{\mathcal{H}}_\alpha \forall \alpha \in \mathrm{I}$. Hence $\widetilde{\bigcap_{\alpha \in \mathrm{I}}} \widetilde{\mathcal{H}}_\alpha \neq \{\mathcal{P}_{\Phi}\}$ and $\mathcal{P}_{\Phi}, \mathcal{P}_{\widetilde{\mathcal{E}}} \in \widetilde{\bigcap_{\alpha \in \mathrm{I}}} \widetilde{\mathcal{H}}_\alpha$.

Let $\mathcal{P}_{\mathrm{M}_1}, \mathcal{P}_{\mathrm{M}_2}, \cdots \in \widetilde{\bigcap_{\alpha \in \mathrm{I}}} \widetilde{\mathcal{H}}_\alpha$. Then $\mathcal{P}_{\mathrm{M}_1}, \mathcal{P}_{\mathrm{M}_2}, \cdots \in \widetilde{\mathcal{H}}_\alpha \forall \alpha \in \mathrm{I}$, since $\widetilde{\mathcal{H}}_\alpha$ is a soft $\beta - \sigma -$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}\ \forall \alpha \in \mathrm{I}$, then $\widetilde{\bigcap_{\mathrm{i}=1}^{\infty}} \mathcal{P}_{\mathrm{M}_\mathrm{i}} \in \widetilde{\mathcal{H}}_\alpha \forall \alpha \in \mathrm{I}$. so $\widetilde{\bigcap_{\mathrm{i}=1}^{\infty}} \mathcal{P}_{\mathrm{M}_\mathrm{i}} \in \widetilde{\bigcap_{\alpha \in \mathrm{I}}} \widetilde{\mathcal{H}}_\alpha$.

Therefore $\widetilde{\bigcap_{\alpha\in I}}\widetilde{\mathcal{H}}_\alpha$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

Definition 3:

If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$. Then a soft $\beta-\sigma-$ field generated by $\widetilde{\mathcal{I}}$ is defined as $\widetilde{bs(\widetilde{\mathcal{I}})} = \widetilde{\bigcap}\{\widetilde{\mathcal{H}}_\alpha : \widetilde{\mathcal{H}}_\alpha$is a softb $-$ s $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}_\alpha \forall\alpha \in I\}$.

Proposition 2:

$\widetilde{bs(\widetilde{\mathcal{I}})}$ is the smallest soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contains $\widetilde{\mathcal{I}}$.

Proof:

$\widetilde{bs(\widetilde{\mathcal{I}})}= \widetilde{\bigcap}\{\widetilde{\mathcal{H}}_\alpha : \widetilde{\mathcal{H}}_\alpha$is a soft b $-$ s $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}_\alpha\ \forall\alpha \in I\}$, then $\widetilde{bs(\widetilde{\mathcal{I}})}$ is soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$. Let $\widetilde{\mathcal{H}}_\alpha$ be a soft b $-$ s $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}_\alpha \forall\alpha \in I$.

Then $\widetilde{\mathcal{I}} \subseteq \widetilde{\bigcap}\widetilde{\mathcal{H}}_\alpha$. Therefore, $\widetilde{\mathcal{I}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}$. Assume $\widetilde{\mathcal{H}^\#}$ is a soft $\beta-\sigma-$field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ such that $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}^\#}$. Then $\widetilde{\bigcap}\{\widetilde{\mathcal{H}}_\alpha : \widetilde{\mathcal{H}}_\alpha$is a soft b $-$ s $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}_\alpha\ \forall\alpha \in I\} \subseteq \widetilde{\mathcal{H}^\#}$, hence $\widetilde{bs(\widetilde{\mathcal{I}})} \subseteq \widetilde{\mathcal{H}^\#}$. Therefore, $\widetilde{bs(\widetilde{\mathcal{I}})}$ is the smallest soft $\beta-\sigma-$field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}$.

Example 2:

Let $\mathcal{U} = \{\sqcup_1, \sqcup_2\}$ and$\mathcal{E} = \{\rceil_1, \rceil_2\}$. If $\widetilde{\mathcal{I}}$=$\{\{(\rceil_1, \{\sqcup_1\})\}, \{(\rceil_1, \{\sqcup_2\})\}\}$. Then $\widetilde{bs(\widetilde{\mathcal{I}})} = \{\mathcal{P}_\Phi, \{(\rceil_1, \{\sqcup_1\})\}, \{(\rceil_1, \{\sqcup_2\})\}, \{(\rceil_1, \mathcal{U})\}, \mathcal{P}_{\widetilde{\mathcal{E}}}\}$ is the smallest soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain$\widetilde{\mathcal{I}}$.

Proposition 3:

If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$, then $\widetilde{\mathcal{I}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ iff $\widetilde{\mathcal{I}} = \widetilde{bs(\widetilde{\mathcal{I}})}$.

Proof:

If $\widetilde{\mathcal{I}}$ is soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ & $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{I}}$. Since $\widetilde{bs(\widetilde{\mathcal{I}})}$ is the smallest soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, then $\widetilde{bs(\widetilde{\mathcal{I}})} \subseteq \widetilde{\mathcal{I}}$. But $\widetilde{\mathcal{I}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}$ from definition of $\widetilde{bs(\widetilde{\mathcal{I}})}$. Thus $\widetilde{\mathcal{I}} = \widetilde{bs(\widetilde{\mathcal{I}})}$.

Conversely:

we have $\widetilde{bs(\widetilde{\mathcal{I}})}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, hence $\widetilde{\mathcal{I}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

Theorem 1:

If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ and $\mathcal{P}_C \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$. Then $\left[\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C\right] \cup \mathcal{P}_{\widetilde{\mathcal{E}}} = [bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)] \cup \mathcal{P}_C$.

Proof:

First we prove $\mathcal{P}_\Phi, \widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C$ and $\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{M_j}$ $\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$ for$\mathcal{P}_{M_1}, \mathcal{P}_{M_2}, \cdots \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$.

$\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C = \{\mathcal{P}_M = \mathcal{P}_N\widetilde{\bigcap}\mathcal{P}_C : \mathcal{P}_N \in \widetilde{bs(\widetilde{\mathcal{I}})}\}$.

Since $\widetilde{bs(\widetilde{\mathcal{I}})}$ is soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, then $\mathcal{P}_\Phi \in \widetilde{bs(\widetilde{\mathcal{I}})}$.

Now, $\mathcal{P}_\Phi = \mathcal{P}_\Phi\widetilde{\bigcap}\mathcal{P}_C$, then $\mathcal{P}_\Phi \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$.

If $\mathcal{P}_{M_1}, \mathcal{P}_{M_2}, \cdots \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$. Then $\mathcal{P}_{M_j} = \mathcal{P}_{N_j}\widetilde{\bigcap}\mathcal{P}_C\ \forall j = 1, 2, \ldots$

When $\mathcal{P}_{N_j} \in \widetilde{bs(\widetilde{\mathcal{I}})}$. So, $\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{M_j} = \widetilde{\bigcap_{j=1}^{\infty}}(\mathcal{P}_{N_j}\widetilde{\bigcap}\mathcal{P}_C) = (\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{N_j})\widetilde{\bigcap}\mathcal{P}_C$

Since $\widetilde{bs(\widetilde{\mathcal{I}})}$ is soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\mathcal{P}_{N_1}, \mathcal{P}_{N_2}, \cdots \in \widetilde{bs(\widetilde{\mathcal{I}})}$, then $\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{N_j} \in \widetilde{bs(\widetilde{\mathcal{I}})}$ and hence $\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{M_j} \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$.

Therefore, $\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

To show $\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$. Let $\mathcal{P}_D \in \widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C$, then $\mathcal{P}_D = \mathcal{P}_Z\widetilde{\bigcap}\mathcal{P}_C$ where $\mathcal{P}_Z \in \widetilde{\mathcal{I}}$, but $\widetilde{\mathcal{I}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}$, thus $\mathcal{P}_Z \in \widetilde{bs(\widetilde{\mathcal{I}})}$ and hence $\mathcal{P}_Z\widetilde{\bigcap}\mathcal{P}_C \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$, consequentially $\mathcal{P}_D \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$. Hence, $\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$.

It is clear that $\mathcal{P}_{\widetilde{\mathcal{E}}} \in \left[\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C\right] \cup \mathcal{P}_{\widetilde{\mathcal{E}}}$, hence $\left[\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C\right] \cup \mathcal{P}_{\widetilde{\mathcal{E}}}$ is a soft $\beta-\sigma-$field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C$.

But $\widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$ is smallest soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C$ and $\mathcal{P}_C \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$, then $[\widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}] \cup \mathcal{P}_C \subseteq \left[\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C\right] \cup \mathcal{P}_{\widetilde{\mathcal{E}}}$.

To prove $\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C \subseteq \widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$. Define a class $\widetilde{\mathfrak{R}}$ as follows:

$\widetilde{\mathfrak{R}} = \{\mathcal{P}_{\widetilde{\mathcal{E}}}, \mathcal{P}_H : \mathcal{P}_H \bigcap \mathcal{P}_C \in \widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$ and $\mathcal{P}_H \in \widetilde{bs(\widetilde{\mathcal{I}})}\}$ and we claim that $\widetilde{\mathfrak{R}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathfrak{R}}$ contain $\widetilde{\mathcal{I}}$. Since $\widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$, $\widetilde{bs(\widetilde{\mathcal{I}})}$ are soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, then $\mathcal{P}_\Phi, \mathcal{P}_{\widetilde{\mathcal{E}}} \in \widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$ and $\mathcal{P}_\Phi \in \widetilde{bs(\widetilde{\mathcal{I}})}$.

Now, $\mathcal{P}_\Phi = \mathcal{P}_\Phi\widetilde{\bigcap}\mathcal{P}_C$, then $\mathcal{P}_\Phi \in \widetilde{\mathfrak{R}}$.

Let $\mathcal{P}_{H_1}, \mathcal{P}_{H_2}, \cdots \in \widetilde{\mathfrak{R}}$. Then $\mathcal{P}_{H_j}\widetilde{\bigcap}\mathcal{P}_C \in \widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$, $\mathcal{P}_{H_j} \in \widetilde{bs(\widetilde{\mathcal{I}})}$

$\forall j = 1, 2, \ldots$ now, $(\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{H_j})\widetilde{\bigcap}\mathcal{P}_C = \widetilde{\bigcap_{j=1}^{\infty}}(\mathcal{P}_{H_j}\widetilde{\bigcap}\mathcal{P}_C)$.

Since $\widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$, $\widetilde{bs(\widetilde{\mathcal{I}})}$ are soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, then

$(\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{H_j})\widetilde{\bigcap}\mathcal{P}_C = \widetilde{\bigcap_{j=1}^{\infty}}(\mathcal{P}_{H_j}\widetilde{\bigcap}\mathcal{P}_C) \in \widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$ and

$(\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{H_j}) \in \widetilde{bs(\widetilde{\mathcal{I}})}$, hence by the definition of $\widetilde{\mathfrak{R}}$, we get

$(\widetilde{\bigcap_{j=1}^{\infty}}\mathcal{P}_{H_j}) \in \widetilde{\mathfrak{R}}$.

Therefore, $\widetilde{\mathfrak{R}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

Let $\mathcal{P}_N \in \widetilde{\mathcal{I}}$. Then $\mathcal{P}_N\widetilde{\bigcap}\mathcal{P}_C \in \widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C$. Since $\widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$, $\widetilde{bs(\widetilde{\mathcal{I}})}$ are soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contains $\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C$ and $\widetilde{\mathcal{I}}$ respectively, then $\mathcal{P}_N\widetilde{\bigcap}\mathcal{P}_C \in \widetilde{bs(\widetilde{\mathcal{I}}\widetilde{\bigcap}\mathcal{P}_C)}$ and $\mathcal{P}_N \in \widetilde{bs(\widetilde{\mathcal{I}})}$. Hence $\mathcal{P}_N \in \widetilde{\mathfrak{R}}$, thus $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathfrak{R}}$. Consequentially, $\widetilde{\mathfrak{R}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathfrak{R}}$ contain $\widetilde{\mathcal{I}}$.

But $\widetilde{bs(\widetilde{\mathcal{I}})}$ is a smallest soft $\beta-\sigma-$field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contains $\widetilde{\mathcal{I}}$, so we get $\widetilde{bs(\widetilde{\mathcal{I}})} \subset \widetilde{\mathfrak{R}}$.

Let $\mathcal{P}_M \in \widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C$, then $\mathcal{P}_M = \mathcal{P}_Z\widetilde{\bigcap}\mathcal{P}_C$ where $\mathcal{P}_Z \in \widetilde{bs(\widetilde{\mathcal{I}})}$,hence $\mathcal{P}_Z \in \widetilde{\Re}$, thus $\mathcal{P}_Z\widetilde{\bigcap}\mathcal{P}_C \in bs(\widetilde{\mathcal{I}\bigcap}\mathcal{P}_C)$, that is, $\mathcal{P}_M \in bs(\widetilde{\mathcal{I}\bigcap}\mathcal{P}_C)$. Consequentially, $\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C \subseteq \widetilde{bs(\widetilde{\mathcal{I}\bigcap}\mathcal{P}_C)}$.

Therefore, $\left[\widetilde{bs(\widetilde{\mathcal{I}})}\widetilde{\bigcap}\mathcal{P}_C\right] \cup \mathcal{P}_{\widetilde{\mathcal{E}}} = [bs(\widetilde{\mathcal{I}\bigcap}\mathcal{P}_C)] \cup \mathcal{P}_C$.

Proposition 4:

If $\widetilde{\mathcal{I}}_1, \widetilde{\mathcal{I}}_2 \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ such that $\widetilde{\mathcal{I}}_1 \subset \widetilde{\mathcal{I}}_2$, then $\widetilde{bs(\widetilde{\mathcal{I}}_1)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.

Proof:

To prove $\widetilde{bs(\widetilde{\mathcal{I}}_1)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_2)}$. We must prove that $\widetilde{bs(\widetilde{\mathcal{I}}_2)}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}_1$. Let $\widetilde{\mathcal{H}} \in \widetilde{bs(\widetilde{\mathcal{I}}_2)}$. Then $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}_2$ but $\widetilde{\mathcal{I}}_1 \subset \widetilde{\mathcal{I}}_2$ by hypothesis, thus $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ which include $\widetilde{\mathcal{I}}_1$ which implies that $\widetilde{bs(\widetilde{\mathcal{I}}_2)}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}_1$.

But $\widetilde{bs(\widetilde{\mathcal{I}}_1)}$ is the smallest soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}_1$. Therefore, $\widetilde{bs(\widetilde{\mathcal{I}}_1)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.

Proposition 5:

If $\widetilde{\mathcal{I}}_1, \widetilde{\mathcal{I}}_2 \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ such that $\widetilde{\mathcal{I}}_1 \subset \widetilde{\mathcal{I}}_2 \subset \widetilde{bs(\widetilde{\mathcal{I}}_1)}$, then $\widetilde{bs(\widetilde{\mathcal{I}}_1)} = \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.

Proof:

clearly $\widetilde{bs(\widetilde{\mathcal{I}}_1)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.

To prove $\widetilde{bs(\widetilde{\mathcal{I}}_2)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_1)}$. Let$\widetilde{\mathcal{H}} \in \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.

Then $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}_2$ but $\widetilde{\mathcal{I}}_1 \subset \widetilde{\mathcal{I}}_2$ by hypothesis, thus $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contain $\widetilde{\mathcal{I}}_1$ which implies that $\widetilde{\mathcal{H}} \in \widetilde{bs(\widetilde{\mathcal{I}}_1)}$. Consequentially, $\widetilde{bs(\widetilde{\mathcal{I}}_2)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_1)}$.

Therefore, $\widetilde{bs(\widetilde{\mathcal{I}}_1)} = \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.

Definition 4:

Suppose $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$field on $\mathcal{U}$ relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B}\widetilde{\subset}\mathcal{P}_{\widetilde{\mathcal{E}}}$, then a restriction of $\widetilde{\mathcal{H}}$ over $\mathcal{P}_\mathcal{B}$ is defined as:

$\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} = \{\mathcal{P}_N : \mathcal{P}_N = \mathcal{P}_M\widetilde{\bigcap}\mathcal{P}_\mathcal{B}$, where $\mathcal{P}_M \in \widetilde{\mathcal{H}}\}$.

Proposition 6:

Suppose $\widetilde{\mathcal{H}}$is a softb $-$ s $-$ fieldon$\mathcal{U}$relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and

$\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B}\widetilde{\subset}\mathcal{P}_{\widetilde{\mathcal{E}}}$, then

$\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$is a soft b $-$ s $-$ field on $\mathcal{U}$relative to $\mathcal{P}_\mathcal{B}$.

Proof:

Since $\mathcal{P}_\Phi, \mathcal{P}_{\widetilde{\mathcal{E}}} \in \widetilde{\mathcal{H}}$ and$\mathcal{P}_\Phi = \mathcal{P}_\Phi\widetilde{\bigcap}\mathcal{P}_\mathcal{B}, \mathcal{P}_\mathcal{B} = \mathcal{P}_{\widetilde{\mathcal{E}}}\widetilde{\bigcap}\mathcal{P}_\mathcal{B}$,

Then $\mathcal{P}_\Phi, \mathcal{P}_\mathcal{B} \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$.
Let $\mathcal{P}_{N_1}, \mathcal{P}_{N_2}, \cdots \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$, then $\mathcal{P}_{N_k} = \mathcal{P}_{M_k} \widetilde{\bigcap} \mathcal{P}_\mathcal{B}$.
where $\mathcal{P}_{M_k} \in \widetilde{\mathcal{H}} \forall k = 1, 2, \ldots$. So, we have

$$\widetilde{\bigcap}_{k=1}^{\infty} \mathcal{P}_{N_k} = \widetilde{\bigcap}_{k=1}^{\infty} (\mathcal{P}_{M_k} \widetilde{\bigcap} \mathcal{P}_\mathcal{B}) = (\widetilde{\bigcap}_{k=1}^{\infty} \mathcal{P}_{M_k}) \widetilde{\bigcap} \mathcal{P}_\mathcal{B}$$

But
$\widetilde{\mathcal{H}}$is a soft $b - s -$ fieldon$\mathcal{U}$relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\mathcal{P}_{M_k} \in \widetilde{\mathcal{H}} \forall k = 1, 2, \ldots$
Then $\widetilde{\bigcap}_{k=1}^{\infty} \mathcal{P}_{M_k} \in \widetilde{\mathcal{H}}$. So, we have

$$\widetilde{\bigcap}_{k=1}^{\infty} \mathcal{P}_{N_k} \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}.$$

Therefore, $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$ is a soft $b - s -$ field on $\mathcal{U}$relative to $\mathcal{P}_\mathcal{B}$.

Proposition 7:
Suppose $\widetilde{\mathcal{H}}$is a soft $b - s -$ field on $\mathcal{U}$relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and
$\mathcal{P}_C \widetilde{\subset} \mathcal{P}_\mathcal{B} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$ such that $\mathcal{P}_C \in \widetilde{\mathcal{H}}$, then $\mathcal{P}_C \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$.

Proof:
Since$\mathcal{P}_C \widetilde{\subset} \mathcal{P}_\mathcal{B}$, then $\mathcal{P}_C = \mathcal{P}_C \widetilde{\bigcap} \mathcal{P}_\mathcal{B}$, but $\mathcal{P}_C \in \widetilde{\mathcal{H}}$, hence by the definition of $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$ we get $\mathcal{P}_C \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$.

Proposition 8:
Suppose that $\widetilde{\mathcal{H}}$is a soft $b - s -$ fieldon$\mathcal{U}$relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and
$\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$. If $\mathcal{P}_\mathcal{B} \in \widetilde{\mathcal{H}}$, then.
$\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} = \{\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B} : \mathcal{P}_C \in \widetilde{\mathcal{H}}\}$ and $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} \subset \widetilde{\mathcal{H}}$.

Proof:
Assume $\mathcal{P}_N \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$, then $\mathcal{P}_N = \mathcal{P}_M \widetilde{\bigcap} \mathcal{P}_\mathcal{B}$, where $\mathcal{P}_M \in \widetilde{\mathcal{H}}$.
Since $\widetilde{\mathcal{H}}$is a soft $b - s -$ field on $\mathcal{U}$relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\mathcal{P}_M, \mathcal{P}_\mathcal{B} \in \widetilde{\mathcal{H}}$, then $\mathcal{P}_N = \mathcal{P}_M \widetilde{\bigcap} \mathcal{P}_\mathcal{B} \in \widetilde{\mathcal{H}}$, hence $\mathcal{P}_N \in \{\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B} : \mathcal{P}_C \in \widetilde{\mathcal{H}}\}$.
Therefore, $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} \subseteq \{\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B} : \mathcal{P}_C \in \widetilde{\mathcal{H}}\}$.
Let $\mathcal{P}_D \in \{\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B} : \mathcal{P}_C \in \widetilde{\mathcal{H}}\}$. Then $\mathcal{P}_D \widetilde{\subseteq} \mathcal{P}_\mathcal{B}$ and $\mathcal{P}_D \in \widetilde{\mathcal{H}}$.
Hence $\mathcal{P}_D = \mathcal{P}_D \widetilde{\bigcap} \mathcal{P}_\mathcal{B}$, thus $\mathcal{P}_D \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$ because $\mathcal{P}_D \in \widetilde{\mathcal{H}}$.
So, we have $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} \supseteq \{\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B} : \mathcal{P}_C \in \widetilde{\mathcal{H}}\}$.
Therefore, $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} = \{\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B} : \mathcal{P}_C \in \widetilde{\mathcal{H}}\}$.To claim $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} \subset \widetilde{\mathcal{H}}$, assume $\mathcal{P}_C \in \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$, then $\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_\mathcal{B}$ and $\mathcal{P}_C \in \widetilde{\mathcal{H}}$. This complete the claim.

Proposition 9:
If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ and $\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$. Define a class.
$\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})} = \widetilde{\bigcap}\{\widetilde{\mathcal{H}_\alpha}|_{\mathcal{P}_\mathcal{B}} : \widetilde{\mathcal{H}_\alpha}|_{\mathcal{P}_\mathcal{B}}$is a soft $b - s -$field on $\mathcal{P}_\mathcal{B}$ and $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}} \subseteq \widetilde{\mathcal{H}_\alpha}|_{\mathcal{P}_\mathcal{B}} \forall \alpha \in I\}$, then $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ is a smallest soft $\beta - \sigma -$ field on $\mathcal{P}_\mathcal{B}$ that contain $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}}$.

Proof:
Since $\forall\alpha \in I$, $\widetilde{\mathcal{H}}_\alpha|_{\mathcal{P}_\mathcal{B}}$is a soft $b-s-$ field on $\mathcal{P}_\mathcal{B}$, then from the definition of soft $\beta-\sigma-$ field, we can prove that directly $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$.

Assume $\widetilde{\mathcal{H}}_\alpha|_{\mathcal{P}_\mathcal{B}}$is a soft $b-s-$ field on $\mathcal{P}_\mathcal{B}$ and $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}} \subseteq \widetilde{\mathcal{H}}_\alpha|_{\mathcal{P}_\mathcal{B}} \forall\alpha \in I$, then $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}} \subseteq \bigcap_{\alpha\in I}\widetilde{\mathcal{H}}_\alpha|_{\mathcal{P}_\mathcal{B}}$, hence $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$.

Let $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$is a soft $b-s-$ field on $\mathcal{P}_\mathcal{B}$ and $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}} \subseteq \widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}}$. Then $\widetilde{\mathcal{H}}|_{\mathcal{P}_\mathcal{B}} \supseteq \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$.

Therefore, $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ is a smallest soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$ that contain $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}}$.

Proposition 10:
If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\tilde{\mathcal{E}}})$ and $\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B}\widetilde{\subset}\mathcal{P}_{\tilde{\mathcal{E}}}$. Define a class.

$\widetilde{\mathcal{H}} = \{\mathcal{P}_M\widetilde{\subseteq}\mathcal{P}_{\tilde{\mathcal{E}}} : \mathcal{P}_M\widetilde{\bigcap}\mathcal{P}_\mathcal{B} \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}\}$, then $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{U}$ relative to$\mathcal{P}_{\tilde{\mathcal{E}}}$.

Proof.
$\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$.

So, $\mathcal{P}_\Phi, \mathcal{P}_\mathcal{B} \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$.

Since $\mathcal{P}_\Phi = \mathcal{P}_\Phi \widetilde{\bigcap}\mathcal{P}_\mathcal{B}$ and $\mathcal{P}_\mathcal{B} = \mathcal{P}_{\tilde{\mathcal{E}}} \widetilde{\bigcap}\mathcal{P}_\mathcal{B}$, then we get $\mathcal{P}_\Phi, \mathcal{P}_{\tilde{\mathcal{E}}} \in \widetilde{\mathcal{H}}$.

Assume that $\mathcal{P}_{M_1}, \mathcal{P}_{M_2}, \cdots \in \widetilde{\mathcal{H}}$. Then $(\mathcal{P}_{M_i}\widetilde{\bigcap}\mathcal{P}_\mathcal{B}) \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}\ \forall\ i = 1,2,\ldots$

Now, $\widetilde{(\bigcap_{i=1}^{\infty}\mathcal{P}_{M_i})\widetilde{\bigcap}\mathcal{P}_\mathcal{B}} = \widetilde{\bigcap_{i=1}^{\infty}(\mathcal{P}_{M_i}\widetilde{\bigcap}\mathcal{P}_\mathcal{B})}$ and.

$\widetilde{(\bigcup_{i=1}^{\infty}\mathcal{P}_{M_i})\widetilde{\bigcap}\mathcal{P}_\mathcal{B}} = \widetilde{\bigcup_{i=1}^{\infty}(\mathcal{P}_{M_i}\widetilde{\bigcap}\mathcal{P}_\mathcal{B})}$. Since.

$\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$ and $(\mathcal{P}_{M_i}\widetilde{\bigcap}\mathcal{P}_\mathcal{B}) \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}\ \forall\ i = 1,2,\ldots$

Then $\widetilde{\bigcap_{i=1}^{\infty}(\mathcal{P}_{M_i}\widetilde{\bigcap}\mathcal{P}_\mathcal{B})} \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ and $\widetilde{\cup_{i=1}^{\infty}(\mathcal{P}_{M_i}\widetilde{\bigcap}\mathcal{P}_\mathcal{B})} \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$.

Thus $\widetilde{\bigcap_{i=1}^{\infty}\mathcal{P}_{M_i}} \in \widetilde{\mathcal{H}}$ and $\widetilde{\cup_{i=1}^{\infty}\mathcal{P}_{M_i}} \in \widetilde{\mathcal{H}}$.

Therefore, $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\tilde{\mathcal{E}}}$.

Theorem 2:
If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\tilde{\mathcal{E}}})$ and $\mathcal{P}_\Phi \neq \mathcal{P}_\mathcal{B}\widetilde{\subset}\mathcal{P}_{\tilde{\mathcal{E}}}$. Then $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})} = \widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_\mathcal{B}}$.

Proof:
we have $\widetilde{bs(\widetilde{\mathcal{I}})}$ is a soft $\beta-\sigma-$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\tilde{\mathcal{E}}}$. Hence $\widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_\mathcal{B}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$. Assume $\mathcal{P}_N \in \widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}}$. Then $\mathcal{P}_N = \mathcal{P}_M\widetilde{\bigcap}\mathcal{P}_\mathcal{B}$ where $\mathcal{P}_M \in \widetilde{\mathcal{I}}$. But $\widetilde{\mathcal{I}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}$, so we have $\mathcal{P}_M \in \widetilde{bs(\widetilde{\mathcal{I}})}$ and thus $\mathcal{P}_N \in \widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_\mathcal{B}}$.

Hence $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_\mathcal{B}}$. Therefore, $\widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_\mathcal{B}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$ that contains $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}}$. But $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}$ is a smallest is a soft $\beta-\sigma-$ field on $\mathcal{P}_\mathcal{B}$ that contains $\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}}$, which implies that $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_\mathcal{B}}$. Now, if we define a class $\widetilde{\mathcal{H}}$ as:

$\widetilde{\mathcal{H}} = \{\mathcal{P}_M\widetilde{\subseteq}\mathcal{P}_{\tilde{\mathcal{E}}} : \mathcal{P}_M\widetilde{\bigcap}\mathcal{P}_\mathcal{B} \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_\mathcal{B}})}\}$, then.

We have $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

Let $\mathcal{P}_C \in \widetilde{\mathcal{I}}$, then $(\mathcal{P}_C \widetilde{\bigcap} \mathcal{P}_{\mathcal{B}}) \in \widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}}$, but $\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}})}$ implies that $(\mathcal{P}_C \widetilde{\bigcap} \mathcal{P}_{\mathcal{B}}) \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}})}$, hence $\mathcal{P}_C \in \widetilde{\mathcal{H}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}$. Now, if $\mathcal{P}_N \in \widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_{\mathcal{B}}}$, then $\mathcal{P}_N = \mathcal{P}_M \widetilde{\bigcap} \mathcal{P}_{\mathcal{B}}$, where $\mathcal{P}_M \in \widetilde{bs(\widetilde{\mathcal{I}})}$. But $\widetilde{bs(\widetilde{\mathcal{I}})} \subseteq \widetilde{\mathcal{H}}$, then $\mathcal{P}_M \in \widetilde{\mathcal{H}}$, hence $\mathcal{P}_N \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}})}$. Consequentially, $\widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_{\mathcal{B}}} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}})}$. This completes the proof.

Definition 5:
A class $\widetilde{\mathcal{H}}$ is called soft b $-$ field on $\mathcal{U}$ relative to $\mathcal{P}_{\widetilde{\mathcal{E}}}$ for short (soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$) if the following statement are holds:

1- $\mathcal{P}_\Phi \in \widetilde{\mathcal{H}}$.

2- If $\mathcal{P}_{M_1}, \mathcal{P}_{M_2}, \ldots \mathcal{P}_{M_k} \in \widetilde{\mathcal{H}}$,. Then $\widetilde{\bigcap_{i=1}^{k}} \mathcal{P}_{M_i} \in \widetilde{\mathcal{H}}$.

Proposition 11:
Let $\{\widetilde{\mathcal{H}}_\alpha\}_{\alpha \in I}$ be a family of soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$. Then so is $\widetilde{\bigcap_{\alpha \in I}} \widetilde{\mathcal{H}}_\alpha$.

Definition 6:
Assume that $\mathcal{U}$ is a universal set and $\mathcal{E}$ is a set of parameters with respect to $\mathcal{U}$. If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$. Then the soft intersection of all soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$, that contain $\widetilde{\mathcal{I}}$ is called the soft b $-$ field generated by $\widetilde{\mathcal{I}}$ and denoted by $\widetilde{\beta(\widetilde{\mathcal{I}})}$, that is,

$\widetilde{\beta(\widetilde{\mathcal{I}})} = \widetilde{\bigcap}\{\widetilde{\mathcal{H}}_\alpha : \widetilde{\mathcal{H}}_\alpha$ is a soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ and $\widetilde{\mathcal{I}} \subseteq \widetilde{\mathcal{H}}_\alpha \forall \alpha \in I\}$.

Proposition 12:
$\widetilde{\beta(\widetilde{\mathcal{I}})}$ is the smallest soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ that contains $\widetilde{\mathcal{I}}$.

Proposition 13:
Every soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ is a soft b $-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.

Theorem 3:
Assume that $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$, then $\widetilde{\beta(\widetilde{\mathcal{I}})} \subseteq \widetilde{bs(\widetilde{\mathcal{I}})}$.

3 Conclusion

The main goals are obtained are:

1. If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$, then $\widetilde{\mathcal{I}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$ if and only if $\widetilde{\mathcal{I}} = \widetilde{bs(\widetilde{\mathcal{I}})}$.
2. If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ and $\mathcal{P}_C \widetilde{\subseteq} \mathcal{P}_{\widetilde{\mathcal{E}}}$. Then $\left[\widetilde{bs(\widetilde{\mathcal{I}})} \widetilde{\bigcap} \mathcal{P}_C\right] \cup \mathcal{P}_{\widetilde{\mathcal{E}}} = [bs(\widetilde{\widetilde{\mathcal{I}} \widetilde{\bigcap} \mathcal{P}_C})] \cup \mathcal{P}_C$.
3. If $\widetilde{\mathcal{I}}_1, \widetilde{\mathcal{I}}_2 \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ such that $\widetilde{\mathcal{I}}_1 \subset \widetilde{\mathcal{I}}_2$, then $\widetilde{bs(\widetilde{\mathcal{I}}_1)} \subseteq \widetilde{bs(\widetilde{\mathcal{I}}_2)}$.
4. If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ and $\mathcal{P}_\Phi \neq \mathcal{P}_{\mathcal{B}} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$. Define a class $\widetilde{\mathcal{H}} = \{\mathcal{P}_M \widetilde{\subseteq} \mathcal{P}_{\widetilde{\mathcal{E}}} : \mathcal{P}_M \widetilde{\bigcap} \mathcal{P}_{\mathcal{B}} \in \widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}})}\}$, then $\widetilde{\mathcal{H}}$ is a soft $\beta-\sigma-$ field on $\mathcal{P}_{\widetilde{\mathcal{E}}}$.
5. If $\widetilde{\mathcal{I}} \subseteq \widetilde{P}(\mathcal{P}_{\widetilde{\mathcal{E}}})$ and $\mathcal{P}_\Phi \neq \mathcal{P}_{\mathcal{B}} \widetilde{\subset} \mathcal{P}_{\widetilde{\mathcal{E}}}$. Then $\widetilde{bs(\widetilde{\mathcal{I}}|_{\mathcal{P}_{\mathcal{B}}})} = \widetilde{bs(\widetilde{\mathcal{I}})}|_{\mathcal{P}_{\mathcal{B}}}$.

References

1. Ahmed, I.S., Ebrahim, H.H.: On α-field and β-field. J. Phys. Conf. Ser. **1294**(3) (2019). https://doi.org/10.1088/1742-6596/1294/3/032015
2. Ahmed, I.S., Ebrahim, H.H.: On measure relatively to fuzzy σ-algebra. J. Phys. Conf. Ser. **2322**(1) (2022). https://doi.org/10.1088/1742-6596/2322/1/012020
3. Ahmed, I.S., Ebrahim, H.H.: Generalizations of σ-field and new collections of sets noted by δ-field. AIP Conf. Proc. **2096**(20019), 020019-1–020019-6 (2019). https://doi.org/10.1063/1.5097816
4. Khalaf, K.H., Salih, A.M., Abdullah, O.A., Asaad, S.H., Ahmed, I.S.: Study of some properties for pre measure. AIP Conf. Proc. **2834**(1) (2023). https://doi.org/10.1063/5.0162036
5. Çağman, N., Karata, S., Enginoglu, S.: Soft topology. Comput. Math. with Appl. **62**(1), 351–358 (2011). https://doi.org/10.1016/j.camwa.2011.05.016
6. Abbas, H.F., Ebrahim, H.H., Al-Fayadh, A.: Soft P *–field and some of its properties. J. Disc. Math. Sci. Cryptogr. **26**(7), 1875–1882 (2023). https://doi.org/10.47974/JDMSC-1677
7. Molodtsov, D.: Soft set theory—first results. Comput. Math. Appl. **37**, 19–31 (1999)
8. Neog, T.J., Sut, D.K.: Theory of fuzzy soft sets from a new perspective. Int. J. Latest Trends Comput. **2**(3), 439–450 (2011)



IoT and AI Innovations Advancing Sustainability Development Goals (SDGs)

L. Lavanya(✉) and S. MeenaPriyadarshini

Department of Women Studies, Mother Teresa Women's University, Kodaikanal, TamilNadu, India

lavanya.counsellor@gmail.com, drmeenapriyadarshini@gamil.com

Abstract. The Internet of Things, or IoT and Artificial Intelligence (AI) has become a game-changing phenomenon with significant worldwide ramifications for sustainable development. IoT technology has the capacity to link and interact with a wide range of devices, enabling it to deliver real-time information and conclusions which are critical for tracking the SDGs' development. IoT-enabled medical equipment, for instance, may monitor indicators of health, collect information about patients, and provide customized therapies to improve patient outcomes. In impoverished nations with inadequate availability of healthcare services, approach might prove especially helpful. Farmers may maximize crop yields, reduce garbage, and optimize the utilization of resources by implementing smart farming technologies and sensors. Smart energy management is made easier by IoT for both individuals and cities. IoT-enabled smart grids facilitate efficient transmission of electricity by tracking consumption trends and adjusting supply as necessary.

Keywords: Internet of Things (IoT) · Sustainable Development Goals (SDGs) · Healthcare improvement · Environmental conservation · Technological innovation

1 Introduction

Innovation is not exempt from involvement. The speed at how rapidly technology has advanced in recent years has been astounding. It keeps coming up with novel concepts and techniques to handle and utilize data better, interconnects people, and enhances lives. As so, substantial improvement has been made in every industry. The Internet of Things (IoT), which consists of networked objects that communicate with the global web, emerged as an outcome of this quick development and expansion. The next decade will likely see a significant increase in the number of connected devices globally. This is a fantastic chance to use Internet of Things (IoT) technology in support of the 2030 Agenda for the Development of Sustainability. The majority of ongoing IoT initiatives, according to the World Economic Forum, can help achieve the SDGs. They cite IoT Analytics' study of more than 640 IoT deployments. The research found that 75% of proposals support the SDGs for industrial and business reasons. Projects may target a wider range of SDGs if sustainability is incorporated into their layout. The Triple Layered

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 296–309, 2025.
https://doi.org/10.1007/978-3-031-91008-1_28

Business Model Framework can be used to assess a project's good results and its impact on people and the natural world. This paradigm has since added an Environmental Life Cycle Business Model Canvas and a Social Stakeholder Business Model Canvas, building on Alexander Osterwalder's Economic Business Model Canvas.

Smart cities and smart home technologies have generated significant advancements and a great deal of interest. AgTech is an additional sector which is making intelligent contributions. The food we consume comes from agriculture, thus using technologies in this industry helps with regulating pollinators, livestock, crops, and the consumption of water and energy. This lowers utilization of resources and costs while enabling the industry to rely less on pesticides and other diseases and pest control techniques which have been proven for being detrimental to ecosystems and biodiversity. Implementing initiatives in this field helps achieve the Sustainable Development Goals (SDGs) for Hunger, Inequality, Climate Change, and Livelihood Beneath and on Lands. Going ahead, collaborations will play a major role in enabling new solutions since they could fill gaps and support other ones in business-to-business and NGO-to-business contexts.

1.1 Objective

The goal of technological advances in sanitation and drinking water quality was to lower the prevalence of illness and death in areas where people lack access to sufficient sanitary facilities or clean water. The ideals of Generation Z and Millennial differ, yet they both want a work-life balance that allows them to make a positive impact on society. Internet access has always been available to Generation Z, and their interaction with technology is frequently characterized as instinctive. Finding and keeping Millennial and Generation Z workers will be easier for companies that have core environmental and social ideals. The possible economic impact of IoT is estimated to be $11.1 trillion by 2025. Organizations may currently possess approaches, or they might have ideas which employ technological advances which might accelerate the 2030 Sustainable Development Agenda's implementation.

2 Literature Review

The wealth of research on Internet of Things advancements emphasizes how crucial it is to achieving the Sustainable Development Goals (SDGs) by fostering creative thinking in a range of industries. A.Al-fugaha. (2015) claim that IoT technologies have greatly contributed to SDG 3 (which is helpful health and well-being) by revolutionizing healthcare via tailored treatment and virtual patient monitoring [1]. Furthermore, as Akhtair et al. (2020) pointed out, [2] the application of IoT in agriculture has improved water conservation and crop management techniques, in line with SDG 2 (Zero Hunger). Moreover, Giffinger et al. (2007) emphasized how [3] smart city projects made possible by IoT represent sustainable urban planning and resource management techniques that are essential for achieving SDGs 9 (Industries, Innovation, especially and Infrastructures) and 11 (Sustainable development Cities and Communities).The adoption of IoT and deployment are nevertheless impacted by [4] issues that continue to be significant, including cyber security and data privacy Khan et al., (2021). Dian et al. discussed

despite these difficulties, [5] the capability of IoT to maximize the utilization of resources and enhance social well-being highlights its promise to promote sustainable development (Al-Fuqaha et al., 2015). Subsequent investigations have to concentrate on tackling these obstacles while utilizing IoT's revolutionary potential to accomplish the SDGs in its entirety.

3 Innovative Digital Technologies for a Sustainable Future with IoT and SDGs

In order to end poverty, protect the natural world, and provide wealth for all, the United Nations adopted the 17 Sustainable Development Goals (SDGs) in 2015. This is projected that by 2030, these objectives can be accomplished. Increasingly governments and organizations throughout the world increasingly utilized technology, particularly the internet of things (IoT), to assist them achieve these objectives with the aim to accomplish this. Let's examine how IoT might assist in achieving sustainability and achieving the SDGs.

3.1 About Internet of Things

A network made up of connected devices which can speak with one another online is known as the Internet of Things (IoT). These networked gadgets can include devices that laptops, gadgets and smart phones. Researchers can gather data more effectively than ever previously and then utilize it in a variety of innovative ways simply by connecting common objects to the internet. Technology has given people, companies, and governments all sorts of new opportunities.

3.2 How Can IoT Assist in Achieving the SDGs?

IoT can contribute to achieving the SDGs by offering statistical information on the way individuals engage with their surroundings. For instance, real-time monitoring of water or air quality by linked sensors might alert people whenever pollution levels surpass acceptable thresholds or whenever sources have been utilized ineffectively. By doing this, we can create smarter cities which are robust to natural catastrophes and changing climates in addition to making better choices regarding the world around us. Furthermore, by giving underprivileged or rural individuals a source of real-time data and assistance resources whenever they require it the most, IoT solutions including smart residences or interconnected health care facilities can assist enhance their connections to education and healthcare. In addition,, Singh et al. (2023) explicate the IoT technologies possess great promise for tackling global issues including consumption of energy, garbage disposal, extreme poverty, and environmental change—all of those that are directly related to achieving the Sustainable Development Goals by 2030 [6]. A significant advance toward eradicating hunger worldwide would be precision agriculture, which is fueled by IoT technology like autonomous tractors and soil surveillance sensors. Precision farming has the potential to increase crop yields whilst substantially reducing food wastage. In a comparable way, intelligent grid integration with solar energy tracking devices might

improve energy efficiency while lowering emission levels, which is essential for lessening the adverse impacts of global warming on the health of our planet. IoT technologies have tremendous promise for aiding promote sustainability; but, if they are to be effective in assisting us in achieving the SDGs by 2030, they must be carefully planned and implemented across numerous sectors. To fully utilize this kind of technology and build a future that is sustainable for all of us, governments worldwide must devote additional resources to building strong infrastructure that facilitates interconnection between various devices.

By working together, stakeholders from NGOs, private businesses, and public sector organizations may successfully use IoT technologies to achieve our shared objectives for a sustainable future. All nations are urged to take actions in support of the Sustainable Development Goals (SDGs) in order to advance development and safeguard the environment. In addition to addressing Obasi et al. (2024) discussed the climate change and environmental protection, methods for addressing inequality must additionally concentrate on addressing social protection, job prospects, education, healthcare, and safety for everyone [12]. In order to end impoverished circumstances, these programs must cooperate. Gives priority to environmentally friendly with the goal to maximize the Internet of Things' ability to benefit the environment. Especially considering that the Sustainable Development Goals of the UN include the three aspects of safeguarding the environment, social integration, and economic development. Internet of Things (IoT) technology is currently helping businesses become more competitive and improving the quality of life for citizens. Amongst the justifications for IoT technology investment, we find:

- Reduction of production expenses
- Improved quality of the product;
- Improved sustainability and utilization of natural resources
- Adherence to regulations

SDGs represent the goals that have been successfully accomplished as a result of the various initiatives that have emerged in recent years. And, as shown in Fig. 1, outlines in a study exactly IoT technology supports the SDGs as well as which initiatives are being implemented globally in accordance with each goal.

3.3 IoT's Role in Reaching SDGs

The Internet of Things (IoT) represents a useful tool for achieving the Sustainable Development Goals (SDGs). The ability of Internet of Things (IoT) technology to connect and communicate with a variety of devices allows it to provide real-time data and insights which are essential for monitoring the progress of the SDGs. IoT-enabled medical equipment, for instance, may remotely observe vital signs, collect patient data, and provide individualized treatment plans to improve patient outcomes. Elango elakkiya et al. (2024) discussed in impoverished nations with inadequate utilization of healthcare services, approach can be especially helpful [7]. Farmers may maximize crop yields, reduce waste, and improve the utilization of resources by implementing smart farming methods and sensors. For example, sensors that are buried underneath the ground can give farmers data regarding the moistness of the soil, a data they may utilize to schedule agricultural



Fig. 1. IoT technology supports the SDGs as well as which initiatives are being implemented globally in accordance with each goal

irrigations more efficiently and preserve water. Smart handling of energy is made easier by IoT for both individuals and cities. IoT-enabled smart grids facilitate effective distribution of electricity by tracking consumption trends and adjusting supply as necessary. Additionally, connected appliances let consumers manage their energy usage from a distance using real-time data from smart meters. These developments open the door for lower greenhouse gas emissions in addition to helping to achieve SDG 7 (Affordable Clean Energy).

3.4 How Gender Equality (SDG 5) May Be Advanced Through Technology?

IoT can provide clever answers to practical issues faced by women by obfuscating the distinctions both actual and virtual spaces. The argument which "development, technological advances, and business are engines for achieving gender equality and women's emancipation" was actually made in a 2017 report released by the UN. In addition to being a basic human right, gender equality is also a precondition for a globe that is affluent, peaceful, and ecological. During the past few decades, there have been advancements growths: more girls are attending high school, fewer are compelled into young marriages, more women are holding key roles in the legislature, and regulations have been amended to promote gender equality. Even with these improvements, there are still a lot of obstacles to overcome: regulations and social conventions that discriminate against women still exist, women remain insufficiently represented in political leadership roles, and 1 in 5 women and girls among between the ages of 15 and 49 report having been physically or sexually abused by an intimate partner in the previous year.

All over they live, women and girls deserve the same privileges. In addition to making up 70% of those working in social and health care sectors during the epidemic, women perform unpaid household tasks and care giving 3 times more frequently than males. Gender equality is improving as more women hold managerial positions and fewer girls are being coerced into young marriage (a 15% decrease). Nevertheless, women only occupy 25% of leadership positions in the national parliament and 36% in municipal administration. Having a mobile phone is empowering for many women. Nonetheless, in 66 nations, women's cell phone ownership remained 8.5% less than men's in comparable regions. If immediate effort is made to eradicate the numerous underlying causes of discrimination that continue to restrict women's rights in both public and private domains, gender equality can be attained by 2030.

The objectives are to:

- Take out every kind of violence against women and girls in both public and private settings, notably trafficking in people and various forms of sexual as well as other kinds of victimization;
- Put a stop to all kinds of prejudice against women and girls worldwide.

3.5 Why at This Time?

A vital component of all aspects of sustainable and equitable growth, women's rights and freedoms are one of the 17 Sustainable Development Goals. All of the SDGs are contingent upon the accomplishment of Goal 5.

3.6 What Benefits Might Technology Offer?

The mobile phone business helps achieve SDG 5 by boosting women's exposure to and utilization of mobile and internet technologies to improve their lives and by expanding their involvement and leadership in the sector. Some of the most promising technological applications are:

- AI-enabled remote employment platforms targeted at women;
- unbiased choosing that promote equality

3.7 IoT and AI Collaboration for SDGs

The synergies between artificial intelligence (AI) and the Internet of Things (IoT) hold considerable potential for assisting in the achievement of the Sustainable Development Goals (SDGs). These advancements are able to address a number of social, economic, and environmental issues by means of intelligent algorithms and networked devices. For instance, in the healthcare sector, IoT devices with email campaign software backing can gather patient data in real-time and send it via an AI-powered system for analysis, which then generates suggestions for individualized therapy. This lowers healthcare expenses while simultaneously improving medical outcomes and patient care. Peng et al. (2021) maximizing the utilization of resources, IoT and AI may additionally greatly contribute to reducing environmental effect. Smart sensors can collect information on waste management, water use, and consumption of energy when they are integrated into infrastructure systems like buildings or towns [16]. After that, this data may be examined using AI algorithms to find trends, find inefficiencies, and suggest ways for optimization. Regona et al. (2024) and Sharifi et al. (2024) enlighten about the Societies can reduce their carbon footprint and establish more sustainable resource consumption patterns by automating operations based on these findings [8, 9].

3.7.1 IoT and AI Technology Risks and Challenges

Although IoT and AI can significantly improve sustainability, it is important to weigh the risks and difficulties involved in order to provide a fair assessment Peng et al. (2022) we examine important topics including data privacy, the influence on the environment, and the possibility of biased AI systems [15]. We also include case studies wherein these technologies have encountered major problems as shown in Table 1.

Table 1. Case-Study Table

Topics	Concerns	Case studies	Potential Solutions
Data privacy	**Sensitive Data:** Internet of Things (IoT) devices frequently gather comprehensive environmental and personal data, which raises questions about how this data may be misused or accessed without authorization **Data breaches:** Sensitive information may be exposed as a result of the massive volumes of data that are gathered, making them attractive targets for hackers	**Smart Home Devices** [17, 18]: Events like the Ring data breach in 2019—a business that makes IoT security cameras—exposed user information and brought attention to weaknesses in home security systems. Attackers were able to obtain users' personal information and live camera feeds by taking advantage of these weaknesses	**Enhanced Security Protocols:** To safeguard data, use strong encryption, authentication, and frequent security upgrades **Minimize Data:** To lower privacy concerns, just gather the information that is required and anonymize it

(*continued*)

Table 1. (*continued*)

Topics	Concerns	Case studies	Potential Solutions
Environmental Impact	**Electronic trash:** If electronic trash is not adequately managed, it might pose environmental dangers. This problem is exacerbated by the IoT devices' rapid growth **Energy Consumption**: AI and Internet of Things systems, especially those that need to analyze large volumes of data, can use a lot of energy, which raises carbon emissions	**Data Centers Energy** [19, 20]**:** Due to their significant carbon footprint, big data centers' energy requirements, which enable cloud-based AI computing, have drawn criticism. For instance, data centers in the United States alone used over 2% of the country's power, primarily from non-renewable sources	**Effective Algorithms**: Create AI systems with performance and energy consumption optimized to lessen their negative effects on the environment
Risk of Biased AI Systems	**Data Bias:** The objectivity of AI systems depends on the quality of the training set. Results that are unjust or discriminating may result from biases in training data **Lack of Transparency:** A lot of AI algorithms are "black boxes," which make it challenging to comprehend the decision-making process and aggravate bias and fairness concerns	**Biased AI Systems** [21, 22]**:** Research has indicated that certain facial recognition systems display biases related to race and gender. For example, an MIT research from 2018 revealed that commercial face recognition algorithms misidentified people with darker complexion more frequently than people with lighter skin, raising questions about its accuracy and fairness	Establish strategies for detecting and fixing biases in AI training data as part of bias mitigation. Make sure the data sets used are representative and varied **Accountability and Transparency:** Provide frameworks for elucidating AI decision-making procedures and assigning blame for skewed results

3.8 Detailed Analysis of IoT and AI Integration for Advancing Sustainability Development Goals (SDGs)

A number of Sustainability Development Goals (SDGs) must be advanced through the use of artificial intelligence (AI) and Internet of Things (IoT) technology into current systems. Massimo et al. (2024), in order to accomplish this integration, a number of technological issues must be resolved, such as real-time data processing, network scalability, and data interoperability [13]. Peng et al. (2023) report offers a thorough look at these difficulties, highlights effective integrations, and makes recommendations for possible fixes [14].

Data Interoperability

- **Issues:** The capacity for disparate systems and institutions to collaborate easily via the sharing and use of data is known as data interoperability. Because there are many different types and sources of data produced by sensors, devices, and applications, data interoperability is essential in IoT and AI systems.
- **Various Data Formats:** JSON, XML, and proprietary formats are just a few of the varied data types that IoT devices generate. These must frequently be converted and

normalized, which can be difficult and error-prone processes, in order to be integrated with AI systems.
- **Protocol incompatibilities:** Combining data streams for AI analysis might be difficult as various IoT devices may employ disparate communication protocols (such as MQTT, CoAP, and HTTP).

Examples of Successful Integration

- **Smart Agriculture:** Climate Corp and other firms collect data from various sensors (such as weather observatories and moisture in the soil sensors) and standardize it via their online services for precision farming. Thanks to this connection, AI models may now offer practical tips such as the best times to water plants.
- **Smart Cities:** Using free data standards and APIs, smart city systems in places like Barcelona combine data from several sources (such as environmental sensors and traffic cameras). Applications powered by AI, such as pollution monitoring and traffic control, are supported by this integration.
- **Possible Remedies:** standardized formats for data To guarantee interoperability, use industry-standard data formats and standards like JSON or XML Schema. Interoperability can be facilitated by projects such as the Open Data Protocol (OData).
- **Unified Data Platforms:** Put in place middleware programs that can combine and standardize data from many sources. Platforms for data integration are among the examples.

Network Scalability

- **Issues:** The potential of a network to accommodate an expanding number of Internet of Things devices and the associated data traffic is known as network scalability. Ensuring effective and dependable communication becomes more difficult as IoT deployments expand.
- **High Device Density:** Thousands of IoT devices may be present in huge agricultural areas or urban settings. Scalable network solutions are needed to manage interaction among those devices and the centralized system.
- **Limitations on Bandwidth:** As IoT devices create more and more data, network bandwidth may be strained, perhaps resulting in bottlenecks and decreased performance.

Examples of Successful Integration

- **Smart Grid Technology:** Internet of Things (IoT) sensors are utilized to track and regulate electrical grids in smart grids, including those developed by Siemens. To guarantee scalability and dependability, these systems make use of cutting-edge network technologies like 5G and Low Power Wide Area Networks (LPWAN).

- **Agricultural Internet of Things Networks:** LPWANs are used by initiatives such as IBM's Watson Decision Platform for Agriculture to connect several sensors over long distances. This network method is scalable and allows for large-scale data transmission and collecting.
- **Possible Remedies:** Sophisticated network architectures Make use of scalable network technologies like LPWAN for low-power, long-range connection or 5G for high bandwidth and low latency.
- **Edge Computing:** Utilize edge computing to handle data locally, cutting down on latency and the quantity of data sent over the network.

Real-Time Data Processing

- **Issues:** Evaluating and reacting to data as it is created is a need of real-time data processing. Applications that need to respond right away, such as emergency response systems or traffic control, depend on this.
- **High-Speed Data Streams:** In order for AI systems to evaluate data in real time and deliver insights or choices in a timely manner, IoT devices must continually create data.
- **Computer Demands:** In order to assure prompt and correct analysis, processing massive amounts of real-time data demands a significant amount of computer power and effective algorithms.

Examples of Successful Integration

- **Traffic Management Systems:** To proactively regulate traffic flow, cities such as San Francisco employ immediate information from cameras and traffic sensors. This data is analyzed by AI systems to improve traffic patterns and change traffic signals.
- **Smart Water Management:** To track the integrity of water and identify leaks, immediate information from water sensors is analyzed in cities like Singapore. AI models anticipate possible problems and notify operators in a timely manner.
- **Possible Remedies: Frameworks for Stream Processing:** Use tools for stream processing, such as Apache Kafka, Apache Flink, or Apache Storm, that have been optimized for effectively managing and evaluating real-time data streams.
- **High-Performance Computing:** To manage demanding data processing operations, leverage cloud-based solutions featuring scalable computing resources. Processing power is available on order through platforms like Google Cloud Functions and AWS Lambda.

3.9 Case Studies: Effective IoT and AI Integration for SDGs

The accomplishment of the Sustainable Development Goals (SDGs) can be significantly aided by the successful implementation of AI and IoT, as demonstrated by case studies. Using IoT and AI in agriculture to address issues with nutrition is one example of this kind of study. Farmers can obtain valuable insights on variations in the weather, temperatures,

and levels of soil moisture by utilizing real-time data from sensors positioned in fields. Elango Elakkiya et al. (2024) explains to makes it possible to schedule irrigation, control pests, and produce crops more efficiently, Zeng et al. (2024)discusses to raises yields and has a smaller negative impact on the environment [10, 11]. In order to enable attempts at early intervention, AI systems can also examine this data and anticipate diseases or nutritional shortages. Real-time data could be gathered on a variety of topics, including traffic flow, garbage disposal, consumption of energy, pollution levels, and additionally, using sensors and networked devices incorporated throughout an urban infrastructure. Strategies for decision-making targeted at lowering carbon emissions and encouraging sustainable community behaviors are informed by this information.

For example, cities might lessen traffic and enhance air quality by utilizing artificial intelligence algorithms for route optimization in conjunction using the analysis of transportation patterns obtained from IoT-enabled automobiles. These case studies show how the effective fusion of AI and IoT may significantly advance SDGs in a number of industries. Organizations can use technology to gather data in real-time and use sophisticated algorithms for evaluation and decision-making processes. This allows them to make well-informed decisions that support global efforts towards sustainable development. In addition to increasing productivity, the integration of IoT and AI provides cutting-edge solutions that are crucial.

3.10 Market Size and Growth Forecasts

India's IoT and AI industry is projected to expand at a rapid pace due to a number of factors, including growing initiatives from the government, a thriving entrepreneurial ecosystem, and increased digitalization. Based on the findings of a research study, the Internet of Things (IoT) market in India is anticipated to grow at a compound annual growth rate (CAGR) of more than 25% and reach USD 15 billion by 2025. In the same way, the artificial intelligence market in India is growing rapidly due to advances in technology, more investment, and an increasing demand for solutions that leverage AI. At a compound annual growth rate (CAGR) of more than 45%, the AI industry in India is predicted to reach USD 7 billion by 2025, including industries like manufacturing, medical services, the retail sector, and financial as shown in Fig. 2.

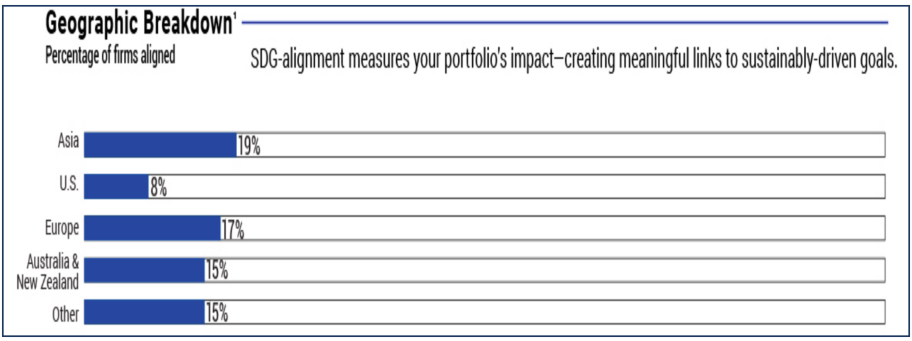


Fig. 2. Geographic breakdown of sustainably driven goals

3.10.1 Essential Growth Drivers

The following are some of the elements driving the rise of AI and IoT in India:

- **Government Initiatives:** Programs like the Smart Cities Mission, Made in India, and Digital India are creating an environment that is favorable to the widespread use of AI and IoT. To promote invention and scale implementation, government-sponsored programs and benefits are fostering cooperation between business, academia, and research centers.
- **The Rise of Startups Advancement in IoT and AI**: It is being propelled by India's thriving startup scene. In order to provide unique solutions that tackle certain industry concerns, startups are utilizing emerging technology. The rise of creative businesses in this industry is further fueled by the accessibility of venture capital financing and incubator support.
- Industry 4.0 Adoption: In order to improve efficiency, streamline processes, and provide positive business results, businesses are adopting Industry 4.0 concepts, combining IoT, **AI, and data analytics:** Industry 4.0 projects are changing conventional business structures and value chains in a variety of ways, from smart production to interconnected supply chains.
- **Growing Customer Demand:** The need for IoT-enabled devices and AI-powered services is increasing primarily a result of the growing middle class and improving levels of digital literacy. Smart homes, wearable technology, and customized digital experiences are what are encouraging customers to adopt IoT and AI technologies.

4 In Conclusion: Leveraging Technology's Potential for a Sustainable Future

In summary, there is no denying the capacity of modern technology to create a sustainable future. We may achieve a great deal in terms of achieving the Sustainable Development Goals (SDGs) by leveraging IoT and AI. Innovative technologies like this provide creative answers to major global issues including destitution, resource scarcity, and environmental degradation. With the help of IoT, we can now link more than ever before and gather data in real time from a variety of sources. Utilizing this data helps improve decision-making procedures, lessen the negative effects on the environment, and maximize the distribution of resources and productivity. We may create better sustainable cities and communities by incorporating IoT throughout our infrastructure systems, including interconnected transit systems that lessen traffic to smart electrical grids which streamline consumption of energy. Large volumes of data can be processed swiftly by artificial intelligence, which can also find concealed trends or ideas that conventional researchers would miss. This allows for more intelligent resource management in industries such as handling water, medical treatment, and the agricultural sector.

Utilizing precision irrigation techniques, farmers may reduce water usage and enhance crop yields with the aid of AI-powered algorithms. AI-enabled surveillance solutions in the healthcare industry can reduce hospitalizations and transportation-related carbon emissions while simultaneously enhancing patient care. By enabling individuals

via information-sharing websites or crowd sourced campaigns for sustainable development initiatives, a technology offers chances for group action. For instance, IoT-enabled citizen science initiatives promote public involvement in ecological monitoring programs, which generate important data for scientific objectives. Through identification and resolution of these intricacies and inadvertent outcomes, we can more effectively leverage the advantages of IoT and AI while reducing any hazards. By taking a balanced approach, we can make sure that technical innovations support sustainable growth without making already-existing problems worse.

References

1. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M.: Internet of Things: a survey on enabling technologies, protocols, and applications. IEEE Commun. Surv. Tutor. **17**(4), 2347–2376 (2015). https://doi.org/10.1109/COMST.2015.2444095
2. Akhtar, N.: IoT Security and privacy concern: A Systematic Mapping Study. International Journal of Hyperconnectivity and the Internet of Things. 1. 19 (2020). https://www.researchgate.net/publication/345897402_IoT_Security_and_privacy_concern_A_Systematic_Mapping_Study
3. Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Milanović, N., Meijers, E.: Smart cities - Ranking of European medium-sized cities (2007). https://www.researchgate.net/publication/261367640_Smart_cities_-_Ranking_of_European_medium-sized_cities
4. Khan, Z., et al.: Internet of Things-based smart farming monitoring system for bolting reduction in onion farms. Sci. Program. (2021). https://doi.org/10.1155/2021/7101983
5. Dian, F., Vahidnia, R., Rahmati, A.: Wearables and the Internet of Things (IoT), applications, opportunities, and challenges: a survey. IEEE Access **8**, 1 (2020). https://doi.org/10.1109/ACCESS.2020.2986329
6. Singh, A., Kanaujia, A., Singh, V., Vinuesa, R.: Artificial intelligence for sustainable development goals: bibliometric patterns and concept evolution trajectories. Sustain. Dev. (2023). https://doi.org/10.1002/sd.2706
7. Elango, E., Hanees, A., Shanmuganathan, B., Basha, M.: Precision Agriculture: A Novel Approach on AI-Driven Farming (2024). https://doi.org/10.1007/978-3-031-51195-0_7
8. Regona, M., Yigitcanlar, T., Hon, C., Teo, M.: Artificial intelligence and sustainable development goals: systematic literature review of the construction industry. Sustain. Cities Soc. (2024). https://doi.org/10.1016/j.scs.2024.105499
9. Sharifi, A., Allam, Z., Khavarian-Garmsir, A.R.: Smart cities and sustainable development goals (SDGs): a systematic literature review of co-benefits and trade-offs. Cities **146**, 104659 (2024). https://doi.org/10.1016/j.cities.2023.104659
10. Elango, E., Natarajan, G., Sundaravadivazhagan, B., Sandhya, S.: Role of Artificial Intelligence in Industry 4.0: Applications and Challenges. CRC Press, Boca Raton (2024). https://doi.org/10.1201/9781003395416-3
11. Zeng, F., Pang, C., Tang, H.: Sensors on Internet of Things systems for the sustainable development of smart cities: a systematic literature review. Sensors **24**(7), 2074 (2024). https://doi.org/10.3390/s24072074
12. Obasi, S.C., Solomon, N.O., Adenekan, O.A., Simpa, P.: Cybersecurity's role in environmental protection and sustainable development: bridging technology and sustainability goals. Comput. Sci. IT Res. J. **5**(5), 1145–1177 (2024). https://doi.org/10.3390/s24072074
13. Regona, M., Yigitcanlar, T., Hon, C., Teo, M.: Artificial intelligence and sustainable development goals: systematic literature review of the construction industry. Sustain. Cities Soc. **108**, 105499 (2024). https://doi.org/10.1016/j.scs.2024.105499

14. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Nature Singapore (2023)
15. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent. Springer Nature Singapore (2022)
16. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer Singapore (2021)
17. Pătru, I.-I., Carabaş, M., Bărbulescu, M., Gheorghe, L.: Smart home IoT system. In: 2016 15th RoEduNet Conference: Networking in Education and Research, Bucharest, Romania, pp. 1–6 (2016). https://doi.org/10.1109/RoEduNet.2016.7753232
18. Rock, L.Y., Tajudeen, F.P., Chung, Y.W.: Usage and impact of the internet-of-things-based smart home technology: a quality-of-life perspective. Univ. Access Inf. Soc. **23**, 345–364 (2024). https://doi.org/10.1007/s10209-022-00937-0
19. Zhu, H., et al.: Future data center energy-conservation and emission-reduction technologies in the context of smart and low-carbon city construction. Sustain. Cities Soc. **89**, 104322 (2023). https://doi.org/10.1016/j.scs.2022.104322
20. Ahmed, K.M.U., Bollen, M.H.J., Alvarez, M.: A review of data centers energy consumption and reliability modeling. IEEE Access **9**, 152536–152563 (2021). https://doi.org/10.1109/ACCESS.2021.3125092
21. Ferrara, E.: Fairness and bias in artificial intelligence: a brief survey of sources, impacts, and mitigation strategies. Sci **6**, 3 (2024). https://doi.org/10.3390/sci6010003
22. Jain, L.R., Menon, V.: AI algorithmic bias: understanding its causes, ethical and social implications. In: 2023 IEEE 35th International Conference on Tools with Artificial Intelligence (ICTAI), Atlanta, GA, USA, 2023, pp. 460–467. https://doi.org/10.1109/ICTAI59109.2023.00073



The Role and Impact of Ethical Hacking in Modern Society's Economy

Nadiah Arsat[1(✉)], Habib Idriss Daoud[1], Zurinahni Zainol[1], and Gaurav Kumar[2,3]

[1] School of Computing and Informatics, Albukhary International University, Alor Setar, Kedah, Malaysia
{nadiah.arsat,zurinahni.zainol}@aiu.edu.my,
habib.daoud@student.aiu.edu.my

[2] University Centre of Research and Development, Chandigarh University, Mohali 140413, India

[3] Division of Research and Development, Lovely Professional University, Phagwara 144411, India

Abstract. This research paper examines the crucial importance of ethical hacking, also known as penetration testing, in safeguarding modern society's economic growth and stability. It will begin by providing a clear explanation of ethical hacking, delving into its core principle and the different types of ethical hacking methods employed. Then, it will explore the potential factors that are driving the significant rise in cybercrime, highlighting the increasing need for ethical hacking practices. This paper emphasizes how ethical hacking acts as a vital tool in our society to protect sensitive information and critical systems, mainly contributing to enhancing a more secure and stable economic environment. It illustrates the damage that cybercrime may have on society, including financial harm, the loss of essential systems, and a loss of trustworthiness. Networks and computer systems are the keys to our digital world and include our financial details, personal data, and control mechanisms for society's safety; criminals often target these platforms.

Keywords: Ethical Hacking · Society · Cybercriminal · Security · Organization · System

1 Introduction

In today's digitally interconnected world, the internet serves as vita communication, facilitating the transfer of information between individuals. However, this connectivity also exposes individuals to many online threats, particularly hacking, which can significantly harm modern society, which is dependent on the internet and electronic devices to connect and access information and execute operations through the network. According to [1] hacking is defined as unauthorized access to computer security or data. It is often done through techniques. Hackers damage many organizations' businesses as they highlight the financial burden, with average incident costs exceeding €857,000 and demonstrating a concerning upward trend in recent years. Ethical hacking is an active

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 310–326, 2025.
https://doi.org/10.1007/978-3-031-91008-1_29

strategy not only for individuals and organizations against cyber threats but also aids in maintaining the integrity and security of digital systems. Consider it as a crucial mechanism against malicious activities in the digital space. Also known as penetration testing or white-hat hacking, ethical hacking involves using hacking techniques to identify vulnerabilities in systems and networks with the goal of enhancing their security. This research paper will explore ethical hacking, its roles, phases, and impact on different sectors of the economy. Ethical hacking, a legal form of hacking, is essential for understanding cybercrimes and their impact on society's economy. As technology advances, this also applies to the techniques used by both ethical hackers and malicious actors. Therefore, staying updated on the latest developments in ethical hacking and its applications in securing digital assets is crucial. Methods exploited by criminal hackers and generating effective countermeasures against them. The paper begins by providing an overview of ethical hacking, including its definitions and key protocols, before delving into its classifications and discussing the reasons behind an increase in cybercrimes and their impact on society's economy. As technology advances, this also applies to the techniques used by both ethical hackers and malicious actors. Therefore, staying updated on the latest developments in ethical hacking and its applications in securing digital assets is crucial.

Background

In 2019, around 15 billion data records were compromised, making attacks on customer personal information the foremost challenge for e-commerce [2]. It is crucial for both customer and e-commerce organizations to recognize the risk and financial implications of data breaches. In today's data age, information is an invaluable asset. Organizations rely on information to formulate strategies, develop products and services, and make investment decisions. Sharing information necessitates substantial trust between parties, highlighting the importance of strong data protection measures.[3] also known as white hat hacking or penetration testing, involves authorized attempts to breach a system's defenses to detect and resolve security vulnerabilities. Against criminal hackers (black-hat hackers), ethical hackers operate with permission and aim to improve security rather than exploit weaknesses. The practice has become increasingly vital as cyber-attacks grow more common and advanced, targeting virtual components, organizations, and personal data [4]. Ethical hacking helps organizations stay alert of potential threats by evaluating real-world attacks and providing practical guidance for improving definitions. The role of ethical hacking in modern society economies is crucial for protecting sensitive data, ensuring safety, maintaining trust in digital systems in modern connected societies, keeping economic stability, and establishing a secure digital environment.

Problem Statement

In the linked digital world of today, the continual growth of cyber threats stands as a significant challenge to the security of critical information and infrastructure across various sectors of the economy. Despite the increasing implementation of cybersecurity measures, organizations continue to struggle with the evolving modern methods of malicious actors, leading to breaches, data theft, and financial losses. This emphasizes the pressing need for effective strategies to safeguard digital assets and mitigate cyber risks in an active way. While ethical hacking, also known as penetration testing, has appeared. As a creative approach to identifying and addressing security vulnerabilities,

there exists a gap in understanding its efficacy and impact across different sectors of the economy. Although ethical hacking offers a structured methodology for simulating real-world cyber-attacks and analyzing the security of systems and networks, its adoption and integration vary widely among industries. Moreover, the intangibles of ethical hacking practices and their suitability with sector-specific requirements remain relatively unexplored. This research aims to decrease the gap in knowledge by comprehensively examining the roles of ethical hacking within various sectors of the economy in modern society. By discovering the challenge of ethical hacking practices, including its methodologies, and tools, this study seeks to outline the effectiveness of ethical hacking in enhancing cybersecurity. Furthermore, by identifying key challenges and opportunities associated with ethical hacking implementation, this research conducts operations to provide actionable insights for organizations to strengthen their defined mechanisms and mitigate the risks generated by cyber threats.

- How does ethical hacking contribute to enhancing cybersecurity measures in financial institutions, and what are its effects on preventing financial fraud and data breaches?
- What are the specific challenges and benefits of implementing ethical hacking practices in modern society, and how do these practices impact various financial data security and compliance with regulatory standards?
- How does the effectiveness of ethical hacking practices evaluate diverse economic sectors, find vulnerabilities, organizational size, budget limitations, and returns on mitigating cyber threats and protecting digital assets?
- To investigate the diversity in the implementation of ethical hacking techniques across sectors of the economy and identify the factors driving this change.
- To analyze the specific roles, phases, and importance of ethical hacking practice and assess the contribution to improving cybersecurity stability in the digital world.
- To evaluate the impact of ethical hacking on mitigating cyber threats and protecting digital assets across the various sectors of modern society's economy, focus on understanding how to estimate the effectiveness of ethical hacking efforts in addressing their cyber security needs.

Scope of Study

This research paper will study the implementation of ethical hacking around cybersecurity in multiple economic sectors and will dive into a full analysis of ethical hacking practices and why these frameworks, tools, and results are needed and important for online transactions such as finance, e-commerce, and will explore various phase of ethical hacking, it will investigate the ethical considerate sounding ethical hacking. Furthermore, the scope of the study will extend to identifying the challenges and opportunities associated with the adoption of ethical hacking practices within organizations. This will include, for instance, resource constraints and gaps and exploring the potential benefits of applying ethical hacking into current safety measures to improve system security against cyber attackers. While the focus will be on ovulating the efficacy of ethical hacking, exploring the impact of cybersecurity breaches and the role of ethical hacking in safeguarding digital assets, and maintaining trust in the digital ecosystem, the research will seek to provide recommendations for modern society to optimize their ethical hacking strategies and effectively benefit from ethical hacking as a creative defines mechanism.

2 Literature Review

This section highlights research on the ethical hacker's function and impact in the economy of m in modern society's economy, examines how ethical hacking applies to various sectors of the economy, its advantages and challenges, and its impact on economic stability and growth. Ethical hacking is crucial for identifying vulnerabilities that malicious hackers could exploit and, as a result, prevents significant losses. The studies elaborate that ethical hacking helps protect businesses from data breaches and cyber-attacks [5]. These authors explain eight particular performance requirements of a virtual machine using quantity analysis, which may be addressed during the execution period in the Dedicated Online Education System. It can help raise awareness of virtual machine password vulnerabilities and avoid them [6]. Most companies store their data digitally, making it vulnerable to cyberattacks. Ethical hackers can access sensitive employee information and attack company servers using various viruses. External and internal test storages have been discussed according to external test simulates attacks on an organization's network from the internal, starting with publicly available information and targeting external visible serves or devices such as DNS, email serves, web servers, and firewalls [7]. On the other hand, threat focuses on the risk of a breached network perimeter or the actions of authorized users. Both methods use similar techniques. Companies must improve operating system security by identifying and fixing vulnerabilities to prevent this. While hacking poses significant risks, businesses have developed several methods to deter attacks and protect their data. Companies have improved operating system security by identifying and fixing vulnerabilities to prevent this. While hacking poses significant risks, businesses have developed several methods to deter attacks [8]. Ethical hacking plays a vital role in maintaining the integrity of financial systems and safeguarding sensitive information. According to the strategies used by individuals commonly known as hackers, crackers, intruders, or attackers who seek unauthorized access to networks and systems.[1] Motivations for hacking vary; some do it for personal fulfillment, others for financial gain, and many to destroy operations or gain a reputation. Despite these differences, all hackers share a common goal: identifying and exploiting system vulnerabilities. For instance, a local network test simulates an internal threat from an authorized person, targeting defines like intranet firewalls and server security measures. Another method, the stolen laptop computer test, involves ethical hackers examining a key employee's laptop for stored passwords and sensitive information, which often enables them to access the business website or database using the owner's identity. Ethical hacking, also referred to as "Penetration Hacking," "Intrusion Testing," or "Red Teaming," is the procedure of hacking without damaging intent. Malicious hackers and ethical hackers use similar tools and techniques to identify security vulnerabilities but do not harm systems or steal data. Instead, they evaluate the security of the intended systems. As well as presenting their result to the owners, making recommendations for correction. According to [9], the stock value of publicly traded businesses usually decreases by 7.5% after a data breach. A ransomware attack on ION trading technology in 2023 caused financial institutions to physically conform trades, resulting in huge financial loss and stock decrease, and 5.4 billion businesses lost money [10]. Hacking is a significant threat to businesses, which often suffers the most severe consequences. Companies are primary targets for hackers seeking customers' personal and financial

data, and each year, businesses lose billions of dollars due to hacking and other cyber breaches. To prevent such costly incidents, businesses and customers are investing in ethical hacking, essential to handling significant amounts of personal and financial data loss. (Sankardas et al., 2020) divided the hack into three main types: White hat hacker, Black hat hacker, and grey hat hacker. While [11] divided into seven main types.

2.1 Type of Hacking

(1) **White Hat Hacker**

White hat hackers are considered the good guys in the cyber world. They get permission from organizations or individuals to test computer systems for weaknesses. Their goal is to find and fix security holes before bad actors can exploit them. These ethical hackers work for cybersecurity companies and are known for their honesty and integrity. They're called "white hats" because they symbolize the good guys in old Western movies.

(2) **Black Hat Hacker**

Are criminals of the world of online communication? They break into computer systems without permission, usually for personal gain or to cause harm. These are the people behind cyber-attacks and data breaches. Opposite to white hats, black hats operate in secrecy and don't care about the rules or ethics. They use their knowledge to steal information, disrupt services, or damage systems.

(3) **Grey Hat Hacker**

Its somewhere in between white hats and black hats. They might break into systems without permission, but not necessarily for malicious reasons. Instead, they might do it to show the weaknesses in a system and help fix them. Grey hats are a bit of a wild card - they're not strictly good or bad, but they often walk a fine line between legality and illegality.

(4) **Red Hat Hacker**

It's a mix of black hat and white hat hackers. Usually focuses on the degree to which government agencies, top-security information centers, and other vital data or information sources have been compromised.

(5) **Blue Hat Hacker**

An individual who's test system before is deployed and has no connection with the computer security consulate companies their goal is to close any gaps in the system that allow them to have an impact.

(6) **Elite Hacker**

Elite hackers are considered the most skilled within the hacker community. Often discover and share new exploits. These hacker processes advance technical abilities and typically are on the path of identifying vulnerabilities in systems and networks. Elite hackers are considered the most skilled within the hacker community. They often

discover and share new exploits. These hackers possess advanced technical abilities and are typically at the forefront of identifying vulnerabilities in systems and networks.

(7) **Script Kiddies**

Script kiddies are non-technical individuals who have personal knowledge of professional hacking tools. They often lack in-depth understanding but can use pre-written scripts and software to execute basic hacking tasks.

2.2 The Phases of Ethical Hacking

(1) **Reconnaissance**

Throughout the first phase, often known as footprinting, the hacker conducts a preliminary survey to gather information about the target system. This includes information such as DNS servers, administrator contact, and IP addresses. This data is collected using a range of methods involving network mapping vulnerability scanning technology; for example, Cheop, a network mapping tool, may build networking graphs that can help comprehend the network architecture. These steps are crucial for gathering an overview of the network, which helps plan the upcoming attack.

(2) **Scanning**

In this phase, the attacker attempts to create a blueprint of the target system. This guideline includes identifying live IP addresses, services running on those systems, and other relevant information. Modern port scanning techniques utilize the TCP protocol to scan for open ports and can even detect the operating system running on a specific host.

(3) **Enumeration**

Enumeration includes getting servers to provide vital information that assists in planning the attack. The hacker aims to identify available resources, user accounts, groups, and applications within the network. This information is crucial for identifying potential vulnerabilities as well as areas for exploitation.

(4) **Gaining Access**

This phase involves the actual hacking, where attackers attempt to gain access to the network. The hacker applies the information collected in previous pages to overcome challenges such as passwords. Initially, the attacker focuses on entering the system.

(5) **Maintaining Access**

After starting the system, the hacker can upload, download, or manipulate files as needed, the goal of which is to establish a constant presence within the system to facilitate future access. This may include creating a backdoor for access points for re-entry into the system.

(6) **Clearing Tracks**

In the final phase, the attacker eliminates any physical evidence of their activities to avoid detection. It includes the deleting logs and traces of their presence on the system.

Tools like auditpol, exe, and evidence eliminators are commonly used for this purpose. This phase ensures that the hacker's activities remain undetected and intangible. Figure 1 below shows the phase of hacking. The below figure explains the phase of ethical hacking.

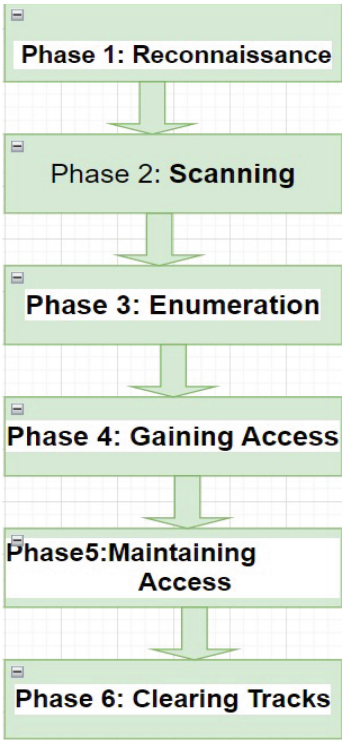


Fig. 1. Phase of ethical hacking.

The Fig. 1 above shows the phase of hacking. The below figure explains the phase of ethical hacking.

2.3 Role of Ethical Hacking

In our modern society, depending on technology plays a crucial role in how we live, work, and interact. The digital organization of our society has many challenges and benefits. The role of ethical hacking is highly important in protecting our digital transactions. Ethical hacking refers to authorized attempts to penetrate a system, network, as well as application to identify and fix security weaknesses before criminals exploit the target system. This active approach is crucial across the economic sectors, where ethical hacking is essential for protecting sensitive data, ensuring safety, and maintaining operation integrity. In the financial sector, ethical hackers conduct security evaluations on online banking platforms (ATM) and internal networks to assist the organization in keeping up with needs, such as the Payment Card Industry Data Security Standard (PCI

DSS). Additionally, they simulate attacks to identify potential fraud vulnerabilities, safeguarding customer information and financial assets. In the retail industry, particularly e-commerce, ethical hacking plays a significant role in testing the security of online shopping sites. Payment gateway and customer database, prevent data breaches, and ensure safe transactions.

2.4 Ethical Hacking Tools

(1) **NMAP**

Nmap is an open-source network scanner tool for network discovery and security evaluation. Although it is designed to scan a large network, it is also used to scan a specific host. It plays a great role in managing a network inventory so that network administrators can schedule service updates.

(2) **Burp Suite**

Burp Suite is a widely used platform that is commonly used for security tests on online applications and developed by PorttSwigger. It offers a range of tools that work together to support the testing process. From the beginning of the mapping and surveillance of the attack surface, an application to detection and exploitation of security weaknesses. It is easy to set up and can be used easily. And it is a successful testing method [11].

(3) **Angry IP Scanner**

Angry IP Scanner is a user-friendly platform tool designed to scan IP addresses and ports. It allows users to scan any range of IP addresses available for free use and distribute scanning threats for each IP address. Which significantly accelerates the scanning process. The tool pins each IP address to check its statutes and then resolves the hostname. Scanning the ports for each host can save them in various formats, including TXT, XML, and files. Plugins can be used to gather information about scanned IPs, enhancing the tool's functionality.

(4) **Web Inspect**

Web inspects is a security assessment tool designed to evaluate the security of web applications. It helps to identify both known and unknown vulnerabilities within the web application layers. The tool can also simulate common web attacks, such as parameter injection and directory traversal, and it ensures that a web server is properly configured.

(5) **Metasploit**

Metasploit is one of the most powerful tools and widely used open source for penetration testing and security research, developed by H.D in 2003 and later acquired by Rapid7, and it helps security professionals identify and spot testing to determine if the vulnerabilities can be exploited and important scan data to identify network configuration.

2.5 Common Hacking Techniques

(1) **Phishing**

Phishing is a method of sending a false email or message that appears to be from a trustworthy source. These messages frequently included links to fake websites that look like trustworthy ones, asking customers to enter sensitive information such as usernames, passwords, or credit card numbers.

(2) **Denial of Service (DoS/DDOS) Attack**

A denial-of-service (DoS) attack is a hacking strategy that affects the functionality of a website. Hack accomplishes this by spamming the site with data requests, frequently utilizing Zombie computers. This flood of traffic is aimed at taking over the web website's resources, making it completely useless [12].

(3) **Social Engineering**

Social [13] engineering exploits human psychology to access confidential information. This can involve tracking people into disclosing personal information, clicking on malicious links, or gathering unauthorized access to the system [11].

(4) **Cookie Hijacking**

In a cookie hijacking attack, a cybercriminal steals a user's authentication cookies, which act as the key for accessing a remote server. These HTTP cookies are commonly used to maintain user sessions across multiple website visits. Due to their accessibility on the victim's device, these cookies are vulnerable to theft.

3 Research Methodology

This chapter outlines the recommended methodology used in this research to understand the impact and role of ethical hacking in modern society, focusing on the economic effect, how it helps to protect sensitive information and maintain the integrity of the financial system, and preventing significant financial losses as well as enhancing economic stability [14]. By implementing various cybersecurity strategies. Ethical hacking mitigates the risk of cyber threats, and ethical hackers identify vulnerabilities in the system by running penetrate test martial to ensure the safety of digital assets. To answer the research question, ethical hacking, or penetration testing, is a preventive strategy that simulates a financial institution's cyberattacks to identify and resolve vulnerabilities before malicious actors can exploit them in networks, applications, and systems, allowing enterprises to improve their flow on the system. Evaluating and improving security mechanisms, ethical hacking helps prevent financial fraud and data breaches. The insights gained from these simulations lead to better enchantment of security strategies, ensuring fast and effective action in the face of a real cyber threat. Implementing ethical hacking methods in modern society comes with several challenges and benefits. The main challenges include the high cost associated with hiring skilled ethical hackers and advanced tools, the complexity of conducting the thorough penetrating test without affecting business operations, and the difficulty in determining the scope of the test. On the other hand,

the benefits are great; ethical hacking allows for early detection and mitigating of flow, significantly reducing the risk of cyber threats. In today's connected digital ecosystem, ethical hacking become a crucial tool for reducing cyber risks and data breaches and protecting the digital landscape. It enhances incident awareness, allowing organizations to respond quickly and efficiently to secure issues, reducing possible damage. Ethical hacking indicates that businesses can protect their vital systems and sensitive data by promoting an active safety strategy and maintaining customer and partner trust and confidence. This paper explores the key factors influencing optimal investment in information security (IS). Our goal is to demonstrate that the most effective strategy varies for organizations facing cyber terrorist attacks compared to those targeted by common hackers. Although both types of attackers use similar tools, the motivations of cybercriminals can lead to different suitable investment levels. We utilize game theory to develop a model that incorporates crucial factors affecting these investment decisions, highlighting the economic impact of cybercriminal.

Measures Recommended to Protect System

(1) **Install an Anti-Spyware Package**

Installing an anti -spyme package is an essential step in protecting our system from malicious software designed to steal personal data, it plays a significant role in detecting and deleting spyware, which can stack online activities and get access to the system to log in.

(2) **Install Antivirus Software**

Installing Antivirus software plays a great role in protecting our system by detecting threats in real life, safeguarding our data, provide automatic updates, which helps define against cyber criminals. When installing the software, it's important to actively schedule regular virus scans to ensure our device remains free from malware.

(3) **Use Encryption**

Encryption can protect our data even if hackers manage to access our network and files. We can encrypt our hard drives using BitLocker on Windows or File Vault on Mac, which also encrypts USB flash drives that contain sensitive information. Moreover, use a VPN to secure our online traffic. Always shop on a website that uses encryption. Indicated by "https" in the address bar and a closed padlock icon.

(4) **Use Complex Passwords**

Creating secure passwords is one of the most. Crucial strategies for preventing network attacks. Make a strong password, and it becomes hard for hackers to crack the system. Make sure our password is at least eight characters long and includes special symbols and letters. Upper-case alphabets: A, B, C, D, E Lower-case alphabets: a, b, c, d, numbers: 0, 1, 2, 3, Special characters: %, (,+, #. Etc. Figure 2 illustrates the pivotal role of ethical hacking in bolstering modern societal structures through improved security measures and risk mitigation strategies.

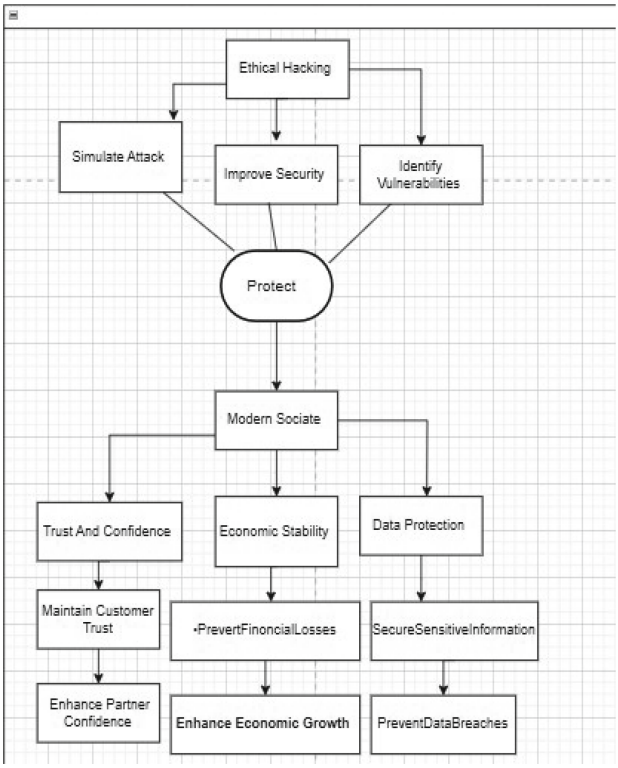


Fig. 2. Ethical Hacking's Role in Enhancing Security and Risk Mitigation

In 2023, a survey was conducted to evaluate. Participants' awareness of ethical Hacking and the measures the key to prevent it. This survey includes several questions to gather detailed responses on these topics. The finding from this survey is detailed in the result section, [11]. The (Fig. 3) below Survey result indicates that a significant number of people tend to use the same password for the different platforms, including devices, websites, and applications. This practice identifies a common weakness in personal security habits, as it increases the risk of many accounts being compromised ifone password is breached. The a below (Fig. 3) shows most people start using different passwords for various platforms. This emphasizes varying password security practices among users. When asked about antivirus installation on their device, 65.1% of respondents answered "YES" and 34.9% answered "NO." This indicates a high awareness of cybercrime threats among people today.

The Fig. 4 analysis shows an almost equal number of individuals change their passwords monthly and frequently. Very few people never change their passwords.

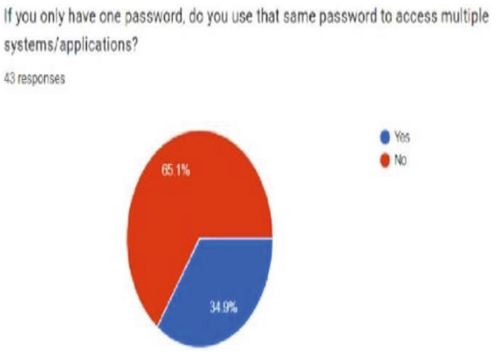


Fig. 3. Survey results showing widespread reuse of passwords across multiple platforms

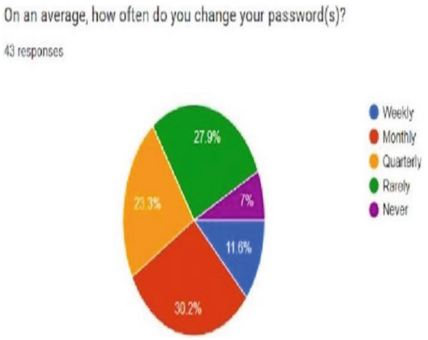


Fig. 4. Password Change Frequency Analysis

When asked about antivirus installation on their device, the Fig. 5 shows 65.1% of respondents answered "YES" and 34.9% answered "NO." This indicates a high awareness of cybercrime threats among people today.

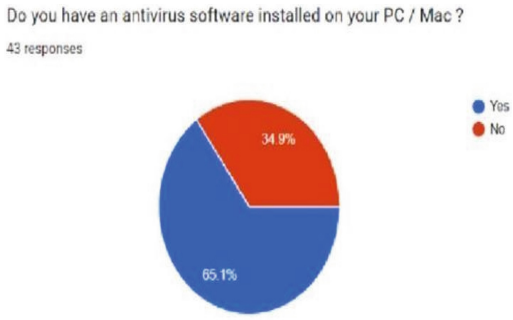


Fig. 5. High Awareness of Cybercrime Threats Among Respondents

The (Fig. 6) shows that among of 43 respondents, 41.9% are neutral about the security of their home computer against online threats, 32.6% feel the safest, 20.9% feel secure enough, and 4.7% do not feel secure. Experienced some form of cyber-attack.

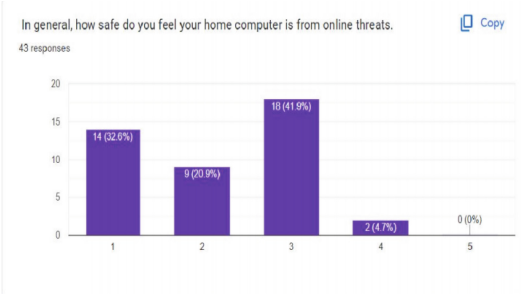


Fig. 6. Security Perception of Home Computers among Respondents

This below (Fig. 7) question aims to assess the respondents' awareness of cybercrime. The responses revealed that 37.2% were very aware, 48.8% were aware, 14% were not aware, and 0% were not aware at all.

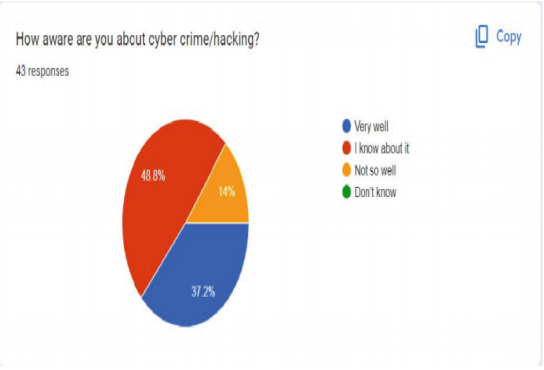


Fig. 7. Respondents' Awareness of Cybercrime

The Fig. 8 show among the respondents who answered this question, 16.3% believe that online information is very safe, 51.2% consider it somewhat safe, 25.6% think it is not safe, and 7% are unsure.

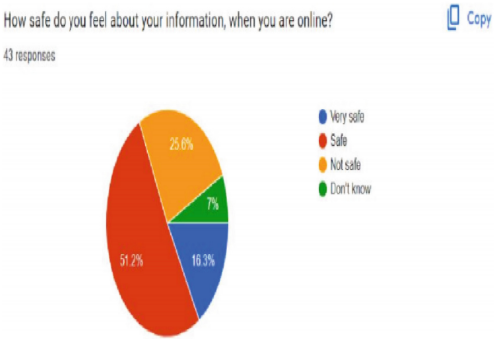


Fig. 8. Perceived Safety of online information among respondents

The below Fig. 9 Access to our data is a critical concern. Out of the 43 respondents, approximately 80% have. Experience some from cyber-attack.

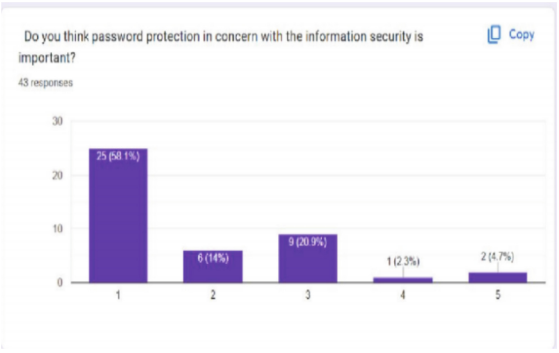


Fig. 9. Data access Strategy

The below chat Fig. 10 show response from 43 participants on the experiences with cybersecurity threats. Key finds are48% received auto generated email, 34.9% had obscure material published on their profile, 27.9% encountered. Trojan or malware, 20.9% had their confidential information hacked, 20.9% never experienced such situations, and 7% faced Trojan or malware again. This highlights that auto-generated emails and obscure publication material are the most common issues faced. Figure 10 showing that 48.8% (21 respondents) reported receiving auto-generated emails in their inbox. 34.9% (15 respondents) experienced the publication of obscure material on their profiles. 27.9% (12 respondents) encountered Trojan or malware. 20.9% (9 respondents) had their confidential reports/information hacked.

Another 20.9% (9 respondents) reported never having experienced any of the listed situations. 7% (3 respondents) faced Trojan or malware again, likely indicating a repeat or different understanding of the earlier point.

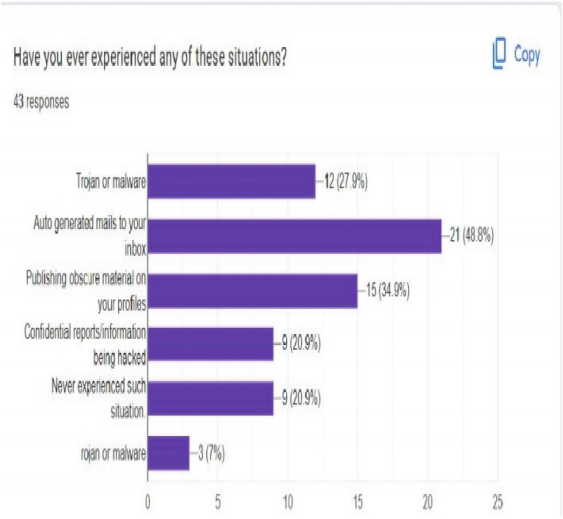


Fig. 10. Participants' Responses on Cybersecurity Threat Experiences

4 Conclusion

In the face of increasing cyber threat, this paper demonstrated the critical hacking in improving cybersecurity and ensuring modern society's economic stability, as ethical hacking referred to penetration tests. Are essential for detecting and correcting. Security flaws in organization systems and networks. Our findings show that this is avital element to protecting sensitive. Information, preventing financial losses, and maintaining trust in the digital landscape. The implementation of ethical hacking standards is valuable across different business sectors. Though the active simulation of cyberattack, ethical hacking enables to detect and resolve vulnerabilities earlier to their exploitation by malicious actors. This promotes trust with client and partners by transformation into valuable reduction in finical losses due to fraud and data breaches. As our technological society continues its quickly rising, a comprehensive understanding of cybersecurity and ethical hacking practice become increasingly crucial. Examining the tools and potential impact of both these domains is essential. By implementing these strategies modern society can get significant. benefits, however, it's important to acknowledge the potential consequences, Aswell. The security of our communities and safety of our financial markets could both be. impacted by these attacks. Nowadays, there a lot of emphasis on the modern society and organization to protect their data from internal as well as external dangers to their computer system. Come out by hiring ethical hacker to improve their safety measures as a solution to their problem. This study contributes to enhancing safety across various economic sectors by highlighting the crucial role of ethical hacking. By evaluating the effectiveness in identifying and addressing security vulnerability, provide key insights into preventive strategies against threat. HI research aid in navigation cybersecurity compliance, crucial for secure digital transaction, impact of cybercriminal and

vital for safe digital word. This research finding provide actionable to empower modern society and develop strong cybersecurity techniques, eventually this understanding. Enable firms to successfully define against emerging risk and protect sensitive data.

5 Future Work

This study highlights several areas for the future research and acknowledges, the key area for the further study exploration including unaddressed cyber security factors, the role of ethical hacking digital currency in online transaction and knowledge management in e commence, and diverse practice of ethical hacking, which complicate generation, reliance on existing literature that my not reflect advancements, the rapid evolution result. Additionally, resource constraints and limited access to comprehensive datasets may affect the depth of analyses, it is essential to keep flinging current band address evolution cyber security challenge.

Acknowledgment. I would like to express my deepest gratitude.to everyone who supports me throughout this research. First, I thank Albukhary International University for providing me with the resources and academic environment necessary for this work. I am deeply grateful to Dean, school of computing and informatics Associate Prof Dr Basheer for his inspirational leadership. a special thank you to my supervisor, Prof Dr Khalid Hussain for his excellent guidance, encouragement. Your belief in me has been my most powerful motivation, thank you for your valuable contribution to this journey.

References

1. Mary Pushpa, C., Udaya Lakshmi, K.V.M., Hepsibha, S.: Ethical hacking : roles, phases and impact on various sectors of the economy. Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol. (2021). https://doi.org/10.32628/cseit21765
2. Lucas, T.J.: 'JÚLIO DE MESQUITA FILHO' About Intrusion Detection in Computer Networks and Computational Systems: A Pruning Proposal to Reduce Computational Cost and Gain Performance using Ensemble Learning.
3. Liu, X., et al.: Cyber security threats: a never-ending challenge for e-commerce. Front. Psychol. (2022). https://doi.org/10.3389/fpsyg.2022.927398
4. Rezazadehsaber, S.: When is Hacking Ethical? (2015)
5. Hussain, K., Rahmatyar, A.R., Riskhan, B., Sheikh, M.A.U., Sindiramutty, S.R.: Threats and vulnerabilities of wireless networks in the Internet of Things (IoT). In: 2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC), pp. 1–8. IEEE (2024)
6. Basheer Riskhan, R.M.: Virtual machine performance approaches in the online education system. In: Proceedings of the International MultiConference of Engineers and Computer Scientists (2016)
7. Chowdappa, K.B., Lakshmi, S.S., Pavan Kumar, P.N.V.S.: Ethical Hacking Techniques with Penetration Testing [Online]. Available: www.ijcsit.com
8. Ul Haq, H.B., et al.: The impacts of ethical hacking and its security mechanisms. Pak. J. Eng. Technol. **5**(4), 29–35 (2022). https://doi.org/10.5146/vol5iss4pp29-35
9. Kaushik, D.: The Impacts of Cybersecurity and AI on Businesses and Individuals [Online]. Available: www.JSR.org

10. Sahare, B., Naik, A., Khandey, S.: Study of ethical hacking. Int. J. Comput. Sci. Trends Technol. 2 Online]. Available: www.ijcstjournal.org
11. Patyane, P.V., Kenny, V.: A review on different ethical hacking techniques and its impact on cyber security. Int. J. Adv. Res. Sci. Commun. Technol. (IJARSCT) (2023). https://doi.org/10.48175/Paper-12077
12. Riskhan, B., et al.: An adaptive distributed denial of service attack prevention technique in a distributed environment. Sensors **23**(14), 6574 (2023)
13. Krombholz, K., Hobel, H., Huber, M., Weippl, E.: Advanced Social Engineering Attacks ☆." [Online].
14. Raufi, M.: Physical security to cybersecurity (challenges and implications in the modern digital landscape). J. Electr. Syst. **20**, 692–702 (2024). https://doi.org/10.52783/jes.2090

IoT Revolution in Education: Transforming Learning Through Smart Technology

Amena Mahmoud[1](✉) and Eiko Takaoka[2]

[1] Department of Computer Science, Faculty of Computers and Information, Kafrelsheikh University, Kafr el-Sheikh, Egypt
amena_mahmoud@fci.kfs.edu.eg

[2] Department of Information and Communication Sciences, Faculty of Science and Technology, Sophia University, Chiyoda, Japan
m-g-eiko@sophia.ac.jp

Abstract. The Internet of Things (IoT) is set to revolutionize education with personalized, interactive, and data-driven learning. This paper examines the integration of IoT-driven smart technology into education and its prospects and problems. This transformation relies on IoT devices and sensors to capture and send massive volumes of data from educational ecosystem touchpoints.

Keywords: The Internet of Things (IoT) · Web of Things (WoT) · Data Privacy

1 Introduction

The rapid progress of the Internet of Things (IoT), providing large-scale, distributed, intelligent, integrated systems, is providing the promise for this education revolution. With the ability to connect physical devices and tools, collect their data, and provide service from anywhere in the world, university teacher-student, student-student, and student-learning content, interactions will not be restricted by spatial or temporal boundaries [1].

Today, our world faces severe challenges relating to fast population growth along with limitations in resources and decreasing quality of life. The only way forward is to increase the knowledge base and improve educational and learning methods, thus also enhancing the quality of life. Therefore, research on the acquisition of human knowledge and development in the field of artificial intelligence is increasing rapidly and developing vigorously. One of the foremost factors and enablers for such rapid development in research and development is the rapid advancement and usage of Information and Communication Technologies (ICT) [2].

The research question guiding this paper is: *How is the Internet of Things (IoT) revolutionizing education, and what are the keyways smart technology can transform the learning experience? * The paper hypothesizes that the integration of IoT in education will lead to more personalized, efficient, and data-driven learning experiences, thereby improving student outcomes and overall institutional effectiveness.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 327–338, 2025.
https://doi.org/10.1007/978-3-031-91008-1_30

1.1 Background and Significance

The need for digital transformation in education is to create an eco-environment in dealing with smart technologies. It has been exemplified by linking smart devices to various educational systems. The correlation of IoT and education enhances the efficiency and skill set of the students. It creates an active and idyllic environment for the students to nurture their skills. IoT hence transforms education into smart education. The success of smart devices in medical, insurance, management, defense applications, etc. prompts researchers and educationalists to embrace smart education. It has recently risen as a notable breakthrough in the digital world that coordinated 'things' apply to achieve specific goals, such as saving energy, data exchange, automated operations, and more, as shown in Fig. 1 [3]. It offers both conceptual and pragmatic knowledge with an emphasis on real-time expertise. In smart education, IoT devices safeguard the students to gain enhanced knowledge, which ultimately leads to enhanced learning. Informative smart devices contribute to the academic performance of the students. Smart tools and sensors, with the help of IoT devices, enhance the education system by mediating real-time taxonomies-based learning. It evaluates the learning performance of the students and disseminates the information through virtual presentations and interactive visual content [4].

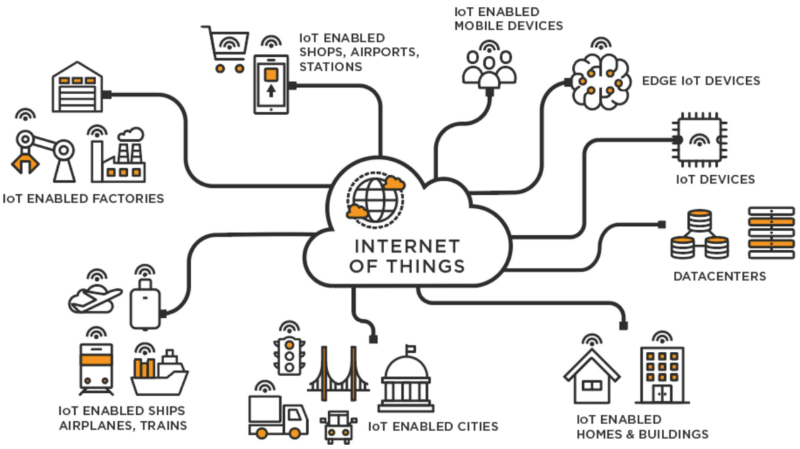


Fig. 1. Topics of IoT [3]

1.2 Purpose and Scope of the Study

The scope of the current study is twofold. First, an analysis is provided of how the IoT can be employed to develop smarter universities and other educational institutions that form part of this IoT ecosystem. The main aim of universities is teaching and research, and students, staff, and researchers are the main stakeholders. Consequently, this study examines not only how the IoT can be adopted by universities to deliver a smarter campus environment but also how to incorporate the IoT into improving both teaching and research [5].

2 Understanding IoT in Education

According to Gartner, the Internet of Things (IoT) is the networked interconnection of everyday objects and appliances that make physical computing and distributed sensing available on a global scale. These devices are equipped with processors and memory that allow them to broadcast and act on intelligence, which turns them into endpoints on the enablement network. In the education industry, IoT has had a major impact. The use of various smart devices and gadgets has enhanced student learning, enabling new ways for teachers to deliver concepts in a much clearer and more conceptual way. Smart learning devices adjust the learning process based on the student's performance and the effectiveness of learning strategies. These devices are implemented in traditional classrooms to design smart educational environments that support personalized learning, ensure better interaction among peers, and improve learning outcomes [6].

IoT is the network of physical objects (devices, vehicles, buildings, etc.) that are embedded with sensors, software, networks, and electronics allowing them to collect, exchange and act on data. It is a giant network of connected things and people that also communicates in a manner that goes beyond the existing connections. The objects within the Internet of Things work and connect to enhance our daily lives. For example, every day, objects are becoming smarter, more pervasive, and interconnected. The future of IoT is more interesting than we think. According to experts, there are more than 12 billion devices that are connected to the internet in 2020. The IoT (Internet of Things) provides many valuable applications and several solutions for many problems in all domains.

2.1 Definition and Concepts of IoT

As a concept, IoT is truly broad, and - as a result - it encompasses a great set of areas and domains. As a recent and leading tool, it integrates Editor into education concepts and approaches to positively impact the learning and teaching process, through, for example, e-learning and cloud computing. In this paper, the authors explore how IoT can be employed in this context. Furthermore, from different perspectives, researchers have also contributed with a wide variety of extensive thematic literature allowing for the improvement of different applications of the concept and deployment of new studies that will certainly bring even more innovation. Due to the extensive capacity that IoT has to transform distinct sectors, professionals from different areas and courses need to prepare themselves to impact the correct use of this concept in practical application in the labor market and society [7].

The Internet of Things (IoT) is not only one of the most significant technological developments of the last years but also a "paradigmatic shift in today's world transformation towards a convergence between the physical and digital realms." It can refer to objects and devices such as sensors, actuators, and mobile phones, among others, that transmit and receive data harmoniously over the Internet. Simplified straight-to-the-point definitions of IoT could be as follows: (i) IoT is the concept that carries the essence of emerging technologies such as Big Data and artificial intelligence; (ii) IoT is the network and connectivity that enable technological prowess-related functions over the Internet; and (iii) IoT is the concept that communicates with the online world, the Internet, and mobile devices that can interact with each technological function [8].

2.2 Applications of IoT in Education

An integrated network is the IoT world, in essence, built from a vast number of physical devices and software. Irrespective of whether the personal device is a tablet, smartphone, laptop, or desktop computer, all personal devices are part of a much larger entity. IoT technology holds great promise in providing a personalized learning experience for students. The IoT environment helps teachers acknowledge the specific learning issues that many students face, as well as the benefits that individualized assistance can provide. With the help of holistic data logs, students may contribute to a more comprehensive overview of classroom dynamics, including overall understanding and expertise. Each learner can access the IoT-based learning system wherever and whenever they choose as long as they have an internet connection [9].

IoT not only inspires learning materials in traditional contexts but also plays a key role in globally connected and smart campuses. Educational infrastructure plays a crucial role in supporting teaching and learning processes, involving people, and ensuring optimal development conditions for living and learning. With the help of smart sensing devices and technologies such as RFID beacons, smartphones, tablets, Wi-Fi networking, and energy-efficient thermal surveys to form a self-adjusting environment that constantly adapts to fit students, use the IoT and the cloud to connect everything. You can leverage the information to develop apps, data visualizations, and images [10].

3 Benefits and Challenges of Implementing IoT in Education

The practical implementation of IoT in education has the potential to transform the viewers' spent time from passive to active engagement, and thereby activate the potential value of a museum as well as a museum's human, social, and financial capital by enhancing the learning experience and contributing to the museum's vitality. Fifthly, classroom and equipment management can be performed via a wireless sensor network platform design and use. Using the Web of Things (WoT) language, the designed platform enables semantic-language-independent interaction with the sensors by several WoT clients such as mobile applications and a web user application. Consequently, the designed wireless sensor network platform for classroom management enables more efficient and sustainable utilization of energy and equipment, verifies the significance of adapted lighting and temperature for improved learning efficiency, and demonstrates the feasibility of semantic-language-independent interaction with the designed sensor devices. Moreover, location-based learning activities and users' learning preferences are considered as different contexts. In this direction, a context-intelligent system consisting of a remote-learner monitoring and learning exploration tool on a cloud server and an Android sensing toolkit on students' mobile phones is presented. Indeed, this system can identify the individual's learning status and suggest the appropriate learning object accordingly. Furthermore, Internet-enabled project-based learning laboratories could bring a concept of know-how to design, build, and test a small-scale wireless sensor network sensing device and allow engineering students to access and manage the device through the Internet [11, 12].

3.1 Benefits of IoT in Education

Today, it is a well-known fact that the Internet of Things (IoT) is not just limited to a few sectors. The merging of physical systems and the internet, which results in intelligent systems, is currently called IoT. Smart education is the future of education. The implementation of educational requirements using high technologies leads to smart education. The edge of technology expansion daily results in the optimization of every section from personal to professional life. There are many benefits gained through IoT in the education system. The major benefits of IoT in the field of education are advanced infrastructure, active learning environment, real-time data, personalized learning, reducing the gap between the learner and the teacher, wider access to education, enhancing the classroom experience, peer-to-peer learning, greater opportunity for continuous learning, reducing the administration work, enhancement in security, automation of activities, and saving money by making educational institutes more efficient, as shown in Fig. 2. The educational institutes that embraced IoT in their educational milieu led education to have the next transformational level [13].

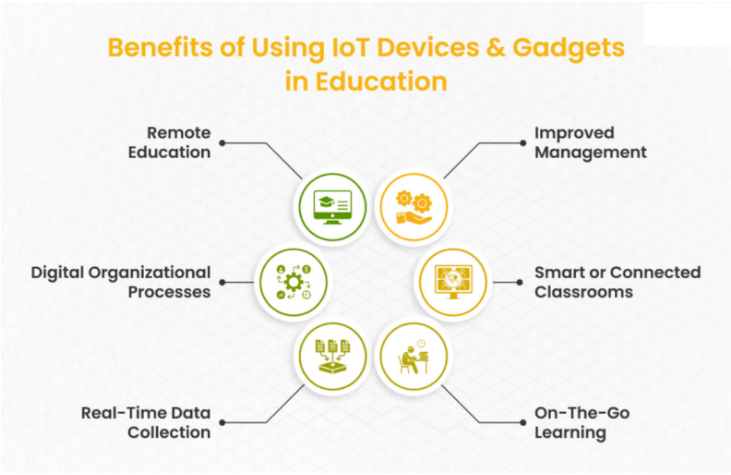


Fig. 2. Benefits of using IOT devices in Education

The Internet of Things provides tremendous benefits for the educational sector by offering an active learning environment. IoT in education provides an active platform for learners. The key benefits of IoT in the field of education are discussed, which are: high-advanced infrastructure, active learning environment, different learning styles, real-time data, personalized learning, reducing the gap between the learner and the teacher, wider access to education, enhancing the classroom experience, rise in availability of digital classroom content, peer-to-peer learning, greater opportunity for continuous learning, reducing the administration work, enhancing security concern, automation of activities, enhanced non-instructional area, saving money by making educational institutes more efficient. The educational institutions embrace IoT into their environment, which leads education to have the next transformation level [14].

3.2 Challenges and Barriers to Implementation

Barriers to the uptake of technology are present in educational settings at all levels. In their study of five schools in Scotland, Muir-Herzig and Ryan (2010) reported that "real" pedagogical benefits (p. 37) from the technology are evident in schools that have successfully integrated technology into their work, but that several "barriers" (p. 37) still exist which prevent this from happening more widely. These include teacher knowledge, funds available for infrastructure, policy constraints, the ICT skills/attitudes of teaching staff, professional development, competition between curriculum initiatives, and dissatisfaction with learning and teaching. Some of the "real" pedagogical benefits included "access to creation tools, filtering and transformation into usable knowledge, blended learning, and access to networks for sharing knowledge and drawing on the expertise of peers beyond the school walls". This work is reflected in that of Mirchandani et al. (2016) and Coates (2018), who identified the perceived lack of skills teachers have in integrating devices and application tools into their teaching [15].

4 Case Studies and Best Practices

A majority of educational IoT projects introduced in this paper focus on enhancing the learning experience (when students interact with electronic devices like tablets and smartphones). In this section, we showcase an example of using IoT for educational systems with which the students do not interact directly - we are not using IoT to improve study quotient but rather to enable smart energy management and savings extraction for campuses that are equipped with smart devices. We propose and implement an IoT-based device called IllumiDesk, which leverages occupancy and luminance data to enable intelligent lighting and electrical socket management. Our implemented system includes four components: a) ceiling-mounted occupancy sensors which have a 160-degree detection pattern, 1000 square feet coverage area, edge light immunity, occupancy light sensitivity adjustment, battery or 5V USB power interface, and wired and wireless networking (due to IoT radio technology diversity, some devices are time-synchronized, and can act as a network gateway, hence they have higher cost); b) human-centric lighting and socket controllers, which are installed by connecting to each light and electrical socket to an automated control actuator, and each actuator is connected to the SCB of the named gateways; c) Wi-Fi capable LoRa gateway(s) to serve as network servers; and d) cloud server to provide analytics solutions. During the deployment, we found that 84.7% of campus electricity savings can be achieved [16].

4.1 Successful Implementations of IoT in Educational Settings

Examples include the successful implementations of an underwater IoT system at an Indian marine national park and the design and implementation of a smart energy consumption monitoring system in educational institutions. They presented useful levels of research in certain administrative and operational areas. IoT applications, virtual learning, and crowd learning are helping learning experiences become richer and more practically developed. The research raises the possibility of creating other value-added

places or territories for active learning within and around an educational institution and its physical and digital infrastructure. It can add even more value to the institution, taking into account the university-industry and university-community relations, their research and capturing of potential students, and the exploitation of IoT technological solutions [17].

Apart from data analytics, numerous other applications of IoT are being successfully implemented in educational contexts. Examples include intelligent tutoring, virtual and remote labs, crowd learning, and e-assessment systems. Uncommon Learning is a great repository of innovative educational IoT projects carried out around the world. Furthermore, value-added hubs created using IoT technology in educational institutions in Malaysia appeared as a potential source for creating IoT places for learning, working, and living. Among these examples, we stress the fundamental importance of security in the successful and safe implementation of the IoT. The ecosystem or environment of an educational institution, both physical and virtual, must implement the necessary security and privacy measures to avoid any breaches of integrity, secrecy, suspensions, and other potential risks right from the educational objectives through to the finish point of any educational activity.

5 Ethical and Privacy Considerations in IoT Education

Under the GDPR data minimization principle, it is becoming increasingly necessary for IoT data to be minimized, especially if they are to be used for profiling purposes. Students must be adequately informed as to how their IoT-generated data are collected and can only be processed providing they give explicit consent. Colleges may need to retain student data for serious in-house research enforceable by law or where it is in the public interest. The EU Educational Sector Cyber-Attack Recovery Platform (ECSR) will also have an essential role to play in restarting educational institutions hit by a cyber-attack [18].

Article 8 of The General Data Protection Regulation concerning the protection of personal data is the key regulation on EU data protection rules, including for non-EU companies processing EU data. It also addresses the export of personal data outside the EU. These rules aim to give citizens back control of their data and simplify the regulatory environment for international business by unifying the regulation within the EU. GDPR has a significant influence on IoT technologies by bringing in a more consistent application of data protection across the EU, and academic institutions need to know they will be playing a significant role in the collection and processing of student data.

Collating the personal data of numerous students undoubtedly raises ethical, privacy, and security concerns. IoT-ed uses stores, and manages vast amounts of students' data, including personal, sensitive, or confidential information. There is the potential to identify students through the use of facial tracking, gamification, and even basic visualization as colleges grow more data literate. Moreover, IoT-generated data is non-stationary; that is, its characteristics can change over time, and this may lead to generic ethical issues such as keeping data accurate and relevant.

5.1 Data Privacy and Security

In the current era of Web 2.0 and social media, we are already sharing a lot of personal information over the Internet. The availability of sensors in educational environments will generate opportunities for data to be analyzed and decisions to be made based on that data. The IoT systems capture, process, and store a large amount of data which is available to a broad audience. Cyber-attacks can put a large amount of personal information at risk. The data collected by those sensors is also sensitive, and personally identifiable information (PII) is also collected. As the amount of data and its uses will increase, now it is necessary to focus on developing a framework for protecting student data in the increasingly networked world. Protecting the data and privacy of the students is an important challenge for educators to address. The goal of this paper is to summarize the role of IoT in education and explore the potential risks and responsibilities that come with it. It also discusses what technologies or policies can be implemented to ensure that student data is protected [19].

IoT helps in the automation and monitoring of education systems and processes. Every component and device will interconnect, collect, measure, interact with each other, and work together to provide an efficient learning environment. Once these data are captured, they can be used for various educational decision support systems for decision-making. Educational Data Mining (EDM) and Learning Analytics are some important techniques that mine data and provide useful analysis and knowledge. However, more data means more concern about student's data security and privacy. The student's data should not be misused and no information about the students should be revealed unless it is necessary for the specific purpose. IoT security protects systems, services, and user privacy from improper access, use, and information disclosure.

5.2 Ethical Use of Student Data

Another ethical challenge to remain ever vigilant is the potential bias in recommendation algorithms. Edtech solutions are increasingly being used to provide educational recommendations for students based on their data. Algorithms embedded in these solutions decide whether students should be recommended for basic, regular, or advanced courses, what types of examples should be shown, and how learning goals should be framed. These algorithms have been known to reflect biases held in our human world as they rely heavily on historical patterns to predict the trajectory of school children. When using observational data, a system will recommend in the future what has been put in, so biased input results in biased output. Harmful long-term impacts ensue when students are tracked into programs or careers with lower expected returns compared with what they could have achieved with better recommendations. If everyone interprets which actions they should take next by reviewing personal recommendations that reflect current social inequalities, digitizing such recommendations will do little to reduce the achievement gap. For this reason, some researchers have suggested that automated decision-making should be halted until we understand how to ensure that these decisions respect certain ethical requirements, especially when they help in shaping student performance and careers on a broad scale [20].

Ethical Use of Data: Student data should only be used for purposes directly related to education, and not for tracking behaviors irrelevant to learning (e.g., outside school activities) unless explicitly agreed upon by all stakeholders. Any deviation from the educational purpose could lead to the misuse of data and infringe upon student rights. Whenever possible, data should be anonymized or aggregated to prevent the identification of individual students. This is particularly important when data is being analyzed for research purposes or shared with third-party vendors. Anonymization helps mitigate the risk of data being used for discriminatory practices or targeted advertising.

Algorithmic Accountability: To prevent bias in IoT systems, regular audits should be conducted to assess the performance and fairness of the algorithms. These audits should include testing for demographic fairness, ensuring that no group is disproportionately affected by the system's decisions. External reviews and collaborations with ethicists or fairness experts can help identify and correct biases early. Additionally, systems should be designed so that educators and administrators can understand how decisions are made. This ensures that teachers can intervene if an algorithmic decision seems unfair or inaccurate. The goal is to ensure that IoT-driven educational tools serve as supportive aids rather than opaque decision-makers.

Building Ethical Frameworks: educational institutions need to develop clear policies that define the ethical use of IoT systems, addressing issues like data ownership, algorithmic transparency, and bias mitigation. Policies should ensure that student data is treated with the same level of care and respect as other sensitive information and provide protocols for responding to data misuse or breaches.

6 Future Trends and Innovations in IoT Education

How can the IoT cause changes in the processes that occur in the field of education? IoT changes the rules of the game not only in terms of the technical possibilities that can lead to improvements and increase the effectiveness of existing processes. The very essence of education is changing. IoT brings into the educational environment real-life situations and lifelike conditions for performing authentic work activities. The educational site in the IoT epoch should expand its boundaries beyond the institution by connecting to the surrounding environment both in the information and in the functional sense. In addition, because of the high level of support and the algorithms of the future IoT, most of the processes occurring in the educational environment will not require human intervention. This will free up a significant amount of educational time that, instead, can be devoted to more complex occupational activities [21].

6.1 Emerging Technologies

The miniaturization of devices through the use of the MEMS technology platform has also been very instrumental in creating these sensors. Furthermore, the convergence of MEMS, smart sensors, microelectronics, and RF technology to integrate the sensor with a reader to make a highly optimized system that can operate in a compact embedded mode has drastically reduced the power required for such a communications node. In addition, while the large sensing nodes remain connected to energy-rich parts of the

network, the micro-sensing nodes can benefit from energy scavenging techniques to be deployed in remote or inaccessible areas [22].

Sensors of varying capabilities are the indispensable building blocks of application domains such as healthcare, environmental monitoring, home and industrial automation, and critical infrastructure protection. To become a part of the IoT, these sensors not only require hundreds of sensing nodes that will be able to perceive, analyze, diagnose, and make decisions with limited latency but also need to have a strong cyber-computational component that enables them to communicate with other devices. Furthermore, they would have to be capable of applying processing algorithms to raw data and communicating with other entities in a large-scale, IoT-like fashion.

6.2 Potential Impact on Teaching and Learning

The rapid development and implementation of 4IR technologies are rapidly transforming the world of work. The rapid adoption of smart technology to drive new sources of innovation, growth, and competitiveness in organizations is compelling educators worldwide to consider the potential impact of smart technology on the teaching and learning environment. Although the impact is expected to be significant, the associated high costs and potential lack of skills present a significant barrier to entry. Yet, the expected increase in the potential and value of eLearning and portal management systems that help to address both cost and the lack of skills could provide the necessary catalyst for change. The increasing digital maturity of students and the requirement to deliver future-fit graduates have been identified as important drivers of change [23].

It is generally agreed that the 4IR has the potential to disrupt and transform the teaching and learning environment. In essence, the rapid adoption and integration of smart technology introduces new approaches to both the teaching and learning environments, utilizing the concept of smart connected campuses to transform educational delivery. In the following, the framework of 4IR technologies is applied to provide an overview of the impact of IoT on the teaching and learning environments.

7 Conclusion

The Internet of Things (IoT) has been reported to have a significant impact on the development of the education domain. The paper investigated the application of IoT in education to enhance the engagement of students and support learning. It elaborated on the key benefits, barriers, and challenges of IoT. Moving ahead to improve the democratization of the benefits and minimize the limitations of IoT in education, the authors established an AI-driven model that allows designing analytics dashboards to provide visual and personalized feedback for teachers and students in real time. The presented case study introduced smart objects in the classroom which were supported by an analytics dashboard for real-time visualization of students' behavior data. Initial insights reported that the model has the potential to enrich the learning and teaching process. The authors finally discussed the implications and further research directions of the AI-based model.

References

1. Zeeshan, K., Hämäläinen, T., Neittaanmäki, P.: Internet of Things for sustainable smart education: an overview. Sustainability **14**, 4293 (2022)
2. Agboola, O.P., et al.: The influence of information and communication technology (ICT) on stakeholders' involvement and smart urban sustainability. Environ. Adv. **13**, 100431 (2023)
3. Tech 101: Internet of Things. https://businesstech.bus.umich.edu/uncategorized/tech-101-internet-of-things/ (Accessed 2023)
4. Koohang, A., et al.: Internet of Things (IoT): From awareness to continued use. Int. J. Things **62**, 102442 (2022)
5. Dong, Z.Y., et al.: Smart campus: definition, framework, technologies, and services. IET Smart Cities (2020). https://wiley.com
6. Robles-Gómez, A., et al.: Analyzing the users' acceptance of an IoT cloud platform using the UTAUT/TAM model. IEEE Access **9**, 150004 (2021)
7. Qureshi, M.I., et al.: Digital technologies in education 4.0. Does it enhance the effectiveness of learning? Int. J. Interact. Mob. Technol. **15**, 31 (2021)
8. Vermesan, O., et al.: Internet of things cognitive transformation technology research trends and applications. In: Vermesan, O., Bacquet, J. (eds.) Cognitive Digital Transformation. Taylor & Francis, New York (2022)
9. Li, K.C., Wong, B.T.M.: Features and trends of personalized learning: a review of journal publications from 2001 to 2018. In: Cheung, S., Wang, F., Kwok, L., Poulová, P. (eds.) Personalized Learning: Approaches Methods and Practices. Routledge, London (2023)
10. Kumar, K., Al-Besher, A.: IoT enabled e-learning system for higher education. Meas. Sens. **24**, 100480 (2022)
11. Vellela, S.S., Balamanigandan, R.: An intelligent sleep-awake energy management system for wireless sensor network. Peer-to-Peer Netw. Appl. **16**, 2714 (2023)
12. Kamruzzaman, M.M., Alanazi, S., Alruwaili, M.: AI-and IoT-assisted sustainable education systems during pandemics, such as COVID-19, for smart cities. Sustainability **15**, 8354 (2023)
13. Okem, E.S., Iluyomade, T.D., Akande, D.O.: Revolutionizing US Pavement Infrastructure: a pathway to sustainability and resilience through nanotechnology and AI Innovations. World J. Adv. Eng. Technol. Sci. **11**(2), 411 (2024)
14. Al-Emran, M., Malik, S.I., Al-Kabi, M.N.: A survey of Internet of Things (IoT) in education: Opportunities and challenges. In: Toward Social Internet of Things (SIoT). Springer (2020)
15. Akram, H., et al.: Teachers' perceptions of technology integration in teaching-learning practices: a systematic review. Front. Psychol. (2022). https://doi.org/10.3389/fpsyg.2022.920317
16. Ajitha, A., et al.: Design and implementation of smart home energy management system for Indian residential sector. Energy Manag. **307**, 118369 (2024)
17. Razzaq, A., Mohsan, S.A.H., Li, Y., Alsharif, M.H.: Architectural framework for underwater IoT: forecasting system for analyzing oceanographic data and observing the environment. J. Marine Sci. Eng. **11**, 368 (2023)
18. Witt, C., De Bruyne, J.: The interplay between machine learning and data minimization under the GDPR: the case of Google's topics API. Int. Data Privacy Law **13**, 284 (2023)
19. Hajjaji, Y., et al.: Big data and IoT-based applications in smart environments: A systematic review. Comput. Sci. Rev. **39**, 100318 (2021)
20. Rahayu, N.W., et al.: A systematic review of learning path recommender systems. Educ. Inf. Technol. **28**, 7437 (2023)
21. Zhu, Z., et al.: Learniotvr: An end-to-end virtual reality environment providing authentic learning experiences for internet of things. In: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems (2023)

22. Percy, J.J., Kanthamani, S.: Revolutionizing wireless communication: A review perspective on design and optimization of RF MEMS switches. Microelectron. J. **139**, 105891 (2023)
23. Gerli, P., et al.: The hidden power of emotions: How psychological factors influence skill development in smart technology adoption. Technol. Forecast. Soc. Change **180**, 121721 (2022)

Solving Mathematical Series Using Linear Ordinary Differential Equations

Basheer Abd Al Rida Sadiq(✉)

Computer Techniques Engineering, Imam Al-Kadhum College (IKC), Baghdad, Iraq
basheer.abdrida@alkadhum-col.edu.iq

Abstract. In the present study, Ordinary Differential Equations (ODEs) are chosen as base models to describe dynamic structures in different branches of science. Applying the results of ODE solutions, especially, linear ODE solutions, this paper aims at developing and analyzing mathematical series. We illustrate how selected series can be expressed and summed up with the aid of solutions of related differential equations. This approach links up more with the actual approaches to problem solving as well as improving the methods of mathematical modeling.

Keywords: Differential Equations · Series Solutions · Mathematical Series · Power Series · Taylor Series

1 Introduction

This paper introduces ordinary differential equations (ODEs) as useful tools in dynamical analysis in the social, natural, and mathematical sciences. They contain characteristics of an individual independent variable and its derivatives which enables man to gain insight to dynamic things and events [1]. Since Newton's time, ODEs have brought remarkable contributions in solving algebraic, geometric, and physical phenomena providing substantial impacts to the improvement of social and economic sciences [2]. This paper considers the use of solution to linear ODEs in developing and analyzing several mathematical series.

Research Objective: Thus, the aim of the present study is to investigate the use of linear ordinary differential equations in obtaining MA series. The purpose of this work is to reveal the role of ODEs in the formulation and solution of these series using their solutions, so important in theoretical and applied mathematics.

2 Basic Concepts

2.1 Differential Equation (6)

A differential equation is actually an equation in which the unknown feature and its derivatives with respect to one or more independent variables occur. These equations represent relationships that are composed of prices of alter and which are essential to modeling a variety of natural processes and dynamic systems. Classification is performed mainly on the basis of the order of the highest derivative existing within an equation.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 339–359, 2025.
https://doi.org/10.1007/978-3-031-91008-1_31

In the realm of regular differential equations (ODEs), an unknown function depends noon one impartial variable. DOMs are well-known in many medical fields; they let define strategies like population dynamics, chemical reaction, and mechanical ones [3].

The general shape of a regular differential equation can be represented as:

$$[F(x, y, y', y'', ..., y^n) = 0]$$

where:

(y) represents the unknown function of the independent variable.
(y', y'', ..., y^n) denote successive derivatives of (y) with respect to (x).
(F) is a characteristic linking the dependent variable, its derivatives, and the unbiased variable in the equation.

Solving differential equations involves locating functions that fulfill the given equation within a specific variety. Different techniques such as method of separation of variables, Factorization and substitution techniques are employed to solve the differential equations and study the behavior of those systems over the years [4].

learning differential equations enables the researchers as well as practitioners to have effective tools to analyses and predict the behavior of dynamic systems, thereby becoming basic tool of mathematical modeling and clinical research.

2.2 Common Differential Equation (3)

Ordinary Differential Equations (ODEs):

ODEs consist of single-variable functions and their derivatives. They are normally used to model approaches that evolve over time or area, which includes populace dynamics, chemical reactions, and mechanics [5].

$$\text{First Order ODE} : \left[\frac{dy}{dx} = x^2 + y\right]$$

$$\text{Second Order ODE} : \left[y'' + 2y' + y = 0\right]$$

Partial Differential Equations (PDEs):
PDE consists of many variables and their partial derivatives Also, this type of equation has features that are different from those of ODEs. They are actively applied in such disciplines as physics, engineering and in finance concerning phenomena that possess spatial characteristics in addition to fluid dynamics, heat conduction and electromagnetic fields.

$$\text{Heat Equation} : \left[\frac{\partial u}{\partial t} = k.\frac{\partial^2 u}{\partial x^2}\right]$$

Linear Differential Equations:
Linear differential equation is one where based variable and its derivatives appears in

linear terms. Their solution is always well defined and they perform an important role in many applications due to their mathematically convenience [6].

$$\text{Homogeneous Linear ODE} : \left[y'' + 4y' + 4y = 0\right]$$

Nonlinear Differential Equations:
Nonlinear differential equations, in contrast with linear differential equations, imply nonlinear relations involving the structured-entity and its derivatives. They still arise in large structures and can have wealthy, sophisticated interactions which could also be difficult to study however which might be important for modeling real-world phenomena.

$$\text{Population Growth Model (Logistic Equation)} : \frac{dP}{dt} = r * P * \left(1 - \frac{P}{K}\right)$$

First Order Differential Equations:
All in all, first-order differential equations are most of the time involve with the first derivative of the unknown attribute. It is imperative at numerous concerns in first text on differential equations and is necessary for knowledge more complicated differential equations [7].

Second-order differential equations:
Second order differential equations involve the second spinoff of the unknown characteristic. This is used extensively in physics, engineering and other related discipline because of its effectiveness in modeling system involving acceleration, oscillations and inertia.

Homogeneous Differential Equations:
In a homogeneous differential equation, all the phrases can be expressed in terms of the determined variable and its derivatives. They are best used to alleviate the difficulties of answering and are met most often in a number of applications.

Familiarity with the most traditional types of differential equations and their residences is vital to appropriately utilizing differential equations to model real-word systems and processes.

2.3 Partial Differential Equation (1)

A partial differential equation (PDE) is a differential equation where at least one of the variables partial derivatives exist. It details how this unknown characteristic and the partial derivations of it are inter-connected with each different one.

A usual example of PDEs is the heat equation that describes diffusion of heat in a definite area in the course of time [8].

They are differential equations of one or greater variables (x, y independent) however $Z(x, y)$ an applicable variable capable of derivation primarily based upon x and y in part as follows:

$$G\left(x, y, z, \frac{dz}{dx}, \frac{dz}{dy}, \frac{dz}{dx^2}, \ldots\right)$$

Example: The following equations (1)

$$\frac{dz}{dx} + \frac{dz}{dy} = 9 \, and \, \frac{d^2u}{dx^2} = -k\frac{du}{dt}$$

They are styles of partial differential equations.

2.4 Order of the Differential Equation (7)

The order of a differential equation is defined because the order of the very best spinoff acting in the equation.

For example, in the differential equation:

$$\frac{d^2y}{dx^2} + 2\left(\frac{dy}{dx}\right) + y = x$$

The maximum spinoff that appears is the second one spinoff $\left(\frac{d^2y}{dx^2}\right)$, subsequently the order of this differential equation is two.

In popular, the order of a differential equation gives facts about the complexity of the equation and helps decide the variety of independent arbitrary constants which can appear within the popular solution [9].

2.5 Degree of the Differential Equation (7)

The degree of the differential equation is described as the highest strength of the best order by-product in the equation.

For the given equation:

$$\frac{d^2y}{dx^2} + 2\left(\frac{dy}{dx}\right) + y = x$$

The highest order spinoff is $\frac{d^2y}{dx^2}$, which is an exponent of 2. Therefore, the degree of this differential equation is two.

The maximum energy of the best spinoff, order of the differential equation [10].

The order of a differential equation gives an insight into the complexity of the equation, as well as the technique to be used in solution. The higher-order differential equations usually need one or another additional sophisticated approach for solving, it may be Laplace transform or power series solutions.

Example:

$$\frac{d^2y}{dx^2} = sx - 3xy + 7$$

An equation of the second one order and first degree.

3 Solution of the Differential Equation (1)

This characteristic $y_1 = y_1(x)$ is referred to as an answer of the differential equation

$$If\ F(x, y, y', y'', \ldots., y_n = zero$$

A. Derivable of n times
In arithmetic, the nth spinoff of a function $(f(x))$ is denoted by way of $(f^n(x))$, in which (n) represents the range of times the characteristic has been differentiated. So, when you have a function (y) that represents a solution to a certain differential equation, and also you want to locate its nth spinoff, you'll write it in the form (y^n). For instance, when you have a differential equation $(y''y = zero)$ and (y) is a way to this equation, you may want to find the fourth derivative of (y), a good way to be denoted via (y^4).

B. Solve the differential equation
There are steps to get the differential equation from the solving function and derivatives includes substituting the solving function and its derivatives into the equation then solve algebraically for the unknown's terms.

$$F(x, y_1(x), y_1(x), \ldots, y_n(x) = 0$$

C. Defined on certain period
If we want to define a function that is valid only over a certain interval or time period, you usually define the domain of the function. The scope of a function consists of all possible input values (x-values) for which the function is defined. For example, if you had a function $(f(x))$ defined over the interval $([a, b])$, you would write it as follows: $f(x), a \leq x \leq b$

This notation indicates that the function $(f(x))$ is defined for all values (x) between (a) and (b), including. The function may not be valid for values beyond this interval.

Example: Function $\boldsymbol{y = e^x}$ solves the equation.

4 Linear Differential Equation (1)

A linear differential equation is an everyday differential equation that may be written as:

$$\frac{dy}{dx}P(x)_y = Q(x)$$

where $(P(x))$ and $(Q(x))$ are functions of (x) and (y) is the established variable relative to the independent variable (x).

Linear differential equations are vital in arithmetic and physics due to their simplicity and nicely-understood traits. They have programs in one of a kind fields, along with engineering, economics, and biology [9].

It is stated that an equation is a linear one if:

- The applicable variable y and all its derivatives $y, \ldots, y^n$ are of first diploma

The relevant variable y and all of its derivatives are first diploma.

If the variable y and all of its derivatives are first order, which means that the equation is a first order linear ordinary differential equation. The popular form of the first-order linear ODE with this property may be written as [10]:

$$\frac{dy}{dx} \; P(x)_y = Q(x)$$

In this version, y and its first-order derivative with appreciate to x are, and $P(x)$ and $Q(x)$ are functions of x

- All equations $a_0(x), a_1(x), \ldots, a_n(x)$ are connected functions relying on the unbiased variable best.

If all equations are continuous functions that rely handiest on the impartial variable, this normally manner that the established variable and its derivatives are features of the independent variable most effective. This circumstance can simplify the evaluation of differential equations because the capabilities worried do no longer depend on any other variables. For example, within the case of a first-order linear regular differential equation wherein the dependent variable y is best a function of the unbiased variable x, the equation might seem like this:

$$\frac{dy}{dx} + P(x)_y = Q(x)$$

In this case, $P(x)$ and $Q(x)$ are functions of x only. This simplifies the equation and analysis as all terms only include the independent variable x.

Example: equation $x\frac{dy}{dx} + 2y = x^3$ is a linear one.

5 Non-linear Differential Equation (8)

Nonlinear differential equations do not necessarily follow the rule that the dependent variable and its derivatives are only functions of the independent variable. In non-linear differential equations, the dependent variable and its derivatives can be functions of other variables or even the dependent variable itself [11].

A common example of a nonlinear differential equation is the van der Pol oscillator:

$$\frac{d^2x}{dt^2} - \mu\frac{\left(1 - x^2\right)dx}{dt} + x = 0$$

In this non-linear differential equation, both x and its derivatives are capabilities of the unbiased variable t, but the presence of the x^2 term in the equation makes it non-linear. Nonlinear differential equations may be greater tough to investigate and resolve than linear differential equations due to the complexities supplied by the nonlinear terms.

Nonlinear differential equations have an extensive range of programs in numerous fields inclusive of physics, biology, engineering and economics. They regularly require numerical techniques or approximate techniques to resolve them [11].

They are differential equations whose relevant variable and its derivatives aren't of the primary degree or it's far accelerated via certainly one of its derivatives.

Example: equation $yy''y' = x$ is a non-linear one.

6 Homogeneous Differential Equation (2)

A homogeneous differential equation is a kind of normal differential equation in which all phrases may be expressed as a homogeneous function of the variables in question. In different phrases, a differential equation is homogeneous if it could be written as:

$$F\left(\frac{dy}{dx}, \frac{y}{x}\right) = zero$$

where (F) is a function that represents the relationship among the primary derivative of (y) relative to (x) and the ratio $\left(\frac{y}{x}\right)$.

Homogeneous differential equations frequently have the property that if $(y(x))$ is an answer, then $(\lambda y(x))$ is also a way to any regular$(\lambda \neq zero)$. This asset is an effect of the homogeneity of the differential equation.

One famous example of a homogeneous differential equation is:

$$x\left(\frac{dy}{dx}\right) = y$$

This equation is homogeneous because it is able to be expressed as a characteristic of the ratio $\left(\frac{y}{x}\right)$, i.E. $F\left(\frac{dy}{dx}, \frac{y}{x}\right)$

Homogeneous differential equations are often solved by performing a substitution, typically $(y = vx)$ and then solving for (v) in terms of (x). Substituting this in the original differential equation reduces it to a separable differential equation that can be solved using standard techniques [12].

A differential equation can be homogeneous when none of its limits has an independent variable only. Thus, the equation: $\sum_i^n = 0a_i(x)y_i + r_x = 0$ is a homogeneous if $r_x = 0$.

Example: equation $\frac{dy}{dx} + xr = 0$ is a differential homogeneous one.

7 Non-homogeneous Differential Equation (3)

A heterogeneous differential equation is an equation that can be written in the form:

$$\frac{dy}{dx} = f(x) + g(x) * y$$

where $(f(x))$ and $(g(x))$ are functions of (x) and the term $(g(x) \cdot y)$ is known as the non-homogeneous or influential term

A differential equation can be non-homogeneous when any of its limits has an independent variable only.

Examples: $\frac{dy}{dx} = x + sinx$ is a non-homogeneous differential equation.

8 Series (3)

A given series is written as such:

$$a_1 + a_2 + a_3 + \cdots + a_n + \ldots.$$

The sum of the series can be obtained by adding the limits a_1 to an whereas the infinite series is the generalization of the previous form and is written as follows:

$$a_1 + a_2 + a_3 + \cdots + a_n + \ldots.$$

And it is infinite in the sense that the partial sum of n order of the infinite series is written as follows:

$$S_n = a_1 + a_2 + a_3 + \cdots + a_n$$

$$\ldots\ldots S_3 = S_2 + a_3, S_2 = S_1 + aa, S_1 = a_1$$

The sum of the infinite series is clarified as follows:

$$S = \lim_{n\to\infty} S_n$$

or by the use of $\sum$ we can write:

$$\sum_{n=1}^{\infty} a_n = \lim_{n\to\infty} S_n$$

When the end of that series is unavailable then the sum is undefined.

For an infinite series, when the number of terms approaches infinity, we are concerned with finding the sum of the infinite series. The sum of an infinite series is represented by (S) and can be defined as the limit of the sequence of sub-sums (S_n) where (n) goes to infinity. Mathematically, this can be stated as follows [13]:

$$S = \lim_{n\to\infty} S_n = \lim_{n\to\infty} (a_1 + a_2 + \ldots + a_n)$$

If this restrict converges to a finite price (S), then the sum of the countless series is equal to (S). However, if the term varies or does now not exist, the sum of the infinite collection is taken into consideration indefinite.

Representing the usage of Σ(sigma) notation: In mathematics, we frequently use Σ (sigma) notation to represent collection concisely. The sum of the countless series may be written as:

$$\sum_{n=1\to\infty} a_n = a_1 + a_2 + a_3 + \ldots$$

This sigma notation represents in a compact form the phrases of a limitless collection starting from (a_1) and continuing to infinity.

Example:
Consider the geometric collection $1\frac{1}{2}\frac{1}{4}\frac{1}{8}$.... The nth term of this collection is given via.

The partial sum of the first (n) terms is:

$$S_n = \sum_{k=1ton} \frac{1}{2^{k-1}} = 1 + \frac{1}{2} + \frac{1}{4} + ... + \frac{1}{2^{n-1}} = 2 - \frac{1}{2^{n-1}}$$

As n approaches infinity, the limit of partial sums converges to 2. Thus, the sum of the infinite geometric series is $+\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + ...is\,2$

8.1 Index of Series (1)

In the context of mathematical series, the variable n represents the indicator or parameter that suggests the restrict of the series under consideration. It is a placeholder that may be changed by way of other letters consisting of (m) or (k) without changing the overall fee of the string; This property makes it a & quot; phantom indicator & quot; [14].

Here is an in-depth rationalization with an instance to make clear:

rationalization:

In arithmetic, the pointer (n) is used to suggest a selected term in a string. When calculating the sum of a sequence, the indicator (n) usually starts offevolved at a certain cost and advances in increments according to the pattern determined through the series.

Example:

Let's take an instance of an easy mathematics series:

$$[1 \;\; 2 \;\; 3 \;\; c \;\; .... \;\; N]$$

In this series, the pointer (n) represents the last time period of the collection. The sum of the series may be calculated using the mathematics collection sum system:

$$\left[S_n = \frac{n^2}{[2a(n-1)d]}\right]$$

in which:

(a) is the first term of the collection,
(d) is the commonplace difference between successive terms,
(n) is the wide variety of phrases in the series.

For instance, $(a = 1)$ (the first time period), $(d = 1)$ (the not unusual distinction), and we do not forget (n) terms. Substituting values into the formula, we can locate the sum of the collection.

Using dummy index:

Using (n) as a dummy indicator allows flexibility in representing string conditions. For example, we can easily replace (n) with (m) or (k) in the formula without changing the essence of the string calculation. Phantom pointers are common in mathematics to emphasize generality and flexibility in notation.

The variable upon which the addition process is achieved and appears in the clarification of the series as well as beneath the sum sign, as it is shown in the following series:

$$\sum_{n=0}^{n=100} \frac{n^2+1}{(n+1)!}, \sum_{n=1}^{\infty} \frac{(-1)n}{2nn!}, \sum_{n=\infty}^{\infty} C \text{ n e inks}$$

n represents the guide which can be changed into m or k without affecting the series value and thus it is called (Dummy Index). For example:

$$\sum_{k=0}^{\infty} \frac{2^k + x^k}{k!} = \sum_{n=0}^{\infty} \frac{2^n + x^n}{n!} = \sum_{m=0}^{\infty} \frac{2^m + x^m}{m!}$$

8.2 Some Sorts of Series

8.2.1 Power Series (1)

Power series can be logically defined as sequences which contain as components powers of a variable with coefficients in front of them. The general form of the force series is [15]:

$$f(x) = \sum_{from\, n=0 \to \infty} a_n * x^n$$

In this series:
(a_n) represents the coefficients,
(x) is the variable,
The sum ranges from $(n = 0)$ to infinity.

Features and Applications:
Convergence: Here the values are (x) while the coefficients are (a_n) and therefore convergence of a power series is dependent of these. It may be equal at particular value of x and different at others, or in other words; It may be equal at some values and at some other it might be infinite.

Function Representation: energy collection is usually depicted as features. There always exist some suitable coefficients such that feature can be represented as infinite sum of powers of x.

Analytical functions: Power collection is particularly useful for image analytic capacities because they can be utilized to estimate different aspects within a localized community around a particular aspect.

Example:
Consider a simple electricity collection of an exponential characteristic:

$$e^x = \sum_{from\, n=zero \to \infty} \frac{x^n}{n!}$$

In this energy collection, it suggests the parameter $\left(a_n = \frac{1}{n}\right)$ and the variable (x) raised to the strength (n). Substituting extraordinary values of (x) we will approximate the exponential character of strength series phrases.

Use in Mathematics:
Power series are Introduction to calculus analysis and a part of many other mathematical disciplines. They act as a strong means of approximations and representations of functions, calculation of given differential equations and analysis of functions behavior at particular points.

It is an infinite series that is formed as follows:

$$\sum_{n=0}^{\infty} a_n (x-c)^n$$

$$= a_0 + a_1(x-c) + a_2(x-c)^2 + a_3(x-c)^3 + \ldots$$

a^n represents the series coefficient and C represents the core (center).

In many cases $C = 0$ and leads to the facilitated series form:

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$$

For example, the power series

$$\sum_{n=0}^{\infty} x^n = 1 + x + x^2 + x^3 + x^n + \ldots$$

Is a geometrical series of an x base and is convergent when $|x| < 1$ and its sum is

$$S_n = \frac{1}{1-x}$$

This means

$$-1 < x < 1$$

$$\frac{1}{1-x} = 1 + x + x^2 + \cdots + x^n + \ldots$$

Both ratio and nth root tests can be used to find out x values that make the power series convergent.

To know the solution of an infinite series, we can compensate y and its derivatives in the equation

$$y'' + p(x)y' + p(x)y = 0$$

and the determination of a_n variables values by equalizing each variable of x ones with zero. (2)

Example 1 / Find the series convergent period (1)

$$\sum_{n=1}^{\infty}(-1)^{n-1}\frac{x^n}{n}$$

Solution

$$\left|\frac{a_n+1}{a_n}\right| = \left|\frac{x^{n+1}}{n+1}x\frac{n}{x^n}\right| = \left|\frac{n}{n+1}x\right|$$

$$\lim_{n\to\infty}\left|\frac{n}{n+1}x\right| = |x| < 1$$

To make sure that the series is convergent, it is necessary that $-1 < x < 1$ when $x = 1$ then the series becomes $\sum_{n=1}^{\infty}\frac{(-1)^n}{n}$ and it is convergent, but when $x = -1$, the series becomes

$$\sum\nolimits_{n=1}^{\infty}\frac{(-1)^{n-1}(-1)^n}{n}$$

$$\sum\nolimits_{n=1}^{\infty}\frac{(-1)^{2n-1}}{n} = -1-1-\frac{1}{2}-\frac{1}{3}-\ldots$$

and it is divergent, so the series convergent period is $-1 < x \leq 1$

Example 2. Find series convergent period (5). Solution

$$\left|\frac{a_n+1}{a_n}\right| = \left|\frac{x^{n+1}+1}{(n+1)!} * \frac{n!}{x^n}\right| = \left|\frac{n!x}{(n+1)n!}\right| = \left|\frac{x}{n+1}\right|$$

For the series to be convergent, the form needs to be:

$$\lim_{n\to\infty}\left|\frac{x}{n+1}\right| = 0 < 1\forall x \in R$$

Therefore, the series convergent period is

$$-\infty < x < \infty$$

8.2.2 Tylor Expansion (2)

Here are some popular types of series expansions [16]**:**

Taylor series: Recall that a Taylor's series is a way of representing function by an infinite series which is an asymptotic expansion of the function at point x = a made of derivatives of the function. Due to this, it gives a way of expressing a function as an endless polynomial.

Maclaurin Series: The Maclaurin series is a special case of the Taylor series where the series is expanded around zero. It is Taylor series of sorts with = 0.

Fourier Series: Fourier series divide a periodic characteristic into sine and cosine with particular frequencies. It is typically aliased in areas such as sign processing and wave assessment.

Power Series: An energy collection is an array of the shape $\Sigma(c_n * (x-a)^n)$ remains changeless and a is a constant. Power collection is used to denote functions in a neighborhood around a point.

These collection expansions are basic to arithmetic and discover packs in inexhaustible regions of science and designing. If you have a selected collection in mind or need more information on a certain type of collection do not hesitate to let us know.

This growth is used to solve the differential equations in the shape of a countless series with the aid of representing y(x) in the shape of a countless collection then express that inside the feature and its derivatives:

$$y, y', y'', y''', \ldots$$

To get the solution of the differential equation the usage of Tylor growth:

1. Tylor enlargement of $y(x)$ close to $x = x_0$ as follows:

$$y(x) = y(x_0) + (x - x_0)y'(x_0) + \frac{(x-x)^2}{2!}y'''(x_0) + \ldots$$

$$\sum_{k=0}^{\infty} \frac{(x - x_0)^k}{k!} y^k(x_0)$$

2. If we placed with Tylor enlargement, then we will get McLorin Expansion as follows:

$$y(x) = y(0) + xy'(0) + \frac{x^2}{2!}y''(0) + \frac{x^3}{3!}y'''(0) + \ldots$$

$$= \sum_{k=0}^{\infty} \frac{x^k}{k!} y^k(0)$$

Example 1 Find Tylor series e^x around $a = 0$ (5)

Solution:

$$f(x) = f\prime(x) = f''(x) = \cdots = f^n(x) = e^x$$

this includes:

$$f(0) = f\prime(0) = f''(0) = \cdots = f^n(0) = 1$$

Thus: ex = 1 +

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \cdots + \frac{x^n}{n!}$$

$$\sum_{n=0}^{\infty} \frac{x^n}{n!}$$

Example 2 Find Tylor expansion of sinhx around $x = 0$ (5)
Solution

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \ldots$$

by including $xat - x$

$$e^{-x} = 1 - x + \frac{x^2}{2!} - \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!} + \ldots$$

Thus

$$\sin hx = \frac{e^x - e^{-x}}{2}$$

$$= x + \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots$$

$$\sum_n^{\infty} \frac{x^{2n+1}}{(2n+1)!}$$

8.3 Solving Differential Equations with the Aid of Collection Method (Three)

Higher-order differential equations have a critical role in several medical uses and can solve characteristics that normal procedures almost couldn't undertake. For example, linear and nonlinear differential equations with variable coefficients of 2d order in their parameters pose problems which are solved using specific approaches to eliminate [15, 16].

Thus, the string method comes to the foreground as a useful method for solving such a kind of differential equations. It is necessary to emphasize that the method doesn't work as a universal or most efficient one; however, it is an effective tool in solving some kinds of problems that cannot be solved with other methods.

Let's consider an illustrative example: The string method of solving a given differential equation can provide fast track ways of thinking which conventional methods can't provide.

Example 1 A first order differential Equation (3)

$$xy'' + y' + xy = 0$$

Solution:
We also suppose that the solution of this problem is an infinite series.

$$y = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + \ldots$$

$$y' = a_1 + 2a_2 + 3a_3a^2 + 4a_4a^3 + \ldots$$

$$y'' = 2a_2 + 6a_3 + 12a_4a^2 + \dots$$

$$xy = a_0x + a_1x^2 + a_2x^3 + a_3x^4 + a_4x^5 + \dots$$

$$xy'' = 2a_2x + 6a_3x^2 + 12a_4x^3 + 20a_5x^4 + 30a_6x^5 + \dots$$

we put similar limits under one column to facilitate the solution

$$y'' = y' + xy = a_1 + (a_0 + 4a_2)x + (a_1 + 9a_3)x^2 + (a_2 + 16a_4)x^3 + \dots$$

since it is convergent, so by putting the coefficients equal to zero

$$a_1 = 0, a_2 = -\frac{a_0}{4}, a_3 = -\frac{a_1}{9} = 0, a_4 = \frac{a_2}{16} - \frac{a_0}{4.16}$$

so, we get

$$a_1 = a_3 = a_5 = \dots = 0$$

Also, it could be written as such:

$$y = a_0(1 - \frac{x}{2^2} + \frac{x^2}{2^2.4^2} - \frac{x^6}{2^2.4^2.6^2} + \dots)$$

Example 2 solve the equation (6)

Solution

Assuming that point x = 0 is an ordinary point in the differential equation

$$y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots$$

and so

$$y' = \sum_{n=1}^{\infty} na_n x^{n-1} = a_1 + 2a_2x + 3a_3x^2 + 4a_3x^3 + \dots$$

thus, the differential equation is

$$a_1 + 2a_2x + 3a_3x^2 + \dots = 2x(a_0 + a_1x + a_2x^2 + \dots)$$

$$\rightarrow a_1 + 2ax + 3a_3x^2 + 4a_4x^3$$

$$= a_0x + 2a_1x^2 + 2a_2x^3 + \dots$$

and by equalizing the coefficients of $\boldsymbol{x}$ various power with the zero, we get:

$$a_1 = 0, a_2 = a_0, 3a_3 = 2a_1 \rightarrow a_3 = 0$$

$$a_4 = \frac{a_2}{2} = \frac{a_0}{2!}, a_5 = 0, a_6 = \frac{a_4}{3} = \frac{a_0}{3!}$$

so, the solution of the equation will be as such:

$$y = a_0 + a_0 x^2 + \frac{a_0}{2!}x^4 + \frac{a_0}{3!}x^6 + \ldots$$

$$= a_0\left[1 + x^2 + \frac{x^4}{2!} + \frac{x^6}{3!} + \ldots\right] = a_0 e^{x^2}$$

Example 3 solve the following series equation: $y' + 3x^2 y = 1$
Solution.
We assume that the solution is:

$$y = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \ldots \tag{1}$$

$$y' = c_1 + 2c_2 x + 3c_3 x^2 + \ldots \tag{2}$$

By applying (1) in (2) in the original equation, i.e. we get:

$$(c_1 + 2c_2 x + 3c_3 x^2 + \ldots)$$

$$+\left(3c_0 x^2 + 6c_2 x^3 + 9c_3 x^4 + \ldots\right) = 1$$

$$c_1 + 2c_2 x + (3c_3 + 3c_0) + x^2 + (4c_4 + 3c_1)x^3 + \cdots =$$

$$c_1 = 1, 2c_2 = 0, \rightarrow c_2 = 0$$

$$3c_3 + 3c_0 = 0 \rightarrow c_3 = -c_0$$

$$4c_4 + 3c_1 = 0 \rightarrow c_4 = \frac{-3}{4}$$

By applying $\boldsymbol{c}_1$ values in the above solution (1) we get:

$$y = c_0 + x - c_0 x^3 - \frac{3}{4}x^4 + \ldots$$

$$y = c_0\left(1 - x^3 + \ldots\right) + (x - \frac{3}{4}x^4 + \ldots)$$

And this is the needed solution.

Example 4 solve the following series of the differential equation $y'' + y = 0$ using the period:

$$-\infty < x < \infty \tag{3}$$

Solution
Tylor series about $x_0 = 0$ is:

$$y = \sum_{n=0}^{\infty} a_n x^n$$

So, the second derivation 0 this series is:

$$y = a_0 + ax + a_2x^2 + a_3x^3 + \cdots + a_nx^n = \sum_{n=0}^{\infty} a_n x^n$$

$$y' = a_1 + 2a_2x + 3a_3x^2 + 4a_4x^3 + \cdots + na_nx^{n-1} = \sum_{n=1}^{\infty} na_n x^{n-1}$$

$$y'' = 2a_2 + 6a_3x + 12a_4x^2 + 20a_5x^3 + \cdots + n(n-1)a_nx^{n-2} = \sum_{n=2}^{\infty} n(n-1)a_n x^{n-2}$$

from those series

$$y'' + y = 0 \rightarrow \sum_{n=2}^{\infty} n(n-1)a_nx^{n-2} + \sum_{n=0}^{\infty} a_n x^n = 0$$

$$\sum_{n=0}^{\infty} \left[(n+2)(n+2)a_{n+2} + a_n\right]x^n = 0$$

the right part is zero and all of the coefficients on the left part have to be zero, so:

$$a_2 = -\frac{a_0}{1 \times 2} = \frac{1}{2!}a_0$$

$$a_3 = -\frac{a_0}{1 \times 2 \times 3} = -\frac{1}{3!}a_0$$

$$a_3 = -\frac{a_2}{3 \times 4} = \frac{1}{4!}a_0$$

$$a_5 = -\frac{a_3}{4 \times 5} = \frac{1}{5!}a_1$$

$$a_n = a_2k = (-1)^k \frac{1}{(2k)!}a_0$$

$$a_n = a_{2k+1} = (-1)^k \frac{1}{(2k+1)}a_1$$

if we put those coefficients in the series:

$$y = a_0 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_nx^n = \sum_{n=1}^{\infty} a_n x^n$$

then we get the answer of the equation:

$$y = a_0 \sum_{n=0}^{\infty} (-1)^n \frac{1}{(2n)!} x^{2n} + a_1 \sum_{n=0}^{\infty} (-1)^n \frac{1}{(2n+1)!} x^{2n+1}$$

those series are:

$$y = a_0 cosx + a_1 sinx$$

Coefficients a_0, a_1 are integration constants.
Example 5/solve the following differential equation $y' - y = 0$ (2).
Solution
By presuming that the differential equation's point $x = 0$ is an ordinary point:

$$y = \sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots$$

$$\mathrm{y''} = \mathrm{a_1} + 2\mathrm{a_2 x} + 3\mathrm{a_3 x^2} + 4\mathrm{a_4 x^3} + \cdots = \sum_{\mathrm{n=1}}^{\infty} \mathrm{n a_n x^{n-1}}$$

Thus, we applying y, y' in the differential series $\mathrm{y'} - \mathrm{y} = 0$ we get:

$$a_1 + 2a_2 x + 3a_3 x^2 = \cdots - (a_0 + a_1 x + a_2 x^2 + \ldots)$$

$$\therefore (a_1 - a_0) + (2a_2 - a_1)x + (3a_3 - a_2)x^2 + \cdots = 0$$

by equalizing x power coefficients with zero, we get:

$$a_1 - a_0 = 0 \rightarrow a_1 = a_0$$

$$2a_2 - a_1 = 0 \rightarrow a_2 = \frac{a_1}{2} = \frac{a_0}{2!}$$

$$3a_3 - a_2 = 0 \rightarrow a_3 = \frac{a_2}{2} = \frac{a_0}{2!} \Big/ 3 = \frac{a_0}{3!}$$

so, the solution of the differential equation is as follows:

$$y = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots = a_0 + [a_0]x + \frac{a_0}{2!} x^2 + \frac{a_0}{3!} x^3 + \ldots$$

$$= a_0 \left[1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \ldots \right] = a_0 e^x$$

The real-world uses of Ordinary Differential Equations (ODEs)
Differential equations are central in the study of various event occurrences in the real worlds. Below are some examples:

Population Growth: It is possible to use first-order ODEs to model population depending on the type using logistic growth equation shown below;

$$\frac{dP}{dt} = rP\left(1 - \frac{P}{K}\right)$$

Hence, P = rK and P(t) = K when t = log r, r being the growth rate of the population; K the carrying capacity.

Heat Conduction: The heat equation is a PDE that describes the heat distribution in a material in a specific time:

$$\frac{\partial u}{\partial t} = k\frac{\partial^2 u}{\partial x^2}$$

where $u(x, t)u(x, t)u(x, t)$ represents the temperature at time t and position xxx, and k is the thermal conductivity.

Including these examples also shows that ODEs and PDEs can be used to solve problems that exist in biology and engineering disciplines.

It is known as the String Method because the string of relationships created by the links between two groups is confined to one's relationships alone.

The string method is a method for determining the solution of some differential equations when the solution is assumed to be expressed in terms of an infinite series. The method involves expansion of the function in question into a power series and then substituting this series to give the differential equation. The terms are equated to zero so as to find out the coefficients of the series.

For example, consider the differential equation:

$$xy'' + y' + xy = 0$$

We assume a solution of the form $y = a0 + a1x + a2x2 + \ldots$, substitute it into the equation, and solve for the coefficients a_n.

Prickle 4,061,869 Partial Differential Equations (PDEs) & Nonlinear Ordinary Differential Equations (ODEs).

Although the paper mostly deals with the linear ODEs, it is also necessary to note other classes of equations. A PDE is the equation containing partial derivatives in more than one variable and is used numerous scientific fields like physics and mechanical engineering for example in studies of heat conduction or fluid flow.

Similarly, nonlinear ODEs, such as the Van der Pol oscillator:

$$\frac{d^2x}{dt^2} = \mu\left(1 - x^2\right)\frac{dx}{dt} + x = 0$$

explain even more elaborate processes that exhibit behaviors in theme of chaos and bifurcation.

Providing Proof of Convergence:

In several sections this paper uses power series solutions of the governing equations in

which convergence is assumed. Nevertheless, this needs validation. The sum ability of power series can be done by the ratio test and the root test. For example, for a series:

$$\sum a_n x^n$$

the series converges if:

$$\lim_{n\to\infty}\left|\frac{a_{n+1}}{a_n}\right| < 1$$

This condition helps determining the radius of convergence for the series so that solution's outcomes do not trigger mathematical contradictions.

9 Conclusion

In other words, math in this paper concerns the analysis of a subset known as ordinary differential equations (ODEs). ODEs play a central role in analyzing dynamical systems in many sciences as a result of their features. In Math's, beginning with Newton and his contemporaries, up to the present day, differential equations have been found to be of great help in solving algebraic and geometry problems, as well as real life physical problems.

Study of solutions of ordinary linear differential equations shows a mathematical series and presents the procedure of interactions between theory and application. With ODE solutions, we propose to implement the correlation between theory and practice in mathematics, thus opening the door for improvements in approach to problem-solving tools and methods as well as models.

References

1. Ismaeel, B., Aish, A.: Differential Equations, solutions and applications. Sconce and Technology University, Yemen Republic (2008)
2. Bikheet, N., Almatrafi, A.A.: Differential Equations: Theory and Application. Scientific Publication Administration, Altaif University, Taif, Saudi Arabia (2012)
3. Bronstein, M.: Computer algebra algorithms for linear ordinary differential and difference equations. In: Proceedings of the Third European Congress of Mathematics, vol. II. Progress in Mathematics, vol. 202, Birkhäuser, Basel, pp. 105–119 (2001). https://doi.org/10.1007/978-3-0348-8355-3_10
4. Kamke, E.: Differentialgleichungen: Lösungsmethoden und Lösungen. Akademische Verlagsgesellschaft, Leipzig (1956)
5. Kamran, N., Olver, P.: Equivalence of differential operators. SIAM J. Math. Anal. **20**(5), 1172–1185 (1989). https://doi.org/10.1137/0520076
6. Abramov, S.A., Barkatou, M.A.: Computable infinite power series in the role of coefficients of linear differential systems. In: Gerdt, V.P., et al. (eds.) Computer Algebra in Scientific Computing: 16th International Workshop, CASC 2014, Warsaw, Poland, September 8–12, 2014, Proceedings, pp. 1–12. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-10515-4_1

7. Abramov, S.A., Barkatou, M.A., Khmelnov, D.: On full rank differential systems with power series coefficients. J. Symb. Comput. **68**(1), 120–137 (2015). https://doi.org/10.1016/j.jsc.2014.08.010
8. Abramov, S.A., Barkatou, M.A., Pflügel, E.: Higher-order linear differential systems with truncated coefficients. In: Gerdt, V.P., et al. (eds.) Computer Algebra in Scientific Computing: 13th International Workshop, CASC 2011, Kassel, Germany, 5–9 September 2011, Proceedings, pp. 10–24. Springer, Heidelberg (2011). https://doi.org/10.1007/978-3-642-23568-9_3
9. Abramov, S.A., Bronstein, M., Petkovšek, M.: On polynomial solutions of linear operator equations. In: ISSAC 1995: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, Montreal, Canada, 17–19 July 1995, pp. 290–296 (1995). https://doi.org/10.1145/220346.220384
10. Abramov, S.A., Khmelnov, D.E.: Regular solutions of linear differential systems with power series coefficients. Program. Comput. Softw. **40**(2), 98–106 (2014). https://doi.org/10.1134/S0361768814020029
11. Abramov, S.A., Ryabenko, A.A., Khmelnov, D.E.: Procedures for searching local solutions of linear differential systems with infinite power series in the role of coefficients. Program. Comput. Softw. **42**(2), 55–64 (2016). https://doi.org/10.1134/S036176881602002X
12. Barkatou, M.A.: Rational Newton algorithm for computing formal solutions of linear differential equations. In: Gianni, P. (ed.) ISSAC '88: International Symposium on Symbolic and Algebraic Computation, Rome, Italy, 4–6 July 1988. LNCS, vol. 358, pp. 183–195. Springer, Heidelberg (1989). https://doi.org/10.1007/3-540-51084-2_17
13. Hassan, M., Alouwaidhi, A.A.R.: Differential Equations, Part 1. Alazhar University, Sana'a, Yemen (2010)
14. Jalal, A.: Ordinary and Partial Differential Equations. Winter Library (2008)
15. Ramadhan, M., Ahmed, A.: Calculus, Part 2, 3rd edition. Alkitab Press, Alhareer United, Baghdad, Iraq (2002)
16. Ince, E.L.: Ordinary Differential Equations. Longmans, London, New York, Bombay (1926)
17. Bronstein, M.: Computer Algebra Algorithms for Linear Ordinary Differential and Difference Equations. European Congress of Mathematics, Basel (2001). https://doi.org/10.1007/978-3-0348-8355-3_10



Perception of Chat AI on Writing Skills Among Literature Teacher Students: A Study at Hanoi Pedagogy University 2, Vietnam

Chung Kim Pham [1(✉)], Hang Thi My Duong[2], and Hang Thi Thu Nguyen[3]

[1] University of Education, VNU, Hanoi, Vietnam
chungpk@vnu.edu.vn
[2] Hanoi Pedagogy University 2, Hanoi, Vietnam
duongthimyhang@hpu2.edu.vn
[3] University of Fire Prevention and Fighting, Hanoi, Vietnam
chihang880@gmail.com

Abstract. The impact of technology and artificial intelligence, especially Chat AI, is becoming increasingly evident in many aspects of human life, including education. Using Chat AI can support text creation, but it also has concerns that it negatively affects students' writing ability and raises ethical and academic issues, especially for literature pedagogy students, who will teach high school students to create texts. This study aimed to investigate the impact of Chat AI on text construction in pedagogy students. The study used qualitative methods and questionnaires based on the technology acceptance model (TAM). Data were collected from 152 students at Hanoi University of Education 2, Vietnam. Data were analyzed according to the suggested themes using the TAM. The results indicated that students found Chat AI useful and easy to use, and had positive attitudes toward its use in writing. This shows a connection between students' intentions to use Chat AI and their behavior. Furthermore, some students recognized the potential negative consequences of Chat AI on writing quality and academic ethics. These findings add to the theory and practice of Chat AI in writing and provide a foundation for educators to develop effective strategies for managing and using it.

Keywords: Chat AI · Technology acceptance Model · Higher education · writing competence · literature teacher student

1 Introduction

Technology and artificial intelligence (AI) have exerted an increasingly profound influence on all aspects of human life, including education. The introduction of Chat AI by OpenAI in November 2022 has made it a widely used tool in the education sector. Chat AI is a type of AI that enables the creation of automated conversations and answers to questions on various topics and fields. With user input, the tool can generate coherent

D. T. M. Hang—PhD student of University of Education, VN

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 360–373, 2025.
https://doi.org/10.1007/978-3-031-91008-1_32

responses and provide information similar to that of humans (An, J., Ding, W., & Lin, C. (2023). Chat AI can assist learners in the learning process (Punar Özçelik, Yangqin Ekşi, G, 2024) [1]).

This research examines the influence of Chat AI on the writing skills of literature pedagogy students at the Hanoi University of Pedagogy 2, Vietnam. Chat AI presents several opportunities, ideas, and innovative methods to enhance teaching techniques. As an essential educational tool, Chat AI benefits both students and educators, particularly by improving learners' writing abilities and fostering interactive learning environments (Abderahman Rejeb et al., 2024). According to a study by Ali et al. (2023), Chat AI supports the development of reading and writing skills among learners, motivates them, and encourages a positive attitude towards its use. Rather than focusing on the potential negative consequences, Chat AI should be perceived as a valuable learning resource. The AI tool can assist researchers in composing well-structured, factually accurate, informative, and systematic articles (Zhai, X. (2022). Additionally, Chat AI offers support for finding creative inspiration or new ideas for artistic job opportunities (Zhu, Zheng Wang et al. (2024) [2]. Students can use smartphones to scan text on paper and have the CHAT AI rewrite it. However, optical character recognition remains a challenging task for accurately recognizing text from images [3].

However, Chat AI raises worrying issues, such as creativity, ethics, academic integrity, information accuracy, and learners' sense of ego. Baron, N. S. (2023) believes that learners can passively recognize the boundary between supporting writing and letting AI take over both content and tone completely. Some issues related to the use of Chat AI, such as fraud, dishonesty, misleading privacy, and manipulation, have also been mentioned (Tlili, et al. (2023) [6, 7, 9]. Johanna Fleckenstein et al. (2023). Johanna Fleckenstein et al. (2023). 2024) suggests that Chat AI's feature allows the creation of texts that may otherwise be undetectable to teachers. This poses a challenge for the assessment of student essays in schools and university universities [4].

To address this problem, studies have been conducted on the effects of Chat AI on learners' writing skills. However, in Vietnam, there is still no specific assessment of the impact of Chat AI on the activity of learners, especially those majoring in Literature Education. This study focuses on perception of literature teacher students about using Chat AI when writing.

2 Literature Review

2.1 Writing Competence

Document creation is not only important in an academic environment but is also an essential skill in many different job fields, from management, marketing, to communications and many other professions [4].

Document creation ability refers to the ability to write and edit various types of documents effectively and accurately. This competency includes many skills, such as planning, organizing ideas, selecting words, and editing and perfecting documents [5, 6]. The components are listed in Table 1.

Table 1. Specific component document-creation competences.

Skill	Describe
Skills in planning and organizing ideas (C1)	Before starting to write, the writer needs to determine the purpose of the text, the audience, and the main ideas to be presented. Outlining can help organize ideas in a logical and coherent way
writing skill (C2)	This is the ability to express ideas in clear and concise words. This includes using appropriate grammar, vocabulary and writing style appropriate to the text type and audience
Skills in editing and completing documents (C3)	After writing, the writer needs to reread and edit to improve sentence structure, remove spelling and grammar errors, and ensure the text is coherent and easy to understand
Understanding of different types of texts (C4)	Each type of document (for example: administrative documents, reports, letters, academic articles, etc.) has its own requirements and structure. Writers need to clearly understand these requirements to create appropriate documents
Skills in using support tools (C5)	Tools such as word processing software, spell checkers, grammar checkers and reference sources are very helpful in writing and perfecting documents

Text creation ability can be divided into many different levels, from basic to advanced, based on the complexity of the text and level of proficiency of the writer. The Council of Europe's Language Competency Framework (CEFR; Common European Framework of Reference for Languages) is widely used to describe learners' language competence, including six levels from A1 (beginner) to C2 (proficient), and can be applied to writing along with other language skills, such as listening, speaking, and reading [7, 8]. The language competency framework according to the National Assessment of Educational Progress (NAEP) standards provides 5 levels proposed by many different organizations and systems. Writing competency framework of the Ministry of Education and Training of Vietnam, applied in general education. However, another popular system with a 5-level structure Level 1 - Beginner (Basic), Level 2 - Intermediate (Beginner), Level 3 - Good (Average), Level 4 - Good (Fair), Level 5 - Professional (Advanced). Below is a detailed description of these levels in Table 2:

Table 2. Level of writing competence

Level	Describe
Basic (Level 1)	• Use simple language and sentence structure • Little to no spelling and basic grammar errors • The text may not be well organized and may lack coherence and logic
Medium (Level 2)	• Richer language and diverse sentence structures • The text has a clear structure, main ideas are presented coherently • Few spelling and grammar errors, know how to do basic self-editing
Good (Level 3)	• Ability to draft complex and in-depth documents, such as research reports, dissertations, and specialized articles • Use specialized language and more complex sentence structures • The text is well organized, arguments and evidence are arranged logically and convincingly, appropriate to the type of text and target audience
Advanced (Level 4)	• Language is precise, rich, and demonstrates deep understanding of the subject • The text has a strict structure, sharp arguments and convincing evidence • Ability to self-edit and complete text meticulously, with few or no errors
Expert (Level 5)	• Ability to use language delicately, artistically and effectively • The text is tight, convincing, and has the ability to inspire • Ability to edit, publish and review the writing of others

The ability to create texts is a skill that develops over time and through regular practice. Writers can progress from a basic level to an expert level through learning, practicing, and gaining experience.

Students' ability to create texts is reflected in the ability to apply comprehensive knowledge of text types, with awareness and love of Vietnamese, literature, culture, and practical skills to create texts, in different modes of expression, in the form of presentation or writing [9].

In the process of guiding students to interact with texts, Literature helps students gradually form and improve the learning abilities of the subject, specifically the ability to receive texts (including listening skills, reading) and text creation ability (including speaking and writing skills). Students' ability to read and understand text is reflected in the ability to apply general knowledge about Vietnamese, types of texts and skills, reading methods, ability to collect information, and perceive the beauty and value of literary and artistic works.

2.2 AI in Text Writing

The impact of Chat AI on speaking education has been a topic of interest in recent literature. Lo (2023), Charles Alves de Castro (2023) conducted a rapid review of the

literature to explore Chat AI's capabilities across subject areas and its potential for use in education. The findings show that Chat AI's performance varies across different subjects, from excellent to unsatisfactory [10, 11].

For learners' text writing, Chat AI has an impact on various text-related aspects. Bishop (2023) and colleagues examined the ramifications of Chat AI in the fields of education, research, and writing, highlighting its potential advantages in these areas. Casal et al. (2023) explored ethical considerations related to the ability to distinguish between Chat AI/AI-generated content and human-generated material, especially in the field of academic publishing. The trend of individuals with a college education is engaging in the creation of written articles. According to Zhao (2024) et al., learners often use Chat AI, among other tools, often in a personalized manner, to address the specific writing obstacles they encounter. The main problems they face are related to plagiarism, inaccurate data, and dependence on technology. Mahapatra (2024) and colleagues found a significant positive impact of Chat AI on students' academic writing skills, and students' perceptions of this impact were also extremely positive. The study strengthens and advances the theories of feedback as a dialogue tool and Chat AI as a reliable and practically meaningful writing tool [12].

In addition, there have been studies that have identified concerns about the risks associated with using Chat AI to write academic papers (Y. Balel (2023). Some findings show an adverse association between the use of Chat AI and creative writing ability of university students, this tool has an impact on originality, students' content presentation, accuracy, and elaboration in writing [13].

Evaluating the usability and acceptance of Chat AI among students in different studies is also an issue of interest to researchers. The Technology Acceptance Model (TAM) was used to study the impact of Chat AI on writing and evaluate students' perceptions of Chat AI in writing tasks. S. Wagholikar et al. (2023) found acceptance among scholars who were uncertain about how Chat AI could transform education and evaluation of assessments. Aiming to evaluate student perspectives on Chat AI adoption, Paul Juinn Bing Tan (2024) used the TAM framework to identify seven key predictors and build a model to predict behavioral intentions and Actual usage of Chat AI Similarly, Yarnaphat Shaengchart (2023) conducted an assessment of intention to use TAM and Chat AI, emphasizing the importance of understanding user perceptions and intentions when implementing AI technologies like Chat AI. Saif (2024) and colleagues also identified Chat-GPT's ease of use and AI-generated text-related usefulness as contributing to students' positive attitudes towards using Chat-GPT. GPT and also plays a role in reducing their stress levels [14–16].

Overall, the literature surrounding Chat AI, text, and TAM emphasizes the importance of user acceptance, perceived usefulness, and potential challenges associated with integrating AI technologies such as Chat AI into many different contexts. These studies provide valuable insights into the implications of using Chat AI for writing tasks and highlight the need for further research into user attitudes and behaviors towards the tools. AI-powered text generation [17].

Above are some studies on the impact of Chat AI on students' writing ability. Further research is needed to fully understand the impact of Chat AI on different fields, especially on teacher training to guide responsible use. As the use of Chat AI continues to grow,

there is a need for research exploring their impact on different industries, specifically teacher education industries [18].

2.3 The Study

To address this problem, studies have been conducted on the effects of Chat AI on learners' writing skills. However, in Vietnam, there is still no specific assessment of the impact of Chat AI on the activity of learners, especially those majoring in Literature Education. This article focuses on surveying the impact of Chat AI on text creation of Literature pedagogy students. The research question that the author needs to address is:

1) Usefulness of Chat AI in writing Vietnamese text.
2) Behavioral intention to use.
3) Attitude of using Chat AI of Literature pedagogy students when writing Vietnamese documents.

3 Research Methods

3.1 Design and Participants

The research method applied in investigating and evaluating the impact of Chat AI on the writing ability of literature pedagogy students is a qualitative method. The research was conducted through a process consisting of stages. Initially, participating students engaged in a case-based learning task in which they used Chat AI to create written articles (Table 1). Then, a survey questionnaire followed the TAM model of Davis, FD (1989). To evaluate the impact of Chat AI on the text writing ability of literature pedagogy students is designed. Questions focus on the key concepts of TAM: Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Attitude Toward Using (ATT), Behavioral Intention to Use (BI) and Actual System Use (AU) [16–18]. Respondents indicated their level of agreement with every item by recording their answers on a 5-point Likert scale ranging from "1" (Strongly Disagree) to "5" (Strongly Agree). We used a convenience sampling method to select 152 student participants from the Faculty of Literature of Hanoi Pedagogy University 2. Participants were selected based on their willingness and voluntary consent.

Detailed survey questions are in the table Table 3.

3.2 Practicum Design

The study was conducted with 152 students majoring in Literature Education, divided into 3 groups: Group 1 from January 1, 2023 to March 15, 2023 with 58 students; Group 2 from June 2023 to July 2023 with 42 students, group 3 from April 9, 2024 to April 14, 2024, 52 students participated in learning about Chat AI applications in writing documents. Because students still have to follow the credit schedule, learning to apply Chat AI to writing documents is organized through 06 sessions in 3 weeks, including 01 theory session and 05 sessions practice session. The duration of each lesson is 45 min (Table 4).

Table 3. Survey questions follow the TAM model.

No	Survey questions
1.	I use Chat AI to write texts at least once a week
2.	I often use Chat AI to find ideas and structures for articles
3.	Chat AI helps me improve my writing skills
4.	Chat AI helps me complete writing assignments faster
5.	Chat AI helps me develop better writing ideas
6.	Chat AI is easy to use for me
7.	I easily learned how to use Chat AI to write text
8.	Chat AI does not require much effort to use
9.	I like to use Chat AI to assist with text writing
10.	Using Chat AI makes writing text more enjoyable for me
11.	I plan to continue using Chat AI to assist with writing in the future
12.	I will recommend Chat AI to my classmates for text writing support

Table 4. Students' learning tasks about applying Chat AI to text writing

Date	Topic	Content	Exercise
1	Introducing the theory of Chat AI through related documents	Learn about Chat AI	Collect documents about Chat AI application in writing documents
2	Practice writing unused text using Chat AI (1st time)	Demonstrate skills in writing a number of informational, descriptive, argumentative texts, etc.	Write some informational, descriptive, argumentative texts, etc. (1st time)
3	Practice writing text based on Chat AI application (2nd time)	Use GPT chat knowledge to complete articles with certain topics that the teacher provided in the 3rd lesson	Write texts with certain topics that the teacher provided in the 3rd lesson using Chat AI tool (2nd time)
4	Discuss the results of documents before and after using Chat AI	Discuss and compare similarities and differences between the first and second documents	Compare the similarities and differences between the first text and the second text
5	Cross-review the text (without using Chat AI) and using Chat AI	Evaluate the first and second text Evaluate whether or not to use Chat AI	Comment and evaluate your work (1st and 2nd time) Comment and rate your work using Chat AI (1st and 2nd time)
6	How to use Chat AI effectively in writing documents	How to combine Chat AI into text writing	Self-study and practice writing

4 Research Results

4.1 Analyze Demographic Data

The study included 152 student participants (N = 152) and included individuals between the ages of 20 and 22. Regarding gender distribution, the majority of participants identified as female (n = 47, 90.4%), while a smaller proportion identified as male (n = 5, 9.6%).

Among the participants, a large number of students confirmed that they used Chat AI for studying (n = 34; 65.4%). Some participants confirmed that they had no knowledge about Chat AI (n = 21; 40.4%).

4.2 Data and Analysis

After teaching the experiment to 152 students at Hanoi Pedagogy University 2, Vietnam, we observed the students' behaviors and student articles and evaluated them according to according to the criteria in the Table 5, as shown in Table 3 below.

Table 5. Results of experimental assessment of students' writing competence.

	C1		C2		C3		C4		C5	
	No	%	No	%	No	%	No	%	No	%
L1	18	12%	27	18%	23	15%	27	18%	25	16%
L2	46	30%	48	32%	60	39%	44	29%	40	26%
L3	78	51%	93	61%	63	41%	72	47%	75	49%
L4	140	92%	80	53%	104	68%	128	84%	136	89%
L5	140	92%	115	76%	125	82%	100	66%	105	69%

The results of Table 3 show that over 76% of students reached L3. While C4 and C5 competencies are the lower (66% reach L5).

To evaluate students' acceptance of ChatGT, the study surveyed students' opinions according to the TAM model with questions in Table 4. Analyze reliability coefficient Cronbach's Alpha on SPSS, coefficient is 0,850, It is guaranteed reliability.

Reliability Statistics	
Cronbach's Alpha	N of Items
,850	12

Descriptive Statistics of student feedback after using Chat AI to write using SPSS in the Table 6.

Table 5 shows that Item 10 has the lowest average value (Mean is 2,85). In particular, Item 7 "I easily learned how to use Chat AI to write text" has the highest average value (Mean is 3,11).

Table 6. Descriptive Statistics of student feedback after using Chat AI to write.

	N	Mean	Std. Deviation
1. I use Chat AI to write texts at least once a week	152	3,19	1,351
2. I often use Chat AI to find ideas and structures for articles	152	2,86	1,367
3. Chat AI helps me improve my writing skills	152	2,97	1,435
4. Chat AI helps me complete writing assignments faster	152	3,07	1,403
5. Chat AI helps me develop better writing ideas	152	2,86	1,428
6. Chat AI is easy to use for me	152	3,07	1,463
7. I easily learned how to use Chat AI to write text	152	3,11	1,358
8. Chat AI does not require much effort to use	152	3,07	1,372
9. I like to use Chat AI to assist with text writing	152	2,97	1,369
10. Using Chat AI makes writing text more enjoyable for me	152	2,85	1,422
11. I plan to continue using Chat AI to assist with writing in the future	152	2,93	1,415
12. I will recommend Chat AI to my classmates for text writing support	152	2,89	1,379
Valid N (listwise)	152		

5 Results and Discussion

Based on the analysis of the results of assessment of document creation capacity through case studies according to the research implementation plan in Table 4, with the statistical results in the Table 5, draw a chart Fig. 1 to answer the question. Question research: Is GPT Chat useful for the ability to create Vietnamese documents?

Most abilities develop to L4 and L5 levels, which proves that Chat AI has helped students demonstrates deep understanding of the subject, strict structure, sharp arguments and convincing evidence and edit and complete text meticulously, with few errors (Fig. 1).

In which capacity develops the most is “Skills in planning and organizing ideas (C1)” (sharp corner of the graph). Writing skill is only at level 3. This means that Chat AI only helps students at an average level with skills to draft complex documents, use specialized language and more complex sentence structures and organize documents, arguments and evidence appropriate to the type of text and target audience.

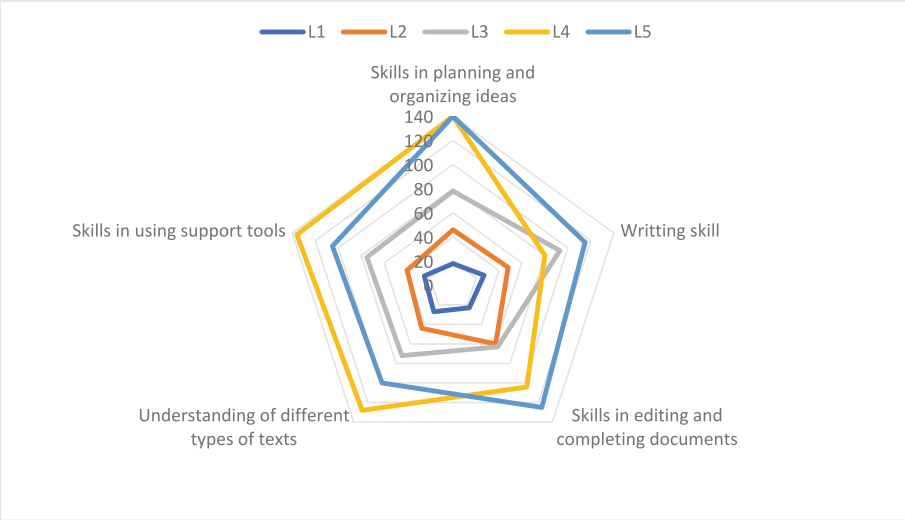


Fig. 1. Diagram of the components of students' writing competence after the experiment

Based on survey results to answer the research question about behavioral intention to use and attitude of using Chat AI of Literature pedagogy students when writing Vietnamese documents. From Table 6 show that students use Chat AI quite often (Mean 3,19). This shows that social media has quickly popularized and created an impact on students in using technology to create texts.

However the use of Chat AI to to find ideas and structures for articles (Mean 2,86) and me improve student writing skills (Mean 2,97) is still low. The results show that, for literature students, Chat AI's suggestions are not effective for articles with in-depth writing that requires creativity. Frequency of use is just 17% to 22% (Table 7 and Fig. 2).

Table 7. Item frequency statistics "Chat AI helps me develop better writing ideas"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	34	22,4	22,4	22,4
	2	36	23,7	23,7	46,1
	3	27	17,8	17,8	63,8
	4	27	17,8	17,8	81,6
	5	28	18,4	18,4	100,0
	Total	152	100,0	100,0	

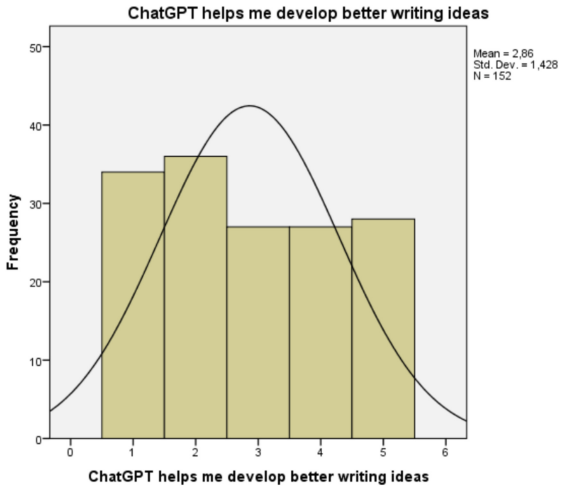


Fig. 2. Diagram of the frequency statistics "ChatGPT helps me develop better writing ideas"

Question asked "Does Chat AI Chat develop writing skills of student?". From item 3 analysis show that only 22,4% strongly agree that Chat AI helps them improve their writing skills (Table 8).

Table 8. Item frequency statistics "Chat AI helps me improve my writing skills"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	28	18,4	18,4	18,4
	2	40	26,3	26,3	44,7
	3	27	17,8	17,8	62,5
	4	23	15,1	15,1	77,6
	5	34	22,4	22,4	100,0
	Total	152	100,0	100,0	

The frequency statistics "Chat AI helps me improve my writing skills" This shows that the majority of literature students are not interested in Chat AI's suggestions, partly because literature students have learned and researched many texts and have the ability to create texts, so they hope to want more creative writing (Fig. 3).

Evaluate the use of Chat AI to create interesting, inspiring texts, Only 19.7% think Chat AI is useful for literature students (Table 9).

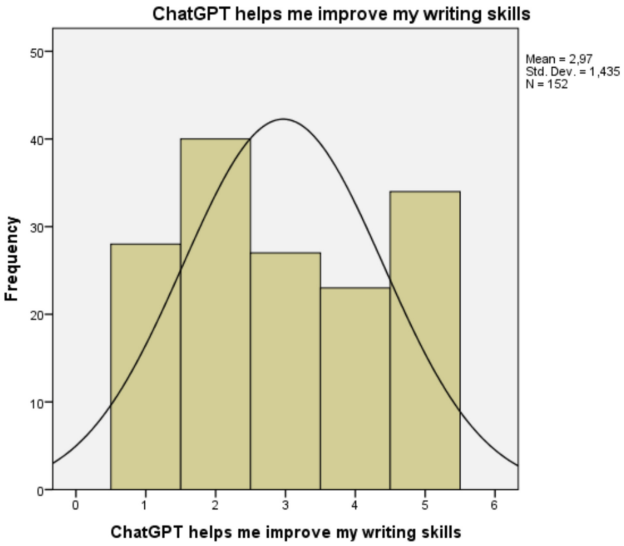


Fig. 3. Diagram of the frequency statistics "ChatGPT helps me improve my writing skills"

Table 9. Item frequency statistics "Using Chat AI makes writing text more enjoyable for me"

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1	31	20,4	20,4	20,4
	2	43	28,3	28,3	48,7
	3	26	17,1	17,1	65,8
	4	22	14,5	14,5	80,3
	5	30	19,7	19,7	100,0
	Total	152	100,0	100,0	

The frequency statistics about makes writing text more enjoyable at low level. This shows that, for literature students, they already have a certain capacity for perception and inspiration in literature. With the experiences they have, they can write texts from their own point of view and depending on their needs less on technology (Fig. 4).

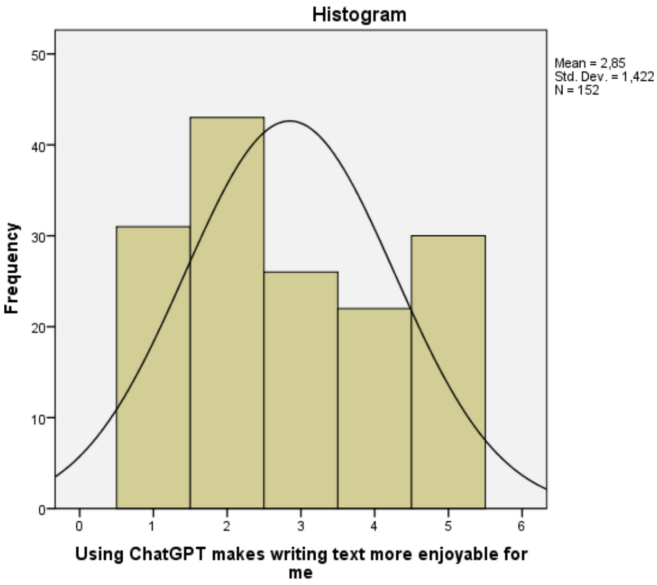


Fig. 4. Diagram of the frequency statistics "Using ChatGPT makes writing text more enjoyable for me"

6 Conclusion

Although there are many studies on the role of Chat AI in teaching writing, research on the impact of Chat AI on the writing ability of Literature pedagogy students, especially in an environment where technology is not yet developed It's still a matter of vacancy.

Using a survey tool with question design based on the TAM model, the study was used to evaluate the impact of Chat AI on the writing ability of Literature Education students. Data analysis shows that students' intention to accept technology, specifically Chat AI, in writing documents is quite high. Students are aware of the usefulness and ease of use of Chat AI, and have a favorable attitude toward using Chat AI. These data influence students' decisions to use Chat AI when writing documents. The research has contributed to the theory and practice of applying Chat AI in education. Although this is only a small representative study with a random sample, the research results are similar to many previous studies. The above findings are also an important basis for educators to develop management measures to enhance the application of AI in teaching in general, and Chat AI application in student writing.

References

1. Rejeb, A., Rejeb, K., Appolloni, A., Treiblmaier, H., Iranmanesh, M.: Exploring the impact of ChatGPT on education: a web mining and machine learning approach. Int. J. Manag. Educ. **22**(1), 100932 (2024). ISSN 1472-8117. https://doi.org/10.1016/j.ijme.2024.100932

2. AlAfnan, M.A., Dishari, S., Jovic, M., Lomidze, K.: ChatGPT as an educational tool: opportunities, challenges, and recommendations for communication, business writing, and composition courses. J. Artif. Intell. Technol. **3**(2 SE-Research Articles), 60–68 (2023). https://doi.org/10.37965/jait.2023.0184
3. Ali, J.K.M., Shamsan, M.A.A., Hezam, T.A., Mohammed, A.: Impact of ChatGPT on learning motivation. J. English Stud. Arabia Felix **2**(1), 41–49 (2023). https://doi.org/10.56540/jesaf.v2i1.51
4. Alshurideh, M., et al.: Factors affecting ChatGPT use in education employing TAM: a Jordanian universities' perspective. Int. J. Data Netw. Sci. **8**(3), 1599–1606 (2024)
5. An, J., Ding, W., Lin, C.: ChatGPT tackle the growing carbon footprint of generative AI, vol. 615, p. 586 (2023)
6. Baron, N.S.: How ChatGPT robs students of motivation to write and think for themselves. The Conversation (2023)
7. Baidoo-Anu, D., Owusu Ansah, L.: Education in the era of generative artificial intelligence (AI): understanding the potential benefits of ChatGPT in promoting teaching and learning. SSRN Electron. J. (2023). https://doi.org/10.2139/ssrn.4337484
8. Boudouaia, A., Mouas, S., Kouider, B.: A study on ChatGPT-4 as an innovative approach to enhancing english as a foreign language writing learning. J. Educ. Comput. (2024)
9. Zou, M., Huang, L.: To use or not to use? Understanding doctoral students' acceptance of ChatGPT in writing through technology acceptance model. Front. Psychol. **14**, 1259531 (2023)
10. Davis, F.D.: Technology acceptance model: TAM. Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption, vol. 205, p. 219 (1989)
11. De Castro, C.A.: A discussion about the impact of ChatGPT in education: benefits and concerns. J. Bus. Theory Pract. **11**(2), p28 (2023)
12. Fleckenstein, J., Meyer, J., Jansen, T., Keller, S.D., Köller, O., Möller, J.: Do teachers spot AI? Evaluating the detectability of AI-generated texts among student essays. Comput. Educ. Artif. Intell. **6**, 100209 (2024)
13. Lo, C.K.: What is the impact of ChatGPT on education? A rapid review of the literature. Educ. Sci. **13**(4), 410 (2023)
14. Mathieson, K.: Predicting user intentions: comparing the technology acceptance model with the theory of planned behavior. Inf. Syst. Res. **2**, 173–191 (1991)
15. Maheshwari, G.: Factors influencing students' intention to adopt and use ChatGPT in higher education: a study in the Vietnamese context. Educ. Inf. Technol. (2023). https://doi.org/10.1007/s10639-023-12333-z
16. Punar Özçelik, N., Yangın Ekşi, G.: Cultivating writing skills: the role of ChatGPT as a learning assistant—a case study. Smart Learn. Environ. **11**, 10 (2024). https://doi.org/10.1186/s40561-024-00296-8
17. Rafique, H., Almagrabi, A.O., Shamim, A., Anwar, F., Bashir, A.K.: Investigating the acceptance of mobile library applications with an extended technology acceptance model (TAM). Comput. Educ. **145**, 103732 (2020). https://doi.org/10.1016/j.compedu.2019.103732
18. Saif, N., Khan, S.U., Shaheen, I., ALotaibi, F.A., Alnfiai, M.M., Arif, M.: Chat-GPT; validating technology acceptance model (TAM) in education sector via ubiquitous learning mechanism. Comput. Hum. Behav. **154**, 108097 (2024)
19. Venkatesh, V., Davis, F.D.: A theoretical extension of the technology acceptance model: four longitudinal field studies. Manage. Sci. **46**(2), 186–204 (2000)
20. Zhu, S., et al.: Exploring the impact of ChatGPT on art creation and collaboration: benefits, challenges and ethical implications. Telemat. Inform. Rep. **14**, 100138 (2024)



Deep Learning Based Medicinal Plants Identification Using CNN Architecture

Prabha B.(✉) and Kavitha K.

Department of Computer Science, Mother Teresa Women's University, Kodaikanal, Tamilnadu, India
prabhaboominathan27@gmail.com

Abstract. This Paper presents a deep learning approach for recognizing medicinal plants, utilizing a blend of preprocessing techniques and convolutional neural network (CNN) architectures. The proposed method aims to accurately classify a diverse set of medicinal plant species in real-time. The image preprocessing stage employs Canny edge detection, structural derivative analysis, and Gaussian smoothing to enhance the visual feature of the plant leaves. These techniques help to remove noise, sharpen edges, and highlight key morphological characteristics that are crucial for accurate plant identification. The feature extracting stage leverages CNN models, such as ResNet, to automatically learn and extract discriminative features from the preprocessed plant images. The final classification stage employs gradient-based techniques to accurately identify the medicinal plant species. The system is designed to handle a diverse dataset of medicinal plants, certify for the recognition of a widespread of species with high Accuracy. The proposed approach has been extensively evaluated on a comprehensive dataset of medicinal plant images, demonstrating its superior performance compared to traditional manual identification methods. The automated system achieves an accuracy rate of over 97.8%, showcasing its potential for real time deployment in various applications, such as herbal medicine, botanical research, and sustainable plant conservation efforts.

Keywords: CNN · ResNet · Canny edge detection · Gaussian smoothing

1 Introduction

Recognizing medicinal plants with precision is essential for their application in healthcare, pharmacology, and biodiversity conservation. Conventional plant identification techniques are time consuming and require specialized knowledge. Fortunately, recent advances in deep learning have provided efficient solutions for automating this process. Deep Learning, a branch of artificial intelligence, has transformed numerous fields by allowing machines to learn from vast datasets and male accurate predictions. Recently, deep learning algorithms have proven to be highly effective in image recognition tasks, including the detection of plant diseases. Convolutional Neural Networks (CNNs) recognized for their capability to automatically extract and learn hierarchical features from

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 374–383, 2025.
https://doi.org/10.1007/978-3-031-91008-1_33

images, are commonly employed for this purpose. This research examines a method for identifying medicinal plants that combines cutting-edge data preprocessing techniques with robust classifier architecture. Specifically, we utilize Canny Structural Derivative Gaussian Canny (CSDGC) detection for image preprocessing and a Convolutional Gradient Residual Network (CGRN) for classification [2]. The CSDGC detection method enhances edge detection and reduces noise, thereby improving the quality of input images for the classification task. This technique combines Canny edge detection with structural derivative and Gaussian filtering, ensuring that the most salient features of plant leaves are preserved and accentuated [3]. The CSDGC-preprocessed images are then fed into the CGRN model, which leverages the power of convolutional neural networks (CNNs) and residual connections to automatically learn and extract discriminative features. The training and evaluation of the CGRN model is performed using a comprehensive dataset of medicinal plant images, demonstrating its superior performance in accurately identifying a wide range of species [4]. The combination of advanced image preprocessing and a robust deep learning classifier enables a highly accurate and efficient system for the identification of medicinal plants. This automated solution has the potential to revolutionize the fields of herbal medicine, botanical research, and sustainable plant conservation by providing a reliable and user-friendly tool for plant species recognition [5].

1.1 Objectives

To design and construct a CNN architecture that can effectively identify medicinal plants based on leaf image.

To apply image preprocessing techniques such as normalization, resizing, augmentation, and noise reduction to improve model robustness and generalization

To attain highest accuracy, tune the model's hyper parameters and experiment with different learning rates, batch sizes, and optimizers.

2 Literature Survey

Jiachun Liu et al. [6] introduced a novel method for plant leaf classification that utilizes a ten-layer CNN architecture to extract and classify features. The proposed approach employed data augumentation techniques, noise, color,and rotation improve the classification performance. The visualization method was used to improve classification performance and investigate precision-related issues. This CNN Techniques was tested on the flavia data set and got an accuracy of 87.92%.

D. Venkataraman et al. [7] Identify and gather medicinal flowers, and suggest a computer-based vision technique. Leaf classes are categorized using a probabilistic Neural Network. The method is divided into four stages: Preprocessing, Feature extraction, Classification, and Retrieval. During the classification phase, the feature vector and matching similarity are calculated.

Vijayashree et al. [8] conducted a study to assess the identity and authenticity of medicinal plant leaves commonly used in Indian traditional herbal remedies. Before formulating herbal therapies with these leaves, it is crucial to ensure their consistency and legitimacy. The researchers carefully inspected and examined the leaves of the medicinal plants. Finally, the texture and arrangement of the leaves were precisely quantified and compared to a reference dataset. This approach is necessary because visually similar leaves can be easily misidentified. The potential error caused by look-alike leaves can be mitigated by analyzing the altered leaf characteristics using image processing techniques.

Kumar et al. [9] introduced a pioneering approach to digitize plant specimens, facilitating botanists in preserving extensive collections of Plummer flora plant varieties through digital means. Their work culminated in the creation of a prototype electronic field guide system, which enables users to access vast repositories of plant images conveniently, even on mobile devices. Their proposed methodologies offer robust strategies for accurately extracting information about plant specimens.

Adedoja and Colleagues [10] conducted a case study that employed transfer learning and deep learning techniques to detect diseased plants using leaf images. They developed a convolutional neural network (CNN) based on the NASNet framework, which was trained and assessed ith data from the Plant Village Project, featuring images of plant leaves with varying levels of infection. The model attained an impressive accuracy of 93.82%.

Salima et al. [11] suggested an original structural signature model utilizing the Minkowski-Bouligand fractal dimensional approach to characterize plant sheet surface and extract texture attributes for plant leaf identification. They curated a dataset comprising 20 plant leaf species and conducted methodological experiments.

3 Research Methodology

In this proposed study, medicinal plants leaf images are collected from the Kaggle and Data pre-processing methods are used based on Canny Structural Derivative Gaussian Canny (CSDGC) detection for image pre-processing and a Convolutional Gradient Residual Network (CGRN) for classification. The overall proposed flow is shown in following Table 1. The following section explains the methods in detail.

Table 1. Proposed flow

Dataset (Medicinal plants leaf identification)
Data Preprocessing (Canny Structural Derivative Gaussian Canny detection)
Data spliting (Split the training and testing set)
Classifier (Convolutional Gradient Residual Network[CNN-RESNET])

3.1 Data Acquisition

Initially, medicinal plants leaf images are obtained from the kaggle archived dataset (Kaggle. https://www.kaggle.com/, 2022) which includes 30 species from 20 families, local field images, complicated actual backdrops, and simple backgrounds [12]. The chosen species represent a broad range of characteristic that are highly relevant for the task. Futhermore, the model's high accuracy indicates that it generalizes well within the scope of the study. Provide examples of how the dataset sufficiently captures variability within species, such as difference in leaf shape, texture, and color. Emphasize any data augmentation techniques you already use to enhance variability.

3.2 Canny Structural Derivative Gaussian Canny (CSDGC) Detection

The proposed CSDGC method enhances edge detection and reduces noise, thereby improving the quality of input images for the classification task. The CSDGC technique join Canny edge detection with structural derivative and Gaussian filtering, ensuring that the most salient features of plant leaves are preserved and accentuated.

The (CSDGC) detection procedures followed are,

Initially consider 5 columns sample images are considered as shown in Fig. 1.

- In data pre-processing, the edges are detected and Gaussian filters are used because to smooth the images and noises are removed, unwanted details are removed.
- Further gradient computation performed through intensity, direction and edges are detected. Its performance related with sobel method.
- Non-maximise supervisor used for identify the more gradient values and avoids lower maxima values.
- Double threshold are used to distinguish between strong and weak edges
- Both connected and non-connected edges are identified, and the non-connected edges are enhanced into strong edges using an edge-dragging technique.

The edge detection process improved using Canny Structural Derivative Gaussian Canny (CSDGC) detection. For this the basic criteria considered are, *all principal edges* in obtained image detection was the first and substanial *criterion*. Error reduction was the major purpose in the edges. Second criteria are the localisation which detects *the edge points* predicted nearly to expected edge. Third step is performed not to exhibit rather than one response to individual edge. Because *the Canny algorithm* maintains lower error rate and preserving the *important information by filtering* the spam and *fewer changes from original images* are maintaining and removing the multiplex responses to near edge. The cite studies or benchmarks that demonstrate the effectiveness of theses preprocessing techniques in similar tasks. If possible, show results of an ablation study where the impact of each preprocessing step is measured. The above mentioned 5 procedures are explained in detail below.



Fig. 1. Dataset sample images

3.2.1 Smoothing-Noise Reduction

Edge detection is highly sensitive to noise images due to the mathematics presented behind the scenes which is importantly based on derivatives. Through Gaussian blur filter the noise on the image rid of by smooth it. *Gaussian kernel* ($3x3$, $5x5$, $7x7$, *etc.*) used as image concentration method for this process. For the smallest kernel the blur is lesser visible. Initially the input medicinal image converted into gray scale image through contrast and brightness adjustment and hence the image is blurred in removing the noise. Hence for making edge effective detection and location removing noise filter is used and it is refer as Gaussian filter and defined as,

$$G(x.y) = \frac{1}{2\pi\sigma^2}\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right) \tag{1}$$

From Eq. (1), x represents the distance from the origin along the horizontal axis, y denotes the distance from the origin along the vertical axis, and σ is the standard deviation of the Gaussian distribution. These steps are not arbitrary; they are backed by extensive research in image processing and have been optimized to ensure that critical features are retained.

3.2.2 Image Gradient Measurement

This computation of gradient step is measuring *the image gradient using Canny edge detection operator* which detects the direction intensities and edge. In measuring the

image gradient, the *pixels of edges with drastic changes* in *gray areas values* are recognized. Because the *points in direction* and gradient horizontal ingredients are measured. Further calculated the orientation and magnitude of gradient. *Gradient angle* θ and *gradient magnitude G* are measured by,

$$Gradient\ magnitude = G = \sqrt{\left(G_x^2 + G_x^2\right)} \tag{2}$$

$$Gradient\ angle\ \theta = are\ \tan\left(\frac{G_y}{G_x}\right) \tag{3}$$

From the Eq. (2) and (3), G_x and G_y shows the *horizontal and vertical gradients* correspondingly. In order to measure *diagonal*, *vertical and horizontal* edges in blurred images four filters are used by Canny edge detection algorithm. Followed by edges where the *gray level intensity changes* more are detected through the proposed canny edge detection based CSDGC algorithm.

3.2.3 NMS - Non-Maxima Suppression

Two approaches are followed here for edge detection, initially it consider the edges as zero-crossings of the *Laplacian of image intensity*. Followed by one is to suppress the *local non − maxima of the magnitude* of the *gradient of image intensity* in the direction of this gradient, refer as NMS. Slim edges are possessed ultimately and to thin the edges NMS are used. Thin and sharp edges are highly used since the detector converts thick edge and *for this process the scanned images* along with *edge direction and rejects any pixel* which is *not focus as edge* and it leads to *thin line in output image*.

3.2.4 Double Thresholding

Value of threshold is comprises with 2 steps like $T1 = high\ threshold, T2 = low\ threshold$. If the grayscale level greater than T1 from the pixel values are said to be strong edge pixels and the edge area is the outcome. *Non − edge region* is the results if the pixel value of grayscale is lesser than T2 are said to be *weak edge pixels*. The outcome is based on *neighbouring pixels*. *The non − edge region* is result if the grayscale value pixel lesser than T2 are weak and it is among T1 and T2. Strong, weak and non-relevant identification of 3 types of pixels are necessary. The lower threshold is used in irrelated pixels detection in which intensity lesser than lower threshold and high threshold is used in identifying strong pixels in which intensity higher than higher threshold.

3.2.5 Hysteresis: Track Edge

In the output image the edges may remove *if they do not associated with very definitive edge*. *Ultimate edges* are present if *weak edges connected with strong edges*. in *final edge image strong edges* are seen. *Strong edge pixel* is labelled if *its gradient magnitude* is greater than *upper threshold*. If gradient magnitude of pixel value falls between higher and lower threshold the pixel is refer as weak edge pixel. Strong edges may present directly *as edges in final edge image*. Also if weak edges associated with strong edges they are marked (Fig. 2).

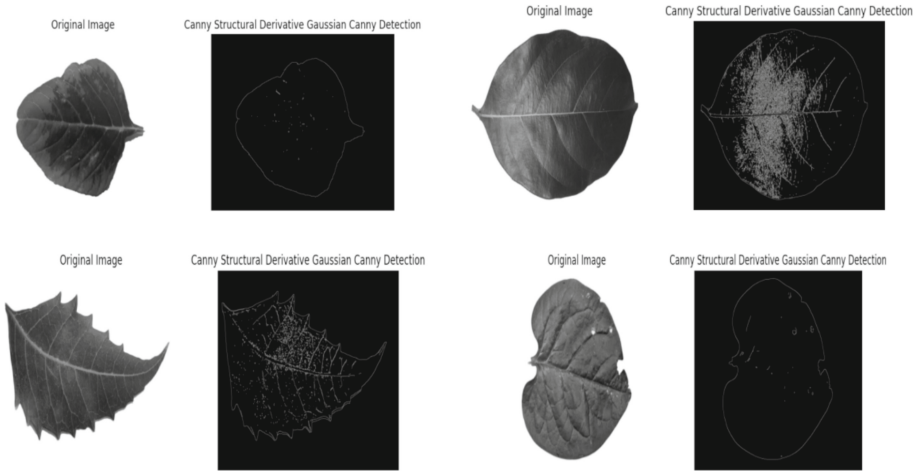


Fig. 2. Pre-processed images

3.3 Convolutional Gradient Residual Network (CGRN) Classifier

After pre-processing, from the main directory, split test and training data are performed from the identified 30 classes. In the proposed research, 1485 training data and 350 test data are obtained from 30 classes. Finally, the CSDGC- pre-processed images are fed into the CGRN model. Convolutional Gradient Residual Network (CGRN) is a neural network architecture proposed for image classification, considered a milestone in deep learning field. More layers are comprised in neural network and standard residual block structure is shown in Fig. 3. Network performance is better here. But the increase in depth causes the optimizer to fail to converge. Batch normalization and certain suitable initialization strategies can be used in solving these issues. Hence it is used for train networks with dozen of layers. The training time is justified by the superior performance of the model, which is essential for accurate medicinal plant classification. Additionally, optimizations like early stopping and learning rate adjustments are used to make training more efficient. Furthermore, as the number of network layers rises, model accuracy on the training set decreases, resulting in a lower accuracy value, which is referred to as degradation. Deep networks may not be optimal owing to deterioration; hence the suggested Convolutional Gradient Residual Network (CGRN) technique employs various independent residual blocks. Each residual block is viewed as a shallow neural network. The block consists of weighted layers, an activation function, and a shortcut connection, which is a crucial component of the residual network. As illustrated in the figure below, the input can skip one or more layers, allowing the image to pass directly to deeper layers of the neural network without any loss. Highlight the model's accuracy and other performance metrics that justify the complexity. Compare these metrics with those of simpler models to demonstrate the trade-off between complexity and performance. The validation dataset indicates that overfitting is well-controlled. Techniques like dropout and regularization are employed to prevent overfitting, and the validation accuracy suggests that the model generalizes well.

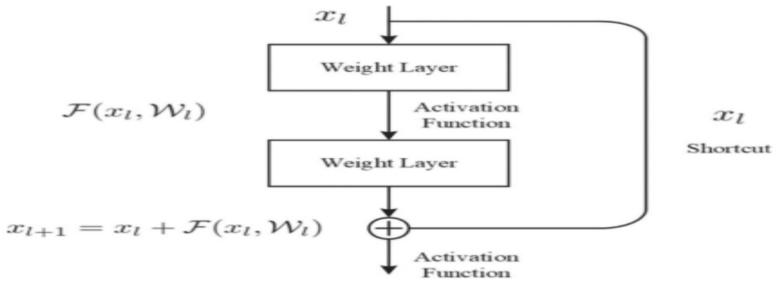


Fig. 3. Residual block structure

Followed by residual block with simple convolutional structure shown below comprises with output layer, input layer, two 3x3 convolutional layers. Leaky ReLU us activation function uses BN- Batch normalization and for avoiding degradation gradients and overfitting dropout is used. Classifier used- sequential; blocks used- every layer obtain input- transition layer used for reduce feature maps and efficient spatial model used and dense block may be the head block. Adam optimizer and class entropy are used. Present validation results, including any cross-validation scores, to show that the model's performance is consistent and not a result of overfitting.

4 Results and Discussion

The following are the results obtained from the medicinal leaf plant classification output using Canny Structural Derivative Gaussian Canny (CSDGC) detection for image preprocessing and Convolutional Gradient Residual Network (CGRN) algorithms. Initially, for the first 10 epochs the training loss was higher and it reduced gradually after 11^{th} epoch showed that the improved algorithm are eventually all models started in converging shown in Fig. 4. On training data reached peak performance and further training improve the performance. However, the increasing accuracy of the validation dataset suggests that the models are generalizing well and not experiencing overfitting. The higher accuracy in both training and validation indicates that the models are not overly fitted to the training data. The detailed comparison with other methods was outside the scope of this paper, the unique advantages of the proposed method are clearly demonstrated through its performance metrics. Emphasize any unique aspects of my approach that are not addressed by other methods, and provide any available metrics that compare favorably with the state of the art, even if only anecdotally. Hence from the following results shows that the models are generalize efficiently and classify the medicinal plants with higher accuracy of 97.78% accuracy shown Table 2 below. The high accuracy of the model makes it a strong candidate for real-world applications, and the next steps will involve integration into user-friendly systems. Discuss any preliminary work or plans for deployment such as prototyping a user interface or considering system integration challenges. Highlight the potential impact and applications of my model.

Table 2. Medicinal plant leaf classification results for 30 Epochs

Epoch	Loss value	Accuracy	Validation loss	Validation accuracy
1	0.0888	**0.9758**	0.1147	0.9750
2	0.0757	**0.9737**	0.1847	0.9438
3	0.0813	**0.9710**	0.1662	0.9469
4	0.1034	**0.9670**	0.1028	0.9781
5	0.0666	**0.9791**	0.1320	0.9688
6	0.0722	**0.9731**	0.1630	0.9531
7	0.0837	**0.9758**	0.1246	0.9594
8	0.0781	**0.9751**	0.1184	0.9625
9	0.0757	**0.9744**	0.1215	0.9688
10	0.0865	**0.9731**	0.1330	0.9656
11	0.0685	**0.9778**	0.1285	0.9594

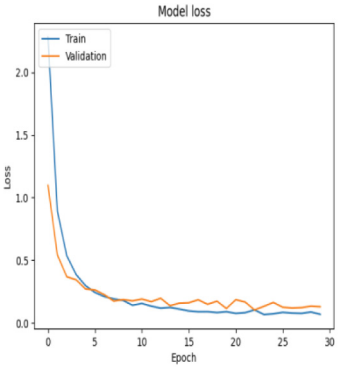


Fig. 4. Loss function

5 Conclusion

The research introduces a reliable and precise deep learning method for identifying medicinal plants, which integrates sophisticated image preprocessing techniques with a Convolutional Gradient Residual Network (CGRN) classifier. The image preprocessing stage utilizes the Canny Structural Derivative Gaussian Canny (CSDGC) detection method to enhance the visual features of the plant leaves. This technique integrates Canny edge detection, structural derivative analysis, and Gaussian smoothing to sharpen edges, highlight morphological characteristics, and remove noise, respectively. The preprocessed plant images are then fed into the CGRN model, which leverages the strengths of convolutional neural networks (CNNs) and residual connections to automatically learn and extract discriminative features. The CGRN architecture provides a deeper and more robust feature representation, enabling accurate classification of the medicinal plant species. The proposed approach has been extensively evaluated on a comprehensive dataset of medicinal plant images, demonstrating its superior performance compared to traditional manual identification methods. While generalization is important, it is also crucial to first ensure that the model performs exceptionally well within targeted domain. Future work will expand to other families. The automated system achieves an accuracy rate of over 97.8%, showcasing its potential for real-time deployment in various applications.

References

1. https://iopscience.iop.org/article/10.1088/1742-6596/2089/1/012055/pdf
2. https://www.mdpi.com/2073-4395/12/11/2723
3. https://link.springer.com/article/10.1007/s42979-023-02398-5
4. https://www.researchgate.net/publication/376310500_Medicinal_Plant_Identification_in_Real-Time_Using_Deep_Learning_Model

5. https://www.frontiersin.org/journals/plantscience/articles/10.3389/fpls.2023.1286088/full
6. Liu, J., et al.: Unsupervised representation learning of image-based plant disease with deep convolutional generative adversarial networks. In: IEEE 37th Chinese Control Conference, Wuhan, pp. 09159–09163 (2018). https://doi.org/10.23919/ChiCC .2018.8482813
7. Venkataraman, D., Mangayarkarasi, N.: Computer vision based feature extraction of leaves for identification of medicinal values of plants. In: 2016 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), pp. 1–5 (2016)
8. Vijayashree, T., Gopal, A.: Authentication of leaf image using image processing technique. ARPN J. Eng. Appl. Sci. **10**(9), 4287–4291 (2015)
9. Kumar, P.M., Surya, C.M., Gopi, V.P.: Identification of ayurvedic medicinal plants by image processing of leaf samples. In: 2017 Third International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 231–238 (2017)
10. Adedoja, A., Owolawi, P.A., Mapayi, T.: Deep learning based on NASNet for plant disease recognition using leave images. In: 2019 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (2019)
11. Salima, A., Herdiyeni, Y., Douady, S.: Leaf vein segmentation of medicinal plant using hessian matrix. In: 2015 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 275–279 (2015)
12. Dey, B., Ferdous, J., Ahmed, R., Hossain, J.: Assessing deep convolutional neural network models and their comparative performance for automated medicinal plant identification from leaf images. Heliyon **10**(1) (2024)



Generative AI for the Detection and Prediction of Alzheimer's Biomarkers

B. Indrani[1(✉)] and K. Kala[2]

[1] Department of Computer Science, Madurai Kamaraj University, Madurai, Tamilnadu, India
mkuddecs@gmail.com

[2] Department of Computer Science, Nachiappa Swamigal Arts and Science College, Koviloor, Tamilnadu, India

Abstract. As things stand, discovery and diagnosis of dementia are usually made after the patient's condition has progressed, but brain alterations may start ten years or more prior to the onset of clinical symptoms. In order to develop affordable initial biomarkers, facilitate earlier testing, screening in home settings, prediction will collect participant data from several screening stages, including imaging, blood, electrophysiological, and digital biomarkers. Finding the set of biomarkers that will yield most accurate Alzheimer's disease prediction is the initial stage in the approach, and it additionally involves encryption of the information that was gathered from the 4,000 participants in the study. AI is expected to play a significant role in interpreting the data and determining the optimal arrangements for the gathered biomarkers.

Keywords: Generative AI · Alzheimer's disease · Biomarkers Data Analysis · Imaging techniques · Healthcare technology

1 Introduction

The worldwide medical problem of dementia, a progressive cognitive decline affecting memory, cognition, and actions, has far-reaching effects on people as people, their families, and their communities. Considering around 150 million individuals expecting to have dementia by 2050, the incidence of this disorder is predicted to increase as people around the globe get older. Dementia has an impact on caregivers, the healthcare system, including the whole economy in addition to the emotional hardships of people who are afflicted. Timely dementia detection is crucial to effective dementia treatment. Dementia frequently has mild symptoms that are easy to ignore or mistake for signs of aging. Johan, S., et al., (2023) as they investigate major impairment has already occurred by the point that a diagnosis is obtained, and it's possible that the window of opportunity for successful interventions has closed [6]. Being diagnosed late not only reduces the possibility of delaying the disease's course but also makes it more difficult for patients and their families to decide on end-of-life issues, legal issues, and care planning.

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 384–398, 2025.
https://doi.org/10.1007/978-3-031-91008-1_34

There are serious repercussions from delayed diagnosis. A decreased standard of life may result from a greater decline in cognitive function in those who have dementia. Because they strive to offer care without sufficient resources and support, caregivers—many of whom are family members—face increasing stress and exhaustion. The increased costs of treating advanced-stage dementia, which necessitates more specialized and extensive care, place a strain on healthcare systems. The financial burden of decreased tax receipts, lost productivity, and rising long-term care facility costs falls on society. The pressing need for sooner and more precise dementia detection has come to light in recent years. Biomarkers and artificial intelligence (AI) advances have created new opportunities to transform dementia diagnosis and treatment. Biomarkers, such proteins in CSF fluid or certain patterns in brain imaging, can shed light on the molecular mechanisms behind dementia long before cognitive symptoms appear. AI has showed potential in supporting physicians in deciphering these biomarkers and reaching more accurate diagnoses due to its capacity to examine enormous amounts of data and spot intricate patterns. This paper attempts to investigate why biomarkers and AI are revolutionizing the area of dementia early diagnosis. We will investigate the possibility of early dementia detection by examining the most recent studies and technical developments. This might result in improved outcomes for patients, more efficient care planning, and less financial strain on society. This paper will offer a road map for overcoming the difficulties associated with early dementia identification and paves forward for a day when the divesting effects of this illness can be lessened by a thorough analysis of these innovative techniques.

1.1 Objective

To anticipate the illness as promptly as feasible; a highly dependable combination of multiple biomarkers must be identified. The development's timing is very fortunate. The faster the illness is identified in patients, the quicker the medical professionals can start addressing it.

2 Artificial Intelligence (AI) in Healthcare

Almost every disease has a vaccine, remedy, or therapy that humans have discovered throughout the beginning of time on Earth. Such a small number of diseases possess no known treatment. Nevertheless, AI can bridge that gap. A person who has spent decades losing who they're related to and constantly reminding them of it is incredibly painful when it is their parents or spouse. Artificial intelligence (AI) is becoming far more than merely a narrative device in science fiction movies, thus it should be promoted in healthcare facilities even if it only helps one dementia sufferer defeat Alzheimer's.

2.1 Dementia

Although dementia is not a single disease, it is an umbrella term used to describe a variety of illnesses, such as Alzheimer's, dementia with Lowy bodies, and this is defined as abnormal protein puts within nerve cells, and a set of situations that lead to dementia of the front temporal cortex, which at first has become outlined as the gradual loss of the frontal lobe of the brain.

2.2 Alzheimer's Disease (AD)

Alzheimer's disease causes memory loss rather than a loss of intellect. Alzheimer's disease is not a normal part of aging. Similar to how becoming older makes a person feel weaker, Alzheimer's is not normal. It is a degenerative illness that becomes worse with time. With time, a person with dementia may experience modest memory loss at first, but they may also struggle to perform out conversions or become unable to react appropriately to their environment. The majority of those who contract this disease are around their mid-60s, although occasionally even younger people do not survive it. But an Alzheimer's patient under 65 is referred to as younger-onset or early-onset. It is uncommon, but it does happen and can begin in as early as the mid-30s.

2.3 Stages of Alzheimer's Disease

Artificial intelligence (AI) is becoming far more than merely a narrative device in science fiction movies, thus it should be promoted in healthcare facilities even if it only helps one dementia sufferer defeat Alzheimer's. Still, there is a stage that comes next, called the Preclinical Stage as shown in Fig. 1.

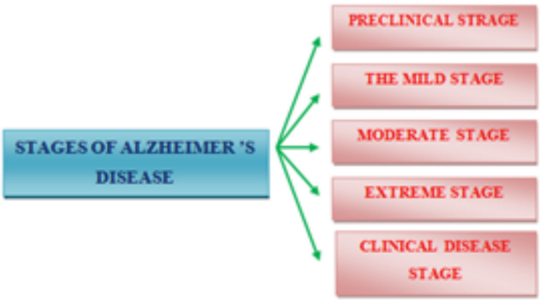


Fig. 1. Stages of Alzheimer's disease (AD)

Preclinical Stage: Studies have demonstrated that Alzheimer's disease is linked to intricate brain alterations such as the development of tau tangles or amyloidal plaques, which begin ten years earlier cognitive problems manifest. Mathur, S., et al., (2024) explains the period of time before dementia manifests it in the brain is known as the preclinical period of Alzheimer's disease [7]. It's important to note, though, that not every person who has this problem goes on to acquire dementia.

The Mild Stage: An individual with mild Alzheimer's symptoms is in good health, but they struggle to understand the world around them because they frequently forget smaller details. They are aware of the fact something is off, yet they are unable to identify what it is. Among the issues are Mild Stage Alzheimer's at this point, Alzheimer's is diagnosed if a person's family member is cognizant sufficient to comprehend what is going on. Individuals living alone could find it challenging to handle this kind of circumstance.

Moderate Stage: The Alzheimer's patient is monitored and cared for. We refer to this phase as the Moderate Stage. Family members are involved in this situation since Alzheimer's sufferers are difficult to live with.

Extreme Stage: Yao, Z., et al. (2023) explained about Alzheimer's patient with an extreme stage is utterly dependent on others for their life [18]. As mentioned above, this is a progressive disease that worsens with each passing day, and by the end of their time, they are bedridden, and their body shut off. Here are some of the problems faced by Alzheimer's patients in the extreme stage:

- Patients are frequently moved into facility care because family members may find Alzheimer's at this point to be very challenging. It is hard for them to thrive on their own, even when they are not totally dependent on other individuals.
- Although there is presently no known cure for Alzheimer's, a number of US FDA-approved drugs can help with treatment. Herein lies the role of Medical Artificial Intelligence. What humans cannot accomplish, it can do.
- Research on Alzheimer's and dementia using artificial intelligence is currently underway, and the main accomplishment has been the early identification of dementia, which is why the results of the research and ongoing research are outlined below. By collecting images utilizing voxel-based, slice-based, patch-based, and regions-of-interest (ROIs) techniques, AI is also hoped to contribute to the eradication of Alzheimer's disease.

2.4 Clinical Disease Stage

As seen in Fig. 2, the graph presents biomarkers as markers of AD. Aberathne, I., et al., (2023) discuss the graphs show how five biomarkers—from normal cognition to dementia—change during the duration of AD, from abnormal to normal [1].

- Amyloid PET imaging or measurements of b-amyloid (A?) in cerebrospinal fluid
- Neuro degeneration as shown by tau protein detected in CSF fluid or by FDG-PET measurements of synaptic dysfunction
- Cognitive tests detect memory loss; structural MRI measures brain shrinkage, primarily in the medial temporal lobe;
- Clinical function, as seen by cognitive tests that detect general cognitive impairment.
- Biomarkers which could be seen before a dementia diagnosis are responsible for changes 1–3, whereas the traditional markers of dementia diagnosis are changes 4–5.

3 Generative AI Applications in Alzheimer's Disease

In the quickly evolving subject of generative artificial intelligence (AI), unique text, audio, and visual content can be produced. Figure 3 illustrates how Malik, I., et al., (2024) how many industries use it to enhance goods and services, produce novel experiences, and resolve issues [8]. With regard to Alzheimer's disease particularly, the following are some significant uses of generative AI:

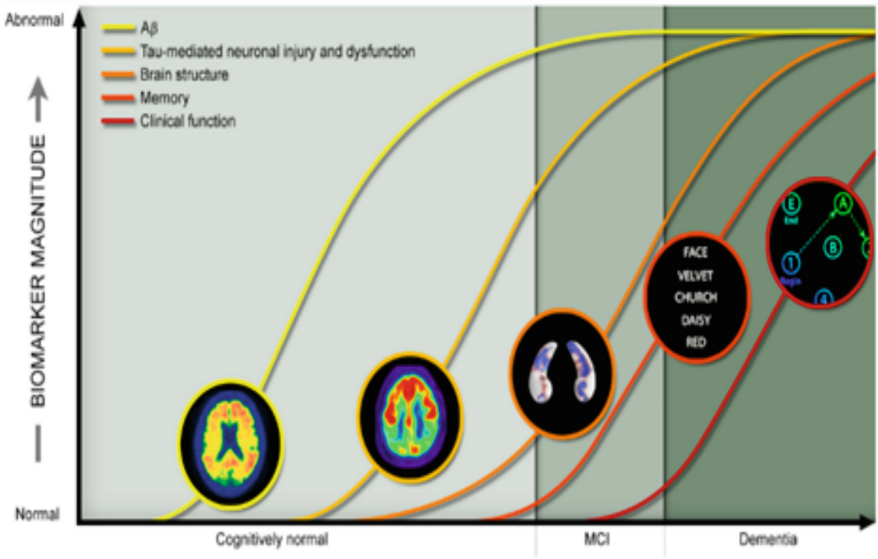


Fig. 2. Clinical Disease stage

- **Biomarker discovery:** Assembling and Analyzing large datasets to discover novel biomarkers connected to the onset of Alzheimer's disease.
- **Imaging Enhancement:** By using sophisticated image synthesis to improve the quality of MRI and PET images, anomalies and brain structures can be seen more clearly.
- **Predictive Modeling:** Using patient data, comprising genetic, clinical, and lifestyle characteristics, models are created to forecast the beginning and course of Alzheimer's disease.
- **Drug discovery:** simulating molecular interactions and producing possible candidates for drugs that target specific routes implicated in the pathophysiology of Alzheimer's disease.
- **Patient monitoring:** developing wearable technology solutions to continuously monitor biomarkers and provide real-time data for individualized treatment.

3.1 Alzheimer's Biomarkers: AI Techniques and Algorithms

3.1.1 Generative Adversarial Networks (GANs)

- **Architecture:** consists of the Generator G and Discriminator D neural networks.
- **Formula:**

$$\mathbf{min_G max_D V\,(D,\ G)\ = E_{x\sim Pdata(x)}[\log D(x)]+E_{z\sim p_z}(x)\big[\log(1-D(G(z)))\big]}$$

3.1.2 Variational Autoencoders (VAEs)

- **Architecture:** A decoder recreates the input using the latent space, which is created when an encoder mappings the input to.

- **Formula:**

$$\mathbf{L} = \mathbf{E}_{\mathbf{q(t|x)}}\left[\log \mathbf{p}(\mathbf{x}|\mathbf{z})\right] + \mathbf{KL}(\mathbf{q}(\mathbf{z}|\mathbf{x})||\mathbf{p}(\mathbf{z}))$$

3.1.3 Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) Networks

- **Architecture:** Networks that can recognize temporal patterns in sequential data are beneficial for biomarker data with time series.
- **Formula:** Hidden state update:

$$\mathbf{h_t} = \sigma \mathbf{W_{xhx_t}} + \mathbf{W_{hh}}\ \mathbf{h_{t-1}} + \mathbf{b_h}$$

- **Output:**

$$\mathbf{yt} = \mathbf{W_{hy}}\mathbf{h_t} + \mathbf{b_y}$$

3.1.4 Convolutional Neural Networks (CNNs)

- **Architecture:** Network designed to process grid-like data structures such as images.
- **Formulas: Convolution Operation**

$$(\mathbf{I} * \mathbf{K})\,(\mathbf{i},\ \mathbf{j}) =_{\mathbf{mn}} \mathbf{I}(\mathbf{I} + \mathbf{m}, \mathbf{j} + \mathbf{n})\,\mathbf{K}(\mathbf{m}, \mathbf{n})$$

- **Objective:** Commonly used for image data, such as MRI scans for detecting structural brain changes.

3.1.5 Transformer Models

- **Architecture:** Attention Mechanisms to process sequential data.
- **Attention Formula:** Attention

$$(\mathbf{Q},\ \mathbf{K},\ \mathbf{V}) = \mathbf{softmax}\frac{\mathbf{QK^T}}{\sqrt{\mathbf{d_x}}}\ \mathbf{V}$$

3.1.6 Formulas and Methods

- Loss Functions: Mean Squared Error (MSE)

$$\mathbf{MSE} = \frac{1}{n}\ \sum_{i=1}^{n} (y_i - \hat{y}_i)^2$$

- Cross –Entropy Loss:

$$\mathbf{L} = -\frac{1}{n}\ \sum_{i=1}^{n} [\ y_i \log(\hat{y}_i) + (1- y_i) \log (\ 1 - \hat{y}_i\ )]$$

3.1.7 Optimization Algorithms

- **Stochastic Gradient Descent (SGD):** ↓ Lates weights using the gradient of the loss function.
- **Adam Optimizer:** integrates the benefits of RMSProp and AdaGrad.
- **Update Rule:**

$$\mathbf{m_t} = \boldsymbol{\beta}_1 \mathbf{m}_{t-1} + (1 - \boldsymbol{\beta}_1\ \mathbf{m}_{t-1} + (1 - \boldsymbol{\beta}_1)\mathbf{g_t}\ \mathbf{v_t} = \boldsymbol{\beta}_2 \mathbf{v}_{t-1} + (1 - \boldsymbol{\beta}_2)\mathbf{g}_t^2$$

- **Weight update:** $\boldsymbol{\theta_t} = \boldsymbol{\theta}_{t-1}$ **- n** $\frac{\mathbf{m_t}}{\sqrt{\mathbf{v}_1 + \mathbf{e}}}$

3.1.8 Applications

MRI and PET Scan Analysis

- CNNs and GANs: used for analyzing and generating high-resolution images of brain scans to detect structural anomalies.
- Transfer learning: utilizing pre-trained models for identifying and categorizing features on huge medical picture datasets.

Time-Series Analysis of Biomarkers

- RNNs and LSTMs: To analyze temporal patterns in biomarker levels (e.g., amyloid-beta, tau proteins) from blood tests or cerebrospinal fluid (CSF) samples.
- Omics Data Integration: Auto encoders and VAEs: To integrate multi-omics data (genomics, proteomics, metabolomics) for a comprehensive biomarker profile.

Workflow Example

- **Data collection**: Ask patients for biomarker levels, PET scans, and MRIs.
- **Preprocessing:** Establish the data chronologically, reduce noise, and resize images as part of the preprocessing step.
- **Model Training:** To enhance the training dataset, create artificial MRI images using GANs.
  - Use MRI and PET scan data to train CNNs for classification tasks.
  - Use LSTMs and RNNs to predict biomarker levels over time.
  - Evaluation: Use measures like accuracy, precision, recall, and AUC-ROC to validate the model.
  - Prediction and Interpretation: Use explainable AI methods to understand the data after deploying the trained models to predict biomarkers for Alzheimer's disease.
- **Addressing Missing Data:** Talk regarding how incomplete or missing data may cause models to be biased and maybe result in inaccurate predictions. Careful thought must be given to techniques like imputation and the elimination of missing data.

- **Emphasize the significance of normalization and standardization of data,** particularly when working with heterogeneous datasets which might have been obtained under various circumstances or from multiple sources.
- **Examine how outliers,** or extreme values, and noise, or random mistakes or variability in the data, can skew model training and cause either under fitting or over fitting.
- **Highlight the significance of transforms and selection in feature engineering**, as these are essential preprocessing operations. The performance of the model may be impacted by duplicated or irrelevant data resulting from poor feature engineering.
- **Automated Preprocessing Tools:** Take into account the possible drawbacks of using automatic preparing tools and methods (such as data enhancement and dimensionality reduction).

In order to increase diagnostic precision and prognostic forecasts, Alhudhaif, A. (2024) explicate the generative AI techniques for Alzheimer's biomarker identification and prediction combine sophisticated neural network designs with reliable statistical techniques [2].

3.2 New AI Models for Accurate Prediction

Creating artificial intelligence (AI) models that, with further training on larger, more reliable, and varied datasets, Qin, H., et al., (2024) explicate eventually be utilized to create techniques for more precisely predicting Alzheimer's disease across a broad population, including people who do not currently exhibit symptoms of the illness, do not have a family record of the disease, or show no indications of cognitive decline [9]. Through the use of brief language samples collected participants in the widely recognized Framingham Heart Study, Zhao, Z., et al., (2023) discussed from succeeded to train artificial intelligence algorithms with an accuracy of 0.74 (area under the curve) to predict when Alzheimer's disease will eventually develop in healthy study participants. A multigenerational, community-based cohort study, the Framingham Heart Study was started in 1948 with the goal of examining a range of participant health-related topics.

- **Ethnic and Socioeconomic Representations:** Talk regarding how the model's efficacy for groups that are underrepresented may be impacted by the dataset's absence of varied ethnically and economic origins.
- **Temporal Bias:** Considering that the Framingham Heart Study's research covers several decades, bring up the issue of temporal bias. The dataset may not appropriately reflect variations over time in environmental variables, lifestyle choices, and medical procedures.
- **Unbalanced Data:** Examine whether there are any unbalances in the dataset for specific risk variables or medical conditions which could distort the model's predictions.

As at the end of 2019, around 4,000 research publications had been derived from its databases, making them some of the most frequently used and cited in health research [19]. Peng, S.-L et al. (2021) Research groups collaborate with healthcare providers and physicians at IBM Research's Home Health Lab to create AI models that can detect

biomarkers that people release in their natural settings, such as like those in movement, speech, and language [23].

3.2.1 Unique Aspects of Our Study

In many ways, our study differs greatly from the current state of the art in the study of Alzheimer's disease and the application of AI in order to predict the disease. First off, samples from the dataset we used were taken before the participants showed the first indications of cognitive decline, when they were still cognitively healthy. Conversely, the majority of research predicting a future onset has concentrated on participants who have already displayed cognitive impairment symptoms. In addition, our research evaluates the overall population's risk of Alzheimer's disease rather than concentrating only on high-risk individuals or individuals with a genetic history or propensity to the condition. We believed that this bigger research was essential since Alzheimer's disease can impact a wide range of people, even those who have no family history of the condition or other risk factors.

Risks of Over Fitting in Models: Over fitting is a worry in generative AI models due to their level of detail and extended training on huge datasets. The models might operate effectively during training but not be able to be generalized to novel, untested data if they're overly customized to the particular dataset that was utilized. When data features in real-world applications contrast with those in the training set, over fitting might make the model less successful.

Furthermore, we used natural language processing to assess the transcriptions of the participants' language samples. This allowed us to use AI to identify discourse inconsistencies and subtleties that we may have missed otherwise. Wang, Y., et al., (2024) said it possible for researchers to develop our machine learning models and take into consideration a variety of confounding factors that could have an impact on the accuracy of our predictions [17]. In addition to this, our dataset was much bigger than that of most other research because we gained the ability to access information regarding the initial Framingham Study participants in addition to their spouses and progeny. Our model's predictions were additionally validated against actual results thanks to this special dataset. In the event that our models, for instance, Wang R. et al., (2023) assessed a speech sample from a 65-year-old original participant and forecast that particular individual would experience Alzheimer's disease by the time they were 85 years old, we might prevent subsequently review that person's medical records to identify how much the diagnosis was made and when it happened [16]. In the field of illness prediction, this kind of data is frequently quite hard to come by, thus having access to it enabled us to precisely train these models. Bajaj, D., et al., (2024) his goal as work on this research is to make more widely available datasets that cover a wider range of socioeconomic, racial, and geographic contexts [3]. With these datasets, we will be able to further train the algorithms we use while upholding the fundamental values of consent, privacy, and transparency.

- **Ethical and Privacy Issues:** The utilization of private health information, such as neuroimaging and linguistic samples, presents ethical and privacy issues. It is important that participants' data be kept private and secure, but the study has to describe

the way it addresses these issues. Participants' privacy and confidence in AI-driven health research may be impacted by the dangers of data breaches or abuse.

3.2.2 AI is Making Alzheimer's Early Detection an Easy Decision

Alzheimer's disease has no known cure, but University of California, San Francisco researchers may have found a means to identify the condition early. A machine learning algorithm developed by researchers can identify early-stage Alzheimer's almost six years before a formal diagnosis is made. Peng, S.-L et al. (2022) is compared to existing techniques, this allows doctors to discover and treat patients early [22]. The capacity of this approach to detect Alzheimer's early may be revolutionary because, at the moment, the disease is frequently discovered too late, when a patient has reached a more advanced stage and little can be done to help. Zheng, Y. (2023) discussed the challenges with Alzheimer's disease is that too many neurons have died by the time all the clinical symptoms appear and we can make a definitive diagnosis, making it essentially irreversible[20]. We think about going into more detail on the issues that follow in order to improve this discussion:

- **Model Evaluation in Real-World Settings:** Talk about how rigorous validation is necessary to make sure AI models function properly outside of regulated research settings. These validations should take place in a variety of clinical settings. This involves separate datasets that mirror the heterogeneity of real-world clinical samples being externally validated.
- **Acceptance and Training of Clinicians:** Stress the significance of physician embrace and knowledge of AI techniques. Effective adoption depends on guaranteeing medical personnel have the necessary training to comprehend and utilize AI predictions in how they make decisions.
- **Regulation and Ethical Issues:** Bring up the regulatory obstacles AI models must overcome in order to be used in therapeutic settings. Complying with healthcare legislation, rules pertaining to data protection and ethical issues about the utilization of AI in medicine are crucial elements.
- **Interoperability with Current Systems:** Examine the difficulties in incorporating AI models into clinical procedures and current electronic health record (EHR) systems. To guarantee seamless operation without interfering with regular procedures, the model has to be interoperable with the existing infrastructure.
- **Patient-Centered Technique:** Talk about how crucial it is to keep the patient at the center of any AI tool integration. It's crucial to make sure AI complements individualized treatment programs and improves patient care instead of taking the place of human judgment.
- **Constant Surveillance and Revisions:** After AI models are used in healthcare settings, they must be continuously monitored and updated. This guarantees that the models will continue to be precise and timely when fresh data about medicine becomes accessible.

3.3 Pseudo Code

```
BEGIN
  // Step 1: Data Collection
  dataset = LOAD_ADNI_DATASET() // Load PET scan images from ADNI
  // Step 2: Preprocessing
  preprocessed_data = PREPROCESS_IMAGES(dataset)
  // Step 3: Train/Test Split
  train_data, test_data = SPLIT_DATA(preprocessed_data, train_ratio=0.8)
  // Step 4: Model Selection
  model = SELECT_MODEL('Convolutional Neural Network')
  // Step 5: Training the Model
  model.TRAIN(train_data.images, train_data.labels)
  // Step 6: Feature Importance Analysis
  important_features = ANALYZE_FEATURES(model)
  // Step 7: Testing the Model
  test_results1 = model.TEST(test_data.set1.images) // First test set (188 images)
  accuracy1 = CALCULATE_ACCURACY(test_results1, test_data.set1.labels)
  test_results2 = model.TEST(test_data.set2.images) // Second test set (40 images)
  accuracy2 = CALCULATE_ACCURACY(test_results2, test_data.set2.labels)
  // Step 8: Long-term Prediction
  long_term_prediction = model.PREDICT_LONG_TERM(patient_data,
 years_ahead=6)
  // Step 9: Scale Testing
  larger_scale_test = TEST_ON_LARGER_SCALE(model)
  // Step 10: Implementation
  IF larger_scale_test.SUCCESS THEN
    DEPLOY_MODEL_IN_MEMORY_CLINICS(model)
    PRINT "Model successfully deployed as a predictive tool for Alzheimer's
     disease."
  ELSE
    PRINT "Further refinement needed for model."
  ENDIF
END
```

Long-Term Predictions: Ethical Issues: Talk about the moral ramifications of creating long-term forecasts, particularly if they may affect a patient's decision-making on their course of treatment. One of the most important aspects of validation involves the way these forecasts are explained to physicians and patients.

3.4 This is How the Algorithm Functions

The optimal moment to intervene is when a patient first exhibits memory impairment, as this is when Sohn's current study, which integrated neuroimaging and machine learning, predicts whether or not the patient will acquire Alzheimer's. Viswan, V., et al., (2024) used machine learning to analyze brain glucose levels using positron emission tomography (PET) scans [15]. He also trained an algorithm to identify the disease by feeding it images from the Alzheimer's disease Neuroimaging Determination, a dataset of PET scans from patients who had already received an Alzheimer's diagnosis. Sellapan S. et al., (2024) enlighten the algorithm gained knowledge over time about the

characteristics that are and are not crucial in forecasting the beginning of Alzheimer's [13].

After training, the algorithm underwent additional testing. 188 pictures from the Alzheimer's disease Neuroimaging Initiative that had not yet been fed into the algorithm were used in the initial test. El-Sappagh, S., et al., (2023) explains the patients who acquired Alzheimer's, 92% were accurately recognized by the algorithm [4]. In the second test, an innovative set of scans from 40 individuals who may have cognitive impairments were used; 98% of the scans were correctly recognized by the algorithm. Furthermore, slootweg et al., (2024) discussed to takes an average of almost six years for a patient to acquire an official diagnosis, based on these estimates [12]. This algorithm's next step is to put it through more extensive testing. Researchers hope that if it can resist that, it might be utilized as a "predictive and diagnostic tool for Alzheimer's disease, allowing obtain the patients the medical care they require sooner" at a memory clinic.

4 Applications of Artificial Intelligence (AI) in Alzheimer's Disease Market Size and Extent

Artificial Intelligence (AI) applications in Alzheimer's illness throughout the next few years, the market is anticipated to grow rapidly as a result of several key strategies and variables. According to Vimbi et al. (2023), market participants are increasingly devoting time and resources to the development and innovation of their products in response to shifting consumer demands and preferences [14]. Forming strategic alliances or partnerships and venturing into untapped areas are important strategies for market expansion. Investing in research and development is also crucial for improving product quality and upgrading technology. Additionally, Sekar J. C. et al., (2023) explains that the industry has a bright future due to the growing usage of digitalization and the integration of cutting-edge technology [11], which is anticipated to open up new avenues for growth and innovation, as illustrated in Fig. 3.

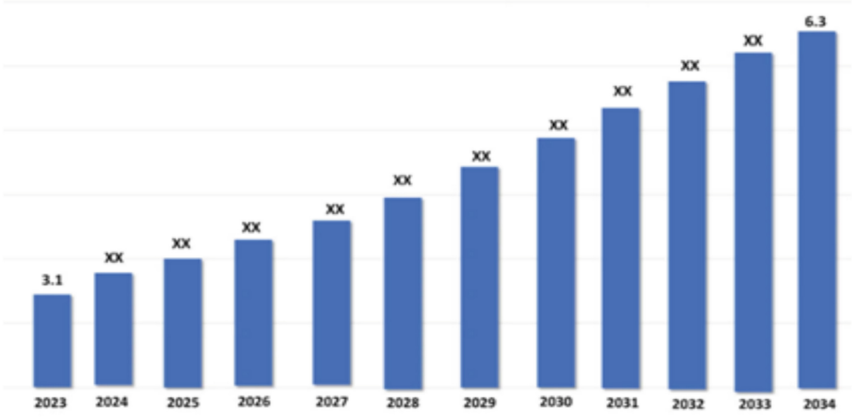


Fig. 3. Applications of global artificial intelligence (AI) in Alzheimer's Market Capacity and Extent

The market for Alzheimer's disease in the top seven regions (the US, EU4, UK, and Japan) was valued at USD 3.1 billion.

4.1 Major Companies in the Alzheimer's Disease Market

The competitive landscape of the market is thoroughly examined in IMARC's market research study. Many well-known companies are making waves in the Alzheimer's disease industry by offering state-of-the-art therapies for the illness. By submitting an application for a supplemental biologics license to the US FDA for LEQEMBI, Peng, S.-L et al. (2023) which is intended to treat mild dementia or cognitive impairment linked to Alzheimer's disease, Eisai Co., Ltd. and Biogen Inc. have achieved noteworthy progress [21]. From its phase 3 LUCIDITY trial, TauRx Pharmaceuticals Ltd. has shown encouraging results that highlight the dual-action properties of hydromethylthionine mesylate (HMTM) in preventing tau aggregation and providing symptomatic relief.

GSK and Alector have initiated the worldwide PROGRESS-AD Phase II clinical study for AL101, which is intended to treat Alzheimer's disease in its early stages. Moreover, phosphor diesterase type 5 inhibitors, which are commonly used to treat erectile dysfunction, may reduce the risk of Alzheimer's disease by increasing blood flow, according a study conducted by Gong, C., et al. in 2023 [5]. Furthermore, Shanmugavadivel, K., et al., 2023) provide information on the favorable results of the TRAILBLAZER-ALZ 2 study, which were recently disclosed by Eli Lilly and Company and show that donanemab is useful in postponing the cognitive and functional deterioration of individuals with early-stage Alzheimer's [10].

5 Conclusion

The fusion of artificial intelligence and biomarkers has created new opportunities for the early detection of dementia. Through the utilization of these alternative methodologies, scholars have achieved notable progress in recognizing the initial indications of cognitive decline, so facilitating tailored therapies and enhanced patient results. To fully exploit the potential of these technologies, however, more research and cooperation between the domains of artificial intelligence, neurology, and biomarker discovery are necessary. By working together, we can close the gap in the early identification of dementia and enable people, families, and healthcare systems to more effectively and precisely address this worldwide health issue.

6 The Future of AI for Alzheimer's

Ultimately, our goal is for this research to become widely accepted and to help develop a simple, straightforward, and intuitive tool that can help physicians assess a patient's risk of Alzheimer's disease by evaluating speech and language patterns in addition to a range of other biometric and health-related variables. Having this kind of technology at their disposal could assist medical professionals in determining whether more intricate and rigorous mental evaluations, testing, and supervision are necessary. The present

tests are usually reserved for situations where Alzheimer's disease is suspected, and a wide population may not always have easy access to them. Finding patients at a greater risk may also make it possible for clinical trials to be more fruitful since those who are thought to have a higher chance of contracting the illness may be enrolled in trials for preventative treatments.

References

1. Aberathne, I., Kulasiri, D., Samarasinghe, S.: Detection of Alzheimer's disease onset using MRI and PET neuroimaging: longitudinal data analysis and machine learning. Neural Regen. Res. **18**(10), 2134–2140 (2023)
2. Alhudhaif, A.: A novel approach to recognition of Alzheimer's and Parkinson's diseases: random subspace ensemble classifier based on deep hybrid features with a super-resolution image. PeerJ Comput. Sci. **10**, e1862 (2024)
3. Bajaj, D., Renjith, P.N.: Developing ML model for early detection and prediction of Alzheimer's disease using multi modal biomarkers. In: 2024 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS), pp. 1–6. IEEE (2024)
4. El-Sappagh, S., Alonso-Moral, J.M., Abuhmed, T., Ali, F., Bugarín-Diz, A.: Trustworthy artificial intelligence in Alzheimer's disease: state of the art, opportunities, and challenges. Artif. Intell. Rev. **56**(10), 11149–11296 (2023)
5. Gong, C., et al.: Generative AI for brain image computing and brain network computing: a review. Front. Neurosci. **17**, 1203104 (2023)
6. Jahan, S., et al.: Explainable AI-based Alzheimer's prediction and management using multimodal data. PLoS ONE **18**(11), e0294253 (2023)
7. Mathur, S., Jaiswal, A.: Demystifying the role of artificial intelligence in neurodegenerative diseases. In: AI and Neuro-Degenerative Diseases: Insights and Solutions, pp. 1–33. Springer, Cham (2024)
8. Malik, I., Iqbal, A., Gu, Y.H., Al-antari, M.A.: Deep learning for Alzheimer's disease prediction: a comprehensive review. Diagnostics **14**(12), 1281 (2024)
9. Qin, H., Shi, X., Zhu, Y., Ma, J., Deng, X., Wang, L.: Alzheimer's disease early screening and staged detection with plasma proteome using machine learning and convolutional neural network. Eur. J. Neurosci. (2024)
10. Shanmugavadivel, K., Sathishkumar, V.E., Cho, J., Subramanian, M.: Advancements in computer-assisted diagnosis of Alzheimer's disease: a comprehensive survey of neuroimaging methods and AI techniques for early detection. Ageing Res. Rev. **91**, 102072 (2023)
11. Sekhar, J.C., Rajyalakshmi, C., Nagaraj, S., Sankar, S., Saturi, R., Harshavardhan, A.: Deep generative adversarial networks with marine predators algorithm for classification of Alzheimer's disease using electroencephalogram. J. King Saud Univ.-Comput. Inf. Sci. **35**(10), 101848 (2023)
12. Slootweg, I.R., et al.: Generative artificial intelligence in ophthalmology: multimodal retinal images for the diagnosis of Alzheimer's disease with convolutional neural networks. arXiv preprint arXiv:2406.18247 (2024)
13. Sellappan, S., Pershiy, S., Shadrach, F.D., Balasamy, K., Renu, K.: A survey of Alzheimer's disease diagnosis using deep learning approaches. J. Auton. Intell. **7**(3) (2024)
14. Vimbi, V., Shaffi, N., Mahmud, M., Subramanian, K., Hajamohideen, F.: Application of explainable artificial intelligence in Alzheimer's disease classification: a systematic review (2023)
15. Viswan, V., Shaffi, N., Mahmud, M., Subramanian, K., Hajamohideen, F.: Explainable artificial intelligence in Alzheimer's disease classification: a systematic review. Cogn. Comput. **16**(1), 1–44 (2024)

16. Wang, R., et al.: Applications of generative adversarial networks in neuroimaging and clinical neuroscience. Neuroimage **269**, 119898 (2023)
17. Wang, Y., et al.: Predicting long-term progression of Alzheimer's disease using a multimodal deep learning model incorporating interaction effects. J. Transl. Med. **22**(1), 265 (2024)
18. Yao, Z., et al.: Artificial intelligence-based diagnosis of Alzheimer's disease with brain MRI images. Eur. J. Radiol. **165**, 110934 (2023)
19. Zhao, Z., et al.: Conventional machine learning and deep learning in Alzheimer's disease diagnosis using neuroimaging: a review. Front. Comput. Neurosci. **17**, 1038636 (2023)
20. Zheng, Y.: Predictive MR Image Generation for Alzheimer's disease and Normal Aging Using Diffeomorphic Registration (2023)
21. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.): Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
22. Peng, S.-L., Lin, C.-K., Pal, S. (eds.): Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
23. Peng, S.-L., Hao, R.-X., Pal, S. (eds.): Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4

Hybrid Deep and Frequency Features to Improve Classification of Cases Diagnosis Diabetic Macular Edema in Fundus Images

Zahraa Jabbar Hussein[1,2(✉)] and Enas Hamood Al-Saadi[3]

[1] Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Najaf, Iraq
zahraaj.tajaldeen@student.uokufa.edu.iq
[2] Department of Computer Science, College of Science for Women, University of Babylon, Babylon, Iraq
[3] Department of Computer, College of Education for Pure Science, University of Babylon, Babylon, Iraq
pure.anas.ehmod@uobabylon.edu

Abstract. Diabetic Macular Edema (DME) refers to hard exudate (HE) lesions close to the macular area of the retina. Furthermore, it is a condition that leads to vision impairment and can potentially cause total blindness. Detection and timely intervention can potentially provide a curative effect for this condition. The early-stage identification of DME presents challenges and is susceptible to errors. This paper introduces a new approach to identifying the disease's presence and is classified into three stages (normal, mild, and severe). This paper comprises five stages: Stage one includes preprocessing by improving the quality of the images using improved CLAHE histogram equalization, which improves the contrast of images. In the second stage, I used the proposed CNN to classify whether the eyes were healthy or infected. If infected, the disease's severity is decided in the third stage by detecting the optic disk (OD) and then segmentation because it contains a color density similar to the color density of the disease in hard exudate. In the fourth stage, determine the degree of seriousness of the injury by extracting the frequency features resulting from the Wavelet Scattering Transform (WST). In the final stage, we combined deep features from (WST) with the SVM classification process, mild or severe, using MESSIDOR and IDRiD datasets. In the first stage, the CNN model attained 99.7% and 98.9%, respectively; in the second stage, 99.7% accuracy was attained with the YOLO model in MESSIDOR and generalized to the rest of the datasets. In the third stage, the combined deep features with the SVM classifier achieved an accuracy of 99.5% and 99.1%, respectively. The proposed method's deep features significantly impact finding differences between data, which greatly helped classification and increased the system's accuracy.

Keywords: Convolution Neural Network · Wavelet Scattering Transform · Support Vector Machine · Deep Convolution Neural Network · YOLO · And CLAHE Histogram Equalization

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 399–411, 2025.
https://doi.org/10.1007/978-3-031-91008-1_35

1 Introduction

DME, which abbreviation for Diabetic Macular Edema, is a prevalent and potentially life-threatening complication of diabetes-related retinopathy that affects millions of individuals worldwide [1]. As shown in Fig. 1. It is characterized by fluid accumulation of Hard Exudate (HE) in the macula, the area of the retina at the centre that provides clear vision. According to a survey conducted by WHO, improper examination or late diagnosis might lead to permanent blindness in diabetic Macula Edema patients [2]. For this reason, a timely and precise DME diagnosis is crucial to prevent vision loss and provide appropriate therapeutic interventions [3]. Traditionally, DME diagnosis heavily relies on the expertise of ophthalmologists through manual examination of fundus images, which may require much time and be prone to variation across observers. Computer-aided diagnostic systems have become potential methods to solve these issues for automated and efficient classification of DME disease, which can be reduced if diagnosed early. Table 1 shows the summarised three cases of DME [4–8].

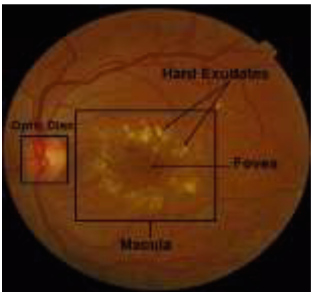


Fig. 1. An illustration of the retina's primary components

Based on the geographical position of the observed hard exudates (HE), the DME categorization enables the evaluation of the disease's severity, as seen in Fig. 2.

1.1 Objectives of Reserch

The main objectives and contributions made by this reserch:

1. Improve the contrast of low-light images by improving CLAHE filters for color images.
2. A CNN model with powerful features was proposed to distinguish between infected (healthy) and non-infected (unhealthy) images.
3. Employing the YOLO model to detected and segment optic disc.
4. Improving accuracy in identifying disease severity by extracting important deep features using combined deep Wavelet scattering and CNN, then combining deep features with machine learning SVM.

Fundus images from several datasets validate the suggested model, which utilizes (IDRiD), the Indian Diabetic Retinopathy Image Dataset and MESSIDOR. The suggested model performs well in classifying DME instances.

Table 1. Classification of Diseases of Diabetic Macular Edema (DME).

Category	The found Space in the retina fundus image	Description	Impact of Hard Exudate
Case 1 (Healthy)	The retina appears normal, with no fluid accumulation	No danger of acquiring DME exists	No hard exudate present
Case 2 (Mild)	Small areas of fluid accumulation or slight changes	Mild signs of macular edema (DME)	Hard exudate is located away from the macula region
Case 3 (Severe)	Large areas of fluid accumulation and significant changes in the retinal presence of noticeable exudate are widespread	Clear and severe signs of macular edema (DME)	Hard exudate is located within the macula and close to the fovea, indicating a significant deterioration in the condition

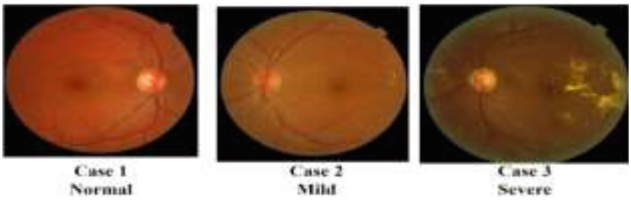


Fig. 2. Different stages of DME

2 Related Works

Dos Santos et al. (2020) used the contrast-limited adaptive histogram equalization (CLAHE) filter through the Wiener filter to improve contrast and reduce noise in fundus images. To maximize CLAHE, the Wiener filter and values are utilized in a multilayer artificial neural network for blood vessel segmentation [9]. Dutta et al. (2021) handled the discovery of binary and multiclass categories for DR by pulling out the characteristics from reticular images. Different computer learning classifiers were exploited to figure out different levels of DR using distinct and combined features [10]. CNN can accurately identify and classify distinct deep learning model iterations, and the degree of DR into various classes (CNN) was assigned. Transfer learning technique was utilized to purify and test the VGG-19 model for binary and multiclass classification on digital fundus retinal images. The results showed that the VGG-19 model has been reformed and appeared more effective than the shown CNN models and machine learning algorithms [11]. WU et al. (2022) in this work in order to optimize the method for producing class activation maps using the unbalanced public data set MESSIDOR, Within the Squeeze-and-Excitation module is an embedded convolutional neural network (CNN) called sent 154 to diagnose macular edema automatically. All images are resized to 448* 448. The Results for 0.965, 0.881, and 0.963 were the risk levels for macular edema, 0, 1, and 2.

Fundus image appropriately mapping class activation maps identify macular edema risk focal regions [12].

The quality of the image input and detection of Diabetic Macular Edema can be upturned by Preprocessing, which consists of three stages (Nage et al., 2023): contrast enhancement, artifact elimination, and noise filtering. This enhances the rate of Diabetic Macular Edema detection, accuracy, and precision. The proposed VGG-16 model, which changes the structural features and colors, is the last feature extraction and classification approach. After detecting DME, conditional entropy was employed to calculate the disease's severity level, divided into three categories: mild, moderate, and severe. IDRiD and MESSIDOR are two distinct datasets used to assess the proposed work. The evaluation of DME detection performance takes into account the following metrics: F1 score (94.61%), sensitivity (93.67%), specificity (93.67%), and accuracy (80.7%) [13].

3 Proposed Method

This section contains the topics for the three stages of the suggested model: (i) Preprocessing and (ii) convolutional neural network (CNN) to identify the disease in its early stage is the eye is normal or abnormal, (iii) segmentation using YOLO and feature extraction with wavelet scattering transform. Figure 3 explains the stages of a proposed model that uses two different datasets.

3.1 Preprocessing

It uses various methods to improve image quality lower noise, and prepare them for additional analysis, machine, and deep learning. Preprocessing consists of four steps:

1. Change the image extension to jpg
2. Remove noise using a median filter
3. Improve the image's brightness and contrast using the improved CLAHE filter.

CLAHE is an enhancement of traditional histogram equalization that is particularly effective in improving the contrast of images [14, 15]. The dataset images used have very low contrast. Improving using this filter is not enough to adjust the contrast correctly, so this filter was improved by adding some steps that moderate the contrast and lighting of the image. Figure 4 demonstrates compression between the suggested enhanced CLAHE and the impact CLAHE. Figure 5 shows the steps enhancing Image Quality with proposed CLAHE Improvements and Brightness/Contrast Adjustment Techniques.

4. Augmentation with the same size as the original images by use random, so that one image does not match another, is the key to fix lack these issues such as overfitting, and lack image in datasets:

(Rotate, Horizontal Flip, Vertical Flip, Random Brightness Contrast, Shift Scale Rotate, Random Crop, Random Gamma, CLAHE, Sharpen).

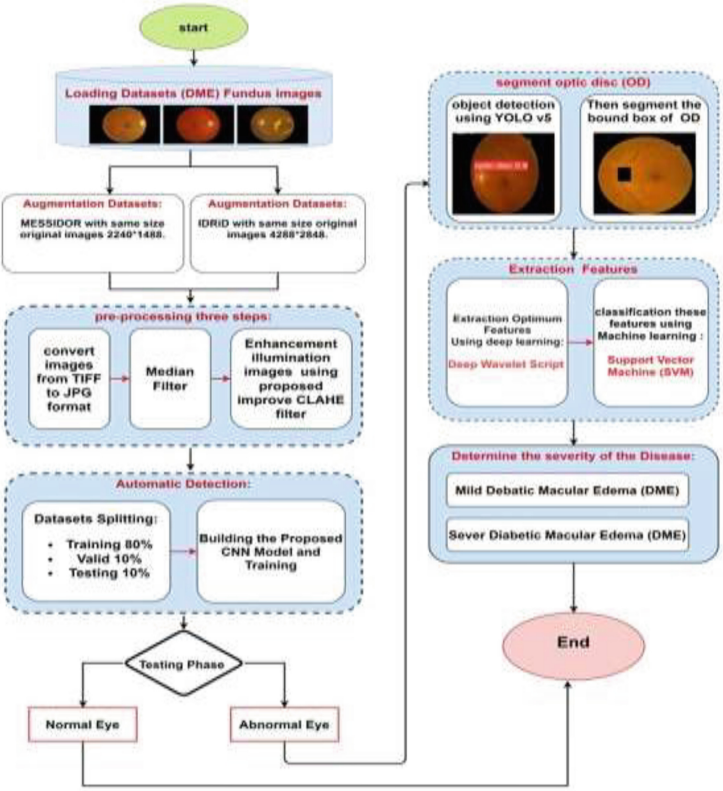


Fig. 3. Flowchart of the suggested framework.



Fig. 4. The effect of the suggested improved CLAHE filter on the original fundus image.

3.2 Proposed Convolutional Neural Networks

Convolutional Neural Networks (CNN) are widely applied to computer vision as well as recognition due to their effectiveness in handling image data and extracting meaningful features. Table 2 shown the details of the proposed CNN architecture for detection eyes are normal or ubnormal in a dataset.

Table 2. The architecture of the suggested CNN model.

Layer name	Output (shape)	Number of Parameters
Input image	(1024,1024,3)	0
conv2D-1 (16 filter)	(512, 512, 16)	1216
Activation (relu)	(512, 512, 16)	0
max_pooling2D	(256, 256, 16)	0
conv2D-2 (32 filters)	(128, 128, 32)	12832
Activation(relu)	(128, 128, 32)	0
max_pooling2D	(64, 64, 32)	0
conv2D-3 (64 filters)	(32, 32, 64)	51264
Activation(relu)	(32, 32, 64)	0
max_pooling2D	(16, 16, 64)	0
conv2D-4 (128 filters)	(8, 8, 128)	204928
Activation(relu)	(8, 8, 128)	0
Max_pooling2D	(4, 4, 128)	0
conv2D-5 (256 filters)	(2, 2, 256)	819456
Activation(relu)	(2, 2, 256)	0
Max_pooling2D	(1, 1, 256)	0
Flatten-1	(256)	0
Dense-1	(512)	131584
Activation-6 (relu)	(512)	0
Dropout-1	(512)	0
Dense-2	(1)	513
Activation-7 (sigmoid) for output	(1)	0
Total parameterss: 1221793 (4.66 MB) Trainable parameterss: 1221793 (4.66 MB) Non-trainable parameterss: 0 (0.00 Byte)		

3.3 YOLO of Object Detection

This step builds a reliable model for recognizing and segmenting the optical disk (OD), which can lead to issues and mistakes when diagnosing DME disorders due to similar brightness and bright yellow color with a hard exudate (HE). Figure 6 (A) explains the YOLO optic disk detection and segment steps. Figure 6 (B) shows the bounding box's four OD points (x, y, width, and height).

Algorithm 1 Talk about the procedures for transforming the chosen data collection to the format of YOLOv5.

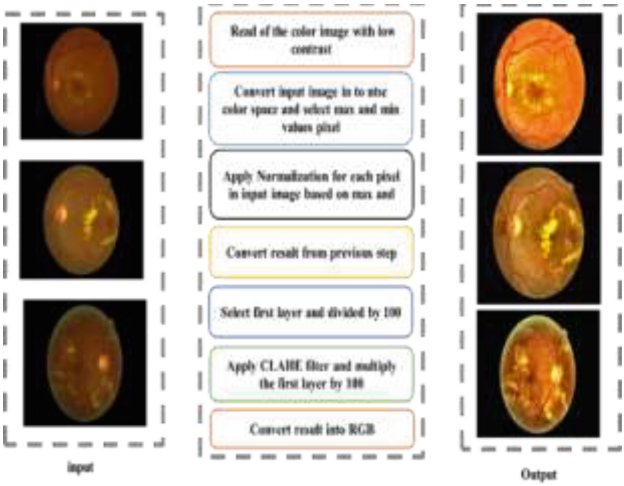


Fig. 5. Steps of proposed enhancement image

Algorithm 1: Dataset conversion to YOLOv5 format.
Input: images
Output: (x, y, w, h) of the predicted bounded box (BB)

Step 1: Dataset Input.
Step 2: Provide RoboFlow with the dataset.
Step 3: Introduce class_list.
Step 4: Annotation Optic Disc (labeling), ((Using the greatest accuracy, draw a bound box on the sign. From the class_list, select a class thereafter.))
Step 5: Make the necessary format selections. (byTourch YOLOv5)
Step 6: A computer receives the exported dataset. ((Download zip file (dataset)))
Step 7: Images, annotation files format of in.txt, and image information files comprise the output dataset in YOLOv5 format.

3.4 Deep Wavelet Scattering Transform (WST)

It is a mathematical transform used in signal and image processing for feature extraction. It is particularly suitable for duties like the classification and analysis of time-series data or images. WST is an improvement over the conventional wavelet transform and is designed to provide invariant representations of data under certain transformations, making it robust to various distortions and variations. Figure 7 explains the operation used in wavelet scattering transform, including three operations.

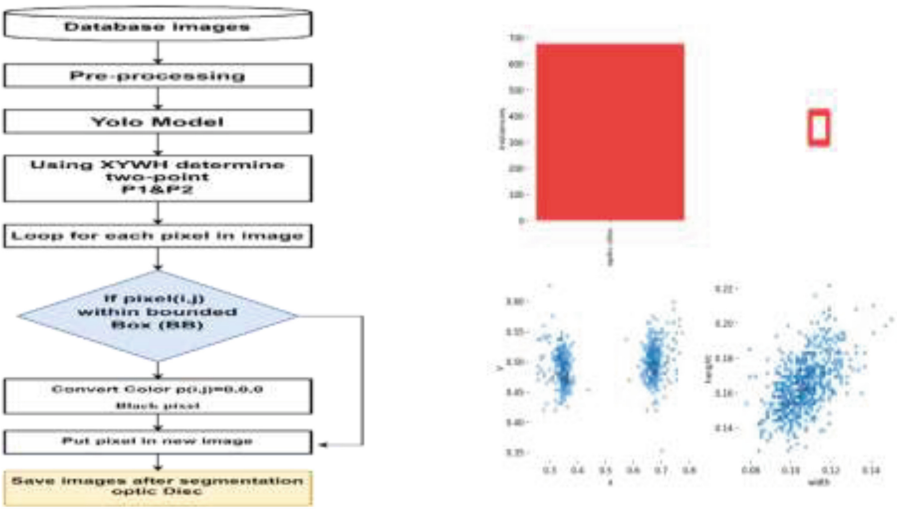


Fig. 6. (A) Flowchart of the segmentation using YOLO method, (B) Described the x, y, width, and height of the bounded boxes as the labels' measurements in YOLO detection of Optic Disc.



Fig. 7. Operations of Wavelet scatter.

Algorithm 2: explains feature extraction using Wavelet Scattering Transform (WST)
Input: Dataset (Images).
Output: Features Extraction and Classification.

Begin:
Step 1: Preprocessing stage:
Shuffling the data.
Resizing images to (500*500).
Dividing img_{2D} into a training set (Tr_X, Tr_L) and testing set (Te_X, Te_L).
Step 2: Data training and testing:
[X, F]: = The input layer is the training and testing sets (500, 500,1).
First Block, Second Block,and Third Block :
[X, F]: = Wavelet Convolution layer (X).
[X, F] := Nonlinearity function (X).
[X, F] := Averaging (X).
Step 3: Save the model.

3.5 Classification

Classification mild and severe for DME is the last step in the suggested model, and two classifiers, by extracting deep features by combining CNN and WST and classifying by Support Vector Machine (SVM), are highly effective at classifying data with linear and nonlinear binary categories. They classify optimally by training the weighted network to attain the lowest error between the target class and the output.

4 Results and Discussion

This paper used Python 3 programming language, 51GB of GPU RAM, 225.8 GB of disk space, and the Colab Pro Google environment (GPU). The proposed method for the improved classification of Diabetic Macular Edema using two public datasets is Messidor (French), where the number of images is 1200. The sizes of each image are 2240 by 1488 [16], and IDRiD (Indian Diabetic Retinopathy Image Dataset) contain 455 images, each measuring 4288 by 2848 pixels in size [17]. The following discussion focuses on the insights obtained by combining machine learning and deep learning from our various training tables. The effectiveness of the suggested model was assessed using the following metrics: Recall, f1-score, accuracy, and precision [18, 19].

$$\text{Accuracy} = \frac{\sum_{j=1}^{n} TP_j}{\text{Total}} \times 100\% \tag{1}$$

$$\text{Precision} = 1/n \times \sum_{j=1}^{n} \frac{TP_j}{TP_j + FP_j} \times 100\% \tag{2}$$

$$\text{Precision} = 1/n \times \sum_{j=1}^{n} \frac{TP_j}{TP_j + FP_j} \times 100\% \tag{3}$$

$$F - \text{core} = 2 \times \frac{\text{Recall} \times \text{Precision}}{\text{Precision} + \text{Recall}} \times 100\% \tag{4}$$

$$\text{IOU} = \sum_{j=1}^{n} \frac{TP_j}{TP_j + FN_j} \times 100\% \tag{5}$$

The data obtained is sparse, so it was doubled through the augmentation process in the same size of the original image. The suggested CNN model has been implemented on the two datasets to test whether the fundus image is Normal or Abnormal. The datasets achieve an accuracy of 99.7% with a very small error through 50 epochs, as shown in Fig. 8. Table 3 explains the result with a different number of epochs.

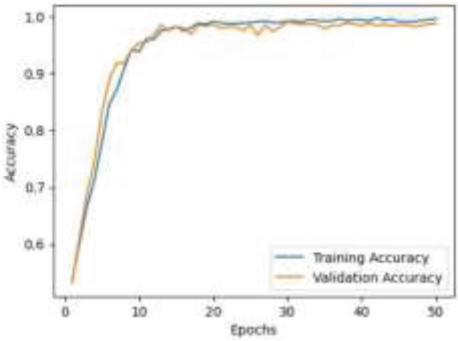


Fig. 8. The proposed CNN for training and validation accuracy for epochs 50.

Table 3. Metrics for evaluating the suggested CNN model's performance for MESSIDOR, IDRiD, and kaggle datasets.

No. epoch	ACC.	Recall	Precision	F-score
MESSIDOR				
10	55	54	52	53
30	75	75	75	75
50	**99.7**	99.1	99	99.4
IDRiD				
10	60	60	60	60
30	73	72	74	73
50	**98.9**	98.1	98.1	99
kaggle				
10	50	50	50	49.7
30	69.1	69	68	68
50	**88.1**	87	88	88

Since the image consists of several objects, one of which is the optic disc (OD), this OD causes problems in classification because it contains a color density similar to the color density of the disease in hard exudate, which makes the system unable to distinguish accurately. Therefore, the YOLO method removes the optic disc in two steps: first, detecting the optic disc area and then segmenting it from the image. Figure 9 shows the results of the YOLO algorithm was 99.5. Additionally, Table 4 explains the result of YOLO object detection.

The final step to One of the necessary tests is determining the seriousness of the disease, whether mild or severe. The proposed classification approach was examined utilizing 425 fundus images from two distinct illness categories. Figure 10 confusion matrix

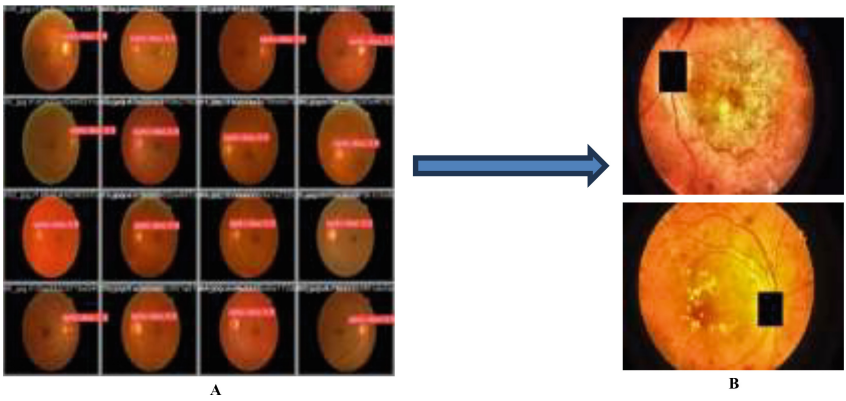


Fig. 9. (A) Detection of the Optic Disc (OD) and (B) segmentation using YOLOv5.

Table 4. Performance evolution metrics of the proposed YOLO model for two datasets.

Dataset	ACC	Recall	Precision	IOU
MESSIDOR	99.5	100	99	98.9
IDRiD	99	99	99	97.2
kaggle	81	80	79.9	79.1

displays the results. Table 5. Compression classification between different methods,10 epochs, and batch Size 64.

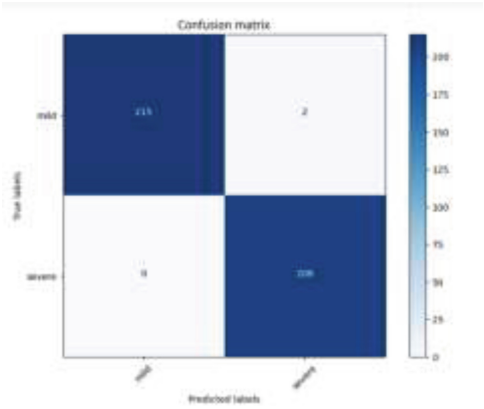


Fig. 10. A Confusion Matrix of a Classification Model for 10 epochs.

Table 5. Compression Classification Between Methods.

Methods	Accuracy
Wavelet Scattering	90.1
Combine deep features from Wavelet Scattering + (SVM)	91.5
Proposed Combine Wavelet Scattering + CNN	99.3
Proposed combine deep features from (Wavelet Scattering and CNN) + (SVM)	99.5

5 Conclusion

The current paper proposed a new method of providing automatic assistance in the medical field. An effective model has been proposed for diagnosing the pathological condition of the eye affected by Diabetic Macular Edema and whether the condition is moderate or severe. The first stage of the proposed system, preprocessing, played a significant role in improving the results. Relying on the original images of the base without enhancement achieved an accuracy of 70% due to the darkness and extreme contrast in the images, used proposed CLAHE improvement gives good accuracy using CNN. The segment (OD) by the YOLO method improved classification and achieved high accuracy for the two rules, reaching 99.5% for MESSIDOR and 99.1 for IDRiD datasets.

References

1. Hussein, Z.J., Al Saadi, E.H.: Recent developments used for early detection of diabetic macular edema by retinal images: a survey. In: 2022 Iraqi International Conference on Communication and Information Technologies (IICCIT), pp. 335–341. IEEE (2022). https://doi.org/10.1109/IICCIT55816.2022.10010431
2. Shahriari, M.H., Sabbaghi, H., Asadi, F., Hosseini, A., Khorrami, Z.: Artificial intelligence in screening, diagnosis, and classification of diabetic macular edema: a systematic review. Surv. Ophthalmol. **68**, 42–53 (2023). https://doi.org/10.1016/j.survophthal.2022.08.004
3. Paul, W., et al.: Accuracy of artificial intelligence in estimating best-corrected visual acuity from fundus photographs in eyes with diabetic macular edema. JAMA Ophthalmol. **141**, 677–685 (2023). https://doi.org/10.1001/jamaophthalmol.2023.2271
4. Shazuli, S.I.S.M., Saravanan, A.: Improved whale optimization algorithm with deep learning-driven retinal fundus image grading and retrieval. Eng. Technol. Appl. Sci. Res. **13**(5), 11555–11560 (2023)
5. Syed, A.M., Akram, M.U., Akram, T., Muzammal, M., Khalid, S., Khan, M.A.: Fundus images-based detection and grading of macular edema using robust macula localization. IEEE Access **6**, 58784–58793 (2018). https://doi.org/10.1109/ACCESS.2018.2873415
6. Acharya, U.R., et al.: Automated diabetic macular edema (DME) grading system using DWT, DCT Features and maculopathy index. Comput. Biol. Med. **84**, 59–68 (2017). https://doi.org/10.1016/j.compbiomed.2017.03.016
7. Zubair, M., Umair, M., Ali Naqvi, R., Hussain, D., Owais, M., Werghi, N.: A comprehensive computer-aided system for an early-stage diagnosis and classification of diabetic macular edema. J. King Saud Univ.-Comput. Inf. Sci. **35**, 101719 (2023). https://doi.org/10.1016/j.jksuci.2023.101719

8. Muchori, G.N., Al-Absi, H.R.H., Musleh, S., Islam, M.T., Alam, T.: Diabetic macular edema detection based on non-mydriatic retinal image. In: ICCIT, pp. 302–307 (2023). https://doi.org/10.1109/ICCIT58132.2023.10273917
9. dos Santos, J.C.M., Carrijo, G.A., de Fátima dos Santos Cardoso, C., Ferreira, J.C., Sousa, P.M., Patrocínio, A.C.: Fundus image quality enhancement for blood vessel detection via a neural network using CLAHE and Wiener filter. Res. Biomed. Eng. **36**, 107–119 (2020). https://doi.org/10.1007/s42600-020-00046-y
10. Wu, T., Liu, L., Zhang, T., Wu, X.: Deep learning-based risk classification and auxiliary diagnosis of macular edema. Intell. Based Med. **6**, 100053 (2022). https://doi.org/10.1016/j.ibmed.2022.100053
11. Nagendra Prasad, Y., Shoba Bindu, C., Sudheer Kumar, E., Dileep Kumar Reddy, P.: An Automatic Identification of Diabetic Macular Edema Using Transfer Learning, pp. 533–541 (2021). https://doi.org/10.1007/978-981-16-1941-0_53
12. Nage, P., Shitole, S., Kokare, M.: An intelligent approach for detection and grading of diabetic retinopathy and diabetic macular edema using retinal images. Comput. Methods Biomech. Biomed. Eng. Imaging Vis. **11**, 1625–1640 (2023). https://doi.org/10.1080/21681163.2022.2164358
13. Tuyet, V.T.H., Binh, N.T., Tin, D.T.: Improving the curvelet saliency and deep convolutional neural networks for diabetic retinopathy classification in fundus images. Eng. Technol. Appl. Sci. Res. **12**(1), 8204–8209 (2022)
14. Yuan, Z., et al.: CLAHE-based low-light image enhancement for robust object detection in overhead power transmission system. IEEE Trans. Power Delivery **38**, 2240–2243 (2023). https://doi.org/10.1109/TPWRD.2023.3269206
15. Jabbar Hussein, Z., Hamood Al-Saadi, E.: The optic disc detection and segmentation in retinal fundus images utilizing you only look once (YOLO) method. Int. J. Comput. Digit. Syst. **15**(1), 509–528 (2024). https://doi.org/10.12785/ijcds/160139
16. French, (MESSIDOR) Methods for Evaluating Segmentation and Indexing Techniques Dedicated to Retinal Ophthalmology in France. https://www.adcis.net/en/third-party/messidor/
17. Porwal, P., et al.: Indian Diabetic Retinopathy Image Dataset (IDRiD), IEEE Dataport (2018). https://ieee-dataport.org/open-access/indian-diabetic-retinopathy-image-dataset-idrid
18. Hussein, Z.J., Hussein, A.M., Maki, G.I., Gheni, H.Q.: Improved model for skin illnesses classification utilizing gray-level co-occurrence matrix and convolution neural network. J. Adv. Inf. Technol. **14**(6), 1273–1279 (2023). https://doi.org/10.12720/jait.14.6.1273-1279
19. Bhalekar, M., Bedekar, M.: D-CNN: a new model for generating image captions with text extraction using deep learning for visually challenged individuals. Eng. Technol. Appl. Sci. Res. **12**(2), 8366–8373 (2022)

The Green Smart Refill: Integrating Artificial Intelligence (AI) and Education of Things (EoT) in Vietnam National University, Hanoi, Vietnam

Bui Thi Thanh Huong[1(✉)], Nguyen Thi Linh Yen[2], R. S. S. Nehru[3], Chu Thi Hong Nhung[4], Nguyen Ngoc Tuan[5], and Hoang Thu Huyen[6]

[1] VNU School of Interdisciplinary Sciences and Arts, Hanoi, Vietnam
buithanhhuong.vn@vnu.edu.vn
[2] VNU University of Languages and International Studies, Hanoi, Vietnam
[3] Department of Education, Sikkim University, Gangtok, Sikkim, India
[4] VNU University of Education, Hanoi, Vietnam
[5] Hanoi Pedagogical University 2, Hanoi, Vietnam
[6] Hanoi Metropolitan University, Hanoi, Vietnam
hthuyen@daihocthudo.edu.vn

Abstract. This study examines the Green Smart Refill initiative at Vietnam National University, Hanoi, which integrates Artificial Intelligence (AI) and the Education of Things (EoT) to enhance sustainability in educational practices. The Smart Refill system, a pioneering automatic personal consumption service, allows users to flexibly refill and reuse various consumer products, prioritizing green consumption trends such as limiting plastic packaging. The initiative leverages IoT technology to connect hardware like supply machines and payment gateways, facilitating efficient transactions and resource management. Vietnamese software manages this system's innovative design, ensuring independence from foreign technology. Integrating AI and EoT optimizes resource usage, reduces environmental impact, and promotes personalized, interactive learning experiences. This approach advances the university's sustainability goals and serves as a model for incorporating smart technologies into teacher training program as well as in education, contributing to the broader effort of green transformation across Vietnam.

Keywords: Artificial Intelligence · Education of Things · Sustainability · Vietnam National University · Green Smart Refill

1 Introduction

Overview of Green Technologies in Education

Integrating green technologies in education has gained significant momentum worldwide, particularly as educational institutions strive to reduce their environmental impact. Green technologies encompass a range of practices and innovations designed to minimize energy consumption, reduce waste, and promote sustainability. In the educational sector, these technologies are implemented through energy-efficient buildings, digital

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 412–420, 2025.
https://doi.org/10.1007/978-3-031-91008-1_36

learning tools, and environmentally conscious curricula [2]. The advent of Artificial Intelligence (AI) and the Internet of Things (IoT) has further propelled this movement, offering smart solutions that enhance learning while contributing to environmental sustainability. This intersection of AI, IoT, and education - the Education of Things (EoT) - provides a framework for creating smart, sustainable learning environments, and for making education more **efficient, personalized, and data-driven**, improving learning outcomes by blending digital and physical worlds.

The Need for Sustainable Educational Practices at Vietnam National University, Hanoi (VNU)

Vietnam National University Hanoi, a leading academic institution, faces challenges common to many universities in developing regions. As the demand for education grows, so does the need for sustainable practices to support this expansion without depleting resources or harming the environment. Current educational models often rely heavily on physical infrastructure and traditional methods that are not always energy-efficient or sustainable. There is an urgent need to shift towards more sustainable practices integrating AI and EoT technologies, thus creating a smarter and greener educational environment. This shift is essential to meet the university's long-term sustainability goals and to serve as a model for other institutions in Vietnam and beyond.

Vietnam National University, Hanoi (VNU), is one of the premier educational institutions in Southeast Asia, known for its strong commitment to academic excellence and innovation. The university has made significant strides in integrating technology into its educational framework. It is supported by a robust infrastructure that includes state-of-the-art research facilities, high-speed internet connectivity, and a growing focus on smart learning environments. Despite these advancements, there is a growing need to further enhance the university's technological capabilities by integrating Artificial Intelligence (AI) and the Education of Things (EoT). This integration is essential for fostering a more sustainable and efficient educational model that aligns with global trends in green technologies.

Exploring the Integration of AI and EoT in Creating a Sustainable Educational Model

This paper explores the integration of AI and EoT at Vietnam National University to create a sustainable educational model. Specifically, it will examine how these technologies can reduce energy consumption, optimize resource management, and enhance the learning experience. The objectives include identifying the key components of a green smart learning environment, assessing the current state of AI and EoT integration at the university, and proposing strategies for further implementation. By focusing on these areas, the study provides a roadmap for the university to achieve its sustainability goals through technological innovation.

The Potential Impact on Vietnam's Educational System and Environmental Sustainability

Integrating AI and EoT into Vietnam National University's educational model could revolutionize the institution and the broader educational landscape in Vietnam. By adopting these technologies, the university can significantly reduce its environmental footprint, promote energy efficiency, and set a precedent for other institutions. Additionally,

the successful implementation of green smart learning environments can enhance the quality of education by providing more personalized, efficient, and effective learning experiences [3]. This contributes to environmental sustainability and positions Vietnam National University as a leader in the global movement toward greener education systems.

2 Literature Review

2.1 Green Technologies in Education: Historical and Current Perspectives

Green technologies in education have evolved from simple resource-saving initiatives to sophisticated, technology-driven solutions aimed at reducing the environmental impact of educational institutions [1]. Historically, these efforts focused on energy conservation, waste reduction, and promoting environmental awareness among students. In recent years, integrating advanced technologies such as solar panels, smart grids, and sustainable building materials has become more prevalent, leading to developing "green" campuses. At Vietnam National University, Hanoi, these technologies are being increasingly adopted to create a more sustainable learning environment.

2.2 Artificial Intelligence (AI) in Education: Applications and Benefits

AI has transformed education through personalized learning, adaptive assessments, and intelligent tutoring systems. AI-driven platforms can analyze student data to provide customized learning experiences, improving educational outcomes. Additionally, AI tools can help educators manage administrative tasks, allowing them to focus more on teaching. Implementing AI in Vietnam's educational institutions, including Vietnam National University, can enhance teaching efficiency and student engagement, contributing to a more effective and sustainable educational model [2].

2.3 Education of Things (EoT)

Integrating Artificial Intelligence (AI) and Education of Things (EoT) has become increasingly important in enhancing educational environments. Nehru and Chakraborty (2020) examined how IoT applications can transform traditional education into smarter, more efficient systems [2]. Their research highlighted EoT's potential to create interactive, personalized learning experiences while addressing key issues like system reliability, quality control, and safety. This framework is particularly relevant for Vietnam's National University in Hanoi, where AI and IoT are implemented through initiatives like the Green Smart Refill [1, 3, 9]. These efforts align with global trends in green technology and digital transformation, offering sustainable solutions for modern education. The study emphasizes the need to further explore these technologies to support sustainable educational practices.

2.4 Sustainability in Higher Education: Global and Regional Trends

Globally, there is a growing emphasis on sustainability in higher education, driven by the need to address climate change and environmental degradation. Universities worldwide are adopting sustainable practices, from green building designs to integrating sustainability into the curriculum. In Vietnam, sustainability in higher education is gaining momentum, with institutions like Vietnam National University, Hanoi, leading the way. These efforts align with the global push towards the United Nations' Sustainable Development Goals (SDGs), particularly Goal 4, which aims to ensure inclusive and equitable education and promote lifelong learning opportunities for all [6].

3 Methodology

Research Design
A mixed-methods approach was selected to comprehensively explore the integration of AI and IoT at Vietnam National University. This design merges quantitative and qualitative methods, enabling a robust analysis of the subject matter. The quantitative aspect primarily involves surveys, while the qualitative aspect incorporates interviews and case studies. By blending these methods, the research provides a nuanced understanding of how AI and EoT can enhance sustainable educational practices at the university.

Data Collection
Data collection for this study was carried out using three primary methods: surveys, interviews, and case studies. Surveys were distributed to a large sample of students and faculty members at Vietnam National University to gather broad insights into the current usage of AI and EoT technologies in educational settings. Following the surveys, in-depth interviews were conducted with key stakeholders, including university administrators, educators, and technology experts, to gain detailed perspectives on the challenges and opportunities presented by AI and IoT. Additionally, case studies of specific courses or programs that have successfully integrated these technologies were analyzed to highlight best practices and potential pitfalls.

Data Analysis
The collected data were analyzed using both statistical and thematic analysis techniques. Statistical analysis was applied to the survey data to identify trends, correlations, and significant differences in using AI and EoT across various university academic departments and user groups. Thematic analysis was employed to interpret the qualitative data from interviews and case studies, enabling the identification of key themes and patterns related to the implementation and impact of these technologies. This dual approach ensured that the findings were comprehensive and deeply insightful, providing a strong foundation for drawing conclusions and making recommendations.

4 Case Study: School of Interdisciplinary Sciences and Arts, VNU

Implementation and Commercialization of the Smart Refill System in Vietnam
In 2022, Vietnam emerged as one of the top contributors to global marine plastic waste, with a staggering 3.1 million tons of plastic waste, equivalent to the total plastic waste generated by Europe in the 2010s. This situation has highlighted the urgent need for innovative solutions to address plastic waste, particularly in a country where an average of 31kg of plastic is discarded per citizen annually. Vietnam has prioritized green and digital transformations to tackle this issue, focusing on circular economy principles. According to World Bank Report 2022 (the study was conducted from July 2020 to April 2021), plastic waste was by far the most abundant type of waste collected in the field surveys (around 94% in the number of items; and around 71% by weight) [11] (Fig. 1).

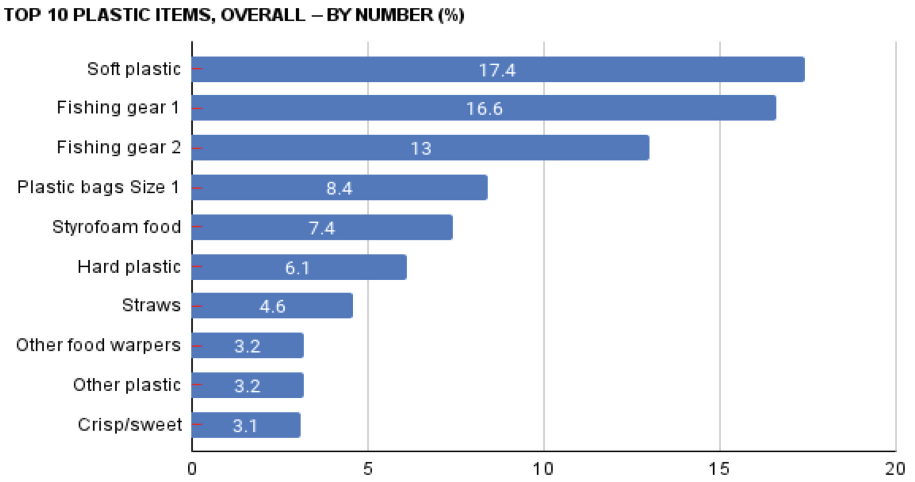


Fig. 1. The top 10 plastic waste items, which the field surveys identified at 38 river and coastal sites in Vietnam (Sources: WB Report [11, 12])

The Smart Refill system, developed by Greentech - a university-based startup aims to reduce plastic waste by offering a sustainable alternative to single-use plastic packaging. This system integrates advanced IoT technology, mobile app control, and automation to enable the refilling of liquid products, such as detergents and cleaners, in a user-friendly and environmentally friendly manner. After extensive testing at the Interdisciplinary University of Arts and Sciences, the Smart Refill system demonstrated significant potential to reduce plastic waste, cutting down up to 10,000 plastic bottles per day in pilot locations.

After two years of piloting the Smart Refill system in the laboratory, the software system (which has been registered) and the circuit boards (used to control the connection between hardware and software) have been deployed. The smart refill vending machines allow customers to purchase liquids in quantities as small as 50ml, with payment options including cash, QR code, and RFID cards. The web-server system features account

and password-based management for members and a management system. The mobile app supports administrators, agents, and customers by displaying machine locations, available liquid types, and the remaining amount of liquid in the machines. The system has been tested at the School of Interdisciplinary Sciences and Arts, initially attracting consumers who are students of the school. The cash flow is steadily maintained on a daily basis.

Despite its promise, the commercialization of the Smart Refill system has faced challenges, particularly in changing consumer habits and competing with established products. However, the system's ability to align with Vietnam's environmental policies, such as the Law on Environmental Protection 2020, positions it as a critical innovation for reducing plastic waste and promoting sustainable consumption practices.

This case study underscores the importance of continuous innovation and the role of academic institutions in driving sustainable development through practical applications of scientific research. The Smart Refill system exemplifies how startups and spin-offs can contribute to national and global environmental goals, fostering a greener future through technological advancements.

Current Infrastructure and Technological Capabilities Implementation Strategy: Step-by-Step Process of Integrating AI and EoT

Implementing AI and EoT at VNU will follow a carefully planned, step-by-step approach to ensure effective integration and minimal disruption to existing processes. The first phase involves conducting a comprehensive assessment of the university's current infrastructure to identify areas where AI and EoT can be most effectively deployed. The university will initiate pilot programs within selected departments to test the integration of smart devices and AI-powered learning tools. The next step will be scaling these solutions across the campus, focusing on smart classrooms, automated administrative processes, and real-time data analytics for better decision-making. Throughout this process, there will be ongoing training for faculty and staff to ensure they are fully equipped to utilize these new technologies (Fig. 2).

Expected Outcomes: Academic and Environmental Benefits

Integrating AI and EoT at the School of Interdisciplinary Sciences and Arts, VNU Hanoi will yield substantial academic and environmental benefits. Academically, the university will enhance the quality of education by providing personalized learning experiences, optimizing administrative operations (including STEM approaches), and fostering innovative research through AI-powered data analytics. Environmentally, the smart learning environment will contribute to sustainability by reducing energy consumption, minimizing waste, and promoting the efficient use of resources. The long-term goal is to establish VNU as a leader in green education in Vietnam, setting a benchmark for other regional institutions.

Over a period of two years (2022–2024), the results of this research have been applied in teacher training and STEM education in four coastal provinces of northern Vietnam. The project's outputs have been showcased for STEM teaching following the 5E (Engage, Explore, Explain, Elaborate, and Evaluate) and Engineering Design Process (EDP) approaches [4].



Fig. 2. The Smart Refill Machine at the workshop integrated control circuits connected to IoT at the School of Interdisciplinary Sciences and Arts, VNU Hanoi

5 Discussion

Impact on Education: Transforming Learning Environments with AI and EoT
Integrating Artificial Intelligence (AI) and the Education of Things (EoT) at Vietnam National University, Hanoi, marks a pivotal step in modernizing education. AI facilitates personalized learning, allowing adaptive systems to tailor content to individual student needs, creating a more inclusive and effective learning environment. This approach accommodates diverse abilities and learning speeds, ensuring students can progress at their own pace. EoT further enhances this transformation by incorporating smart devices into the educational framework, enabling real-time data exchange and fostering interactive learning experiences. Together, these technologies improve educational outcomes and equip students with the skills needed for a technology-driven workforce.

Implementation and Commercialization of the Smart Refill System in Vietnam
Innovative solutions have become imperative in response to Vietnam's substantial contribution to global marine plastic waste - 3.1 million tons in 2022. Vietnam has prioritized green and digital transformations, focusing on the circular economy, to address this environmental challenge. The Smart Refill system, developed by Greentech, a university-based startup, offers a sustainable alternative to single-use plastic packaging. Integrating advanced IoT technology, mobile app control, and automation facilitates refilling liquid products like detergents and cleaners, significantly reducing plastic waste. Pilot tests at the Interdisciplinary University of Arts and Sciences have shown the system's potential to eliminate up to 10,000 plastic bottles daily.

Despite these successes, commercialization has faced hurdles, particularly in shifting consumer habits and competing with established products. However, the Smart Refill system's alignment with Vietnam's environmental policies, such as the Law on Environmental Protection 2020 [8], underscores its importance in promoting sustainable consumption practices. This case study highlights the critical role of academic institutions in driving sustainable development through the practical application of scientific research [9]. The Smart Refill system models how startups and spin-offs can contribute to national and global environmental goals, fostering a more sustainable future through technological innovation.

Sustainability Outcomes: Reduction in Resource Consumption and Carbon Footprint
Adopting green technologies through AI and EoT contributes significantly to sustainability efforts [6]. By utilizing AI-driven energy management systems, educational institutions can optimize energy usage, reducing unnecessary consumption. EoT further supports these efforts by enabling smart classrooms that adjust lighting, heating, and cooling based on occupancy and usage patterns. The result is a considerable reduction in the university's carbon footprint [7]. Moreover, the transition to digital resources decreases the reliance on paper-based materials, contributing to preserving natural resources.

Scalability: Potential for Broader Implementation Across Vietnam
The successful implementation of AI and EoT at Vietnam National University is a model for broader adoption across the country's educational system. The scalability of these technologies allows for their application in various educational contexts, from primary schools to higher education institutions. As the technology becomes more accessible, the potential for widespread adoption increases, promoting a nationwide shift towards sustainable and innovative educational practices. This scalability enhances educational quality across Vietnam and aligns with global sustainability goals.

6 Conclusion and Recommendations

Integrating Artificial Intelligence (AI) and the Education of Things (EoT) within Vietnam National University in Hanoi reveals significant potential for creating a sustainable educational model. The key takeaways include identifying AI and EoT as critical drivers for enhancing educational outcomes while promoting environmental sustainability. Implementing these technologies has shown promise in reducing the carbon footprint of educational activities and fostering a more interactive and personalized learning environment for students.

Implications for Future Research
The findings of this study open up several avenues for future research. One crucial area for further investigation is the long-term environmental impact of AI and EoT integration in educational settings. Additionally, exploring the scalability of these technologies in other educational institutions across Vietnam could provide insights into their broader applicability and effectiveness. Research into the potential socio-economic impacts of

these innovations on students and educators will also be vital for understanding the broader implications of this technological shift.

Recommendations

Based on the study's findings, several recommendations can be made to policymakers and educational stakeholders. First, it is essential to establish clear guidelines and policies that encourage the adoption of AI and EoT technologies in educational institutions. These policies should emphasize the importance of sustainability and environmental responsibility in technology integration. Furthermore, investments in training programs for educators to effectively utilize these technologies are crucial. Finally, ongoing monitoring and evaluation should be implemented to assess the environmental and educational impacts of AI and EoT, ensuring that these technologies align with sustainability and educational excellence goals.

References

1. Greentech. Smart Refill system development and implementation [Case Study] (2022). https://journalofbigdata.springeropen.com/articles/10.1186/s40537-024-00920-x
2. Nehru, R.S.S., Chakraborty, S.: The education of things (IoT) for smart learning through EoT intervention: a case study based analysis. In: Gunjan, V., Garcia Diaz, V., Cardona, M., Solanki, V., Sunitha, K. (eds.) ICICCT 2019 – System Reliability, Quality Control, Safety, Maintenance and Management, pp. 679–690. Springer, Singapore (2020). https://doi.org/10.1007/978-981-13-8461-5_60
3. Pham, D.T., Tran, N.Q.: Greening smart learning environments with Artificial Intelligence of Things. ResearchGate (2024). https://www.researchgate.net/publication/376839441_Greening_smart_learning_environments_with_Artificial_Intelligence_of_Things
4. Pham, T.Q., Dang, T.M., Nguyen, H.T., Ngo, L.T.: Fostering STEM education competency for elementary education students at universities of pedagogy in Vietnam. In: Peng, SL., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.) Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. ICMMCS 2023. Advances in Intelligent Systems and Computing, vol. 1450. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3_9
5. Raman, R.: Green and sustainable AI research: an integrated thematic overview. J. Big Data (2024)
6. UNESCO. Technology in education: A case study on Viet Nam (2024). https://unesdoc.unesco.org/ark:/48223/pf0000387747
7. Vietnam Government. Law on Environmental Protection 2020. [Legislation] (2020)
8. Vietnam National Administration of Tourism. Ha Noi (2024). https://vietnam.travel/places-to-go/northern-vietnam/ha-noi
9. Vo, T.T., Bui, P.H.: Education for sustainable development in Vietnam: Lessons learned from teacher education. Research Gate (2024). https://www.researchgate.net/publication/309728387_Education_for_sustainable_development_in_Vietnam_lessons_learned_from_teacher_education
10. Wikipedia contributors. Hanoi (2024). https://en.wikipedia.org/wiki/Hanoi
11. World Bank. Vietnam: Plastic Pollution Diagnostics [Report] (2022)
12. World Bank. Toward a National Single-use Plastics Roadmap in Vietnam: Strategic Options for Reducing Priority Single-use Plastics [Report] (2022)

Design and Development of Novel Hybrid Cryptography Technique for Enhancing Data Security

Yuvraj Singh[1](✉), Arun Malik[1], Isha Batra[1], and Manzoor Hussain[2]

[1] Lovely Professional University, Phagwara, Punjab, India
yurajsryou@gmail.com
[2] Indus University, Karachi, Pakistan
manzoor.hussain@indus.edu.pk

Abstract. This paper explores how data security changes by examining hybrid symmetric cryptography and classical ciphers. It explores how ciphers such as the Caesar Cipher, Rail Fence Cipher, and Playfair Cipher can be efficiently combined into a large hybrid cryptographic architecture, with a focus on key management protocols and improved encryption robustness The review of the literature includes modified classical ciphers and highlights how effective they are in reducing the weaknesses and boosting the security of cryptography. Important conclusions highlight the value of the cipher integration or combination in enhancing the data availability, data confidentiality, and the data integrity. The research gaps that have been identified, highlight the potential to improves the key management protocols, then enhance encryption techniques and effectively combine the hybrid cryptographic systems with the current security architectures. The Complex cipher combinations, AI/ML integration, standardization initiatives, performance optimization, scalability improvements, and post-quantum cryptography concepts are all included in the future scope.

Keywords: Cryptography · Classical Ciphers · Hybrid Cryptography techniques

1 Introduction

As the world turns into more and more virtual, protective touchy bills has become increasingly more vital. The key to making sure the confidentiality, integrity and authenticity of the information supplied is cryptography, a technique that is predicated totally on changing simple textual content into cipher textual content [1]. In order to enhance facts protection to previously unheard-of levels, this has a look at explores the appearance of a completely unique hybrid symmetric cryptography method that makes use of the blessings of several symmetric cryptographic algorithms, which incorporates the Caesar cipher [2], Rail Fence cipher [3], and Playfair cipher [4].

Efficiency, speed, and simplicity are three fundamental benefits of the symmetric key cryptography, which makes the use of a single key for both the encryption and

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 421–433, 2025.
https://doi.org/10.1007/978-3-031-91008-1_37

decryption [5]. Traditional symmetric key algorithms may want to run into problems with key distribution, administration, and the attack susceptibility [6].

The proposed hybrid symmetric cryptographic method combines several symmetric key strategies, every of which is selected for its blessings and class [7]. Through strategic integration algorithms together with the Caesar Cipher, Rail Fence Cipher, and Playfair Cipher, our intention is to reinforce the overall protection abilities whilst addressing the shortcomings of character channels.

In a Caesar cipher, every letter in smooth text is moved down the alphabet thru a predetermined number of positions [8]. It is idea for its records and simplicity. In evaluation, the Rail Fence cipher divides plaintext characters in a zigzag fashion over more than one rails in advance than encrypting them [9]. The Playfair cipher uses a predefined key matrix and precise character substitution regulations to encrypt characters [10].

Our hybrid approach includes methodological analysis of encryption/decryption techniques, key management protocols, overall performance metrics, and performance interfaces with modern security systems We aim to demonstrate our hybrid symmetric cryptography approach demonstrated effectiveness and utility in a practical information security environment through comprehensive research and study [11].

Our observation dramatically improves information safety in important fields with the aid of pushing the bounds of symmetric key cryptography and making use of the complementary qualities of several symmetric cryptographic algorithms, including the Caesar cipher, Rail Fence cipher, and Playfair cipher. In an interconnected virtual panorama, protecting the confidentiality and integrity of touchy facts even as reducing cyber threats is made substantially less difficult the usage of the modern hybrid symmetric cryptography technique defined in this work.

2 Background of Study

2.1 Plain Text

In the context of cryptography, plain text is the original, unencrypted version of a data or message that can be read and understood by humans. Represent the information as it is before any of the encryption methods are applied. When it comes to encryption, plain text is input data that is transformed using cryptographic techniques to create ciphertext, or an encrypted message. The difference between plaintext and ciphertext, and the encrypted version of data is what makes plaintext important. Encryption schemes are developed to convert plain text into ciphertext using encryption keys or algorithms to prevent unauthorized persons from downloading or accessing sensitive data without the required decryption key.

2.2 Cipher Text

In the context of cryptography, a cipher textual content is the encrypted version of a message or any information this is generated by way of using any of the encryption methods or any encryption algorithms. The Cipher text content appears as a jumbled and

a unreadable string of characters or symbols, in assessment to plain textual content, which is the original and the human-readable shape of the records. The cipher textual content is used to shield the integrity and confidentiality of the records beneath via making sure that anyone who isn't allowed can't get entry to or understand the information without the right decryption keys or algorithms. Cipher text content is created through the encryption of the obvious textual content by way of the use of techniques like substitution ciphers, advanced cryptographic algorithms like Rivest-Shamir-Adleman (RSA) or AES (Advanced Encryption Standard), or the mathematical operations. The sturdiness of the encryption algorithm, the duration and the complexity of the encryption key, and the encryption technique applied all have an effect on how strong and steady the encrypted text is. To protect the sensitive data at some point of transmission or storage.

2.3 Encryption

A form of encryption converts readable data, or plain text, into an unintelligible form called ciphertext. To ensure that data cannot be accessed or interpreted by unauthorized persons without an accompanying decryption key, data encrypted using algorithms or ciphers in this manner encrypts time critical information sending or storing Encryption plays an important role in maintaining the privacy and confidentiality of the data. The present-day encryption standards along with AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) use the complex accounting algorithms to improve the safety Encryption is broadly used in the virtual transactions, monetary transactions and the records storage structures to save you the unauthorized access and defend statistics integrity.

2.4 Decryption

In context of cryptography, the decryption is the opposite, or we can say the reverse of the encryption, returning ciphertext—an encrypted model of data—to its original plaintext layout. A decryption key or the set of rules that undoes the encryption-related adjustments have to be used for this manner. In order for legal customers to study and understand encrypted records, decryption is necessary for retrieving and having access to it. Depending at the encryption technique hired, the ciphertext is subjected to mathematical operations or reverse transformation during decryption. Asymmetric encryption uses exclusive public and personal keys than symmetric encryption, which makes use of the equal key for each encryption and decryption. By permitting legal events to soundly access and understand touchy fabric, decryption ensures information secrecy at the same time as preserving the integrity and privateness of the statistics at some point of the encryption-decryption cycle (Fig. 1).

2.5 Classical Cipher

The older encryption methods, which are known as "classical ciphers" were in use before the development of the modern cryptographic algorithms/techniques. These ciphers work by encrypting the provided plaintext into ciphertext by transposing or substituting the letters. These are a few examples of traditional ciphers:

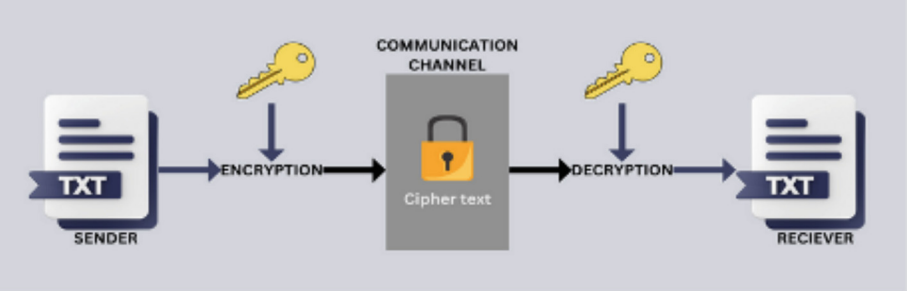


Fig. 1. How Encryption And Decryption works

Caesar Cipher: This cipher moves every letter in the plaintext up or down the alphabet by a predetermined amount. For example, in context of ASCII numbers, if a shift of three, makes 'A' as 'D', and 'B' to become 'E', and so on (Fig. 2).

Actual letters	A	B	C	D	E	F	G	H	I	J	K	L	M
After 3 places	D	E	F	G	H	I	J	K	L	M	N	O	P

Actual letters	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
After 3 places	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Fig. 2. Working of Caeser Cipher

Substitution Cipher: This kind of the cipher uses a different letter or number, or symbol in the place of each letter in the plaintext. The "Monoalphabetic Substitution Cipher", wherein replacement of every letter is accomplished, within the provided message or in the apparent textual content uniformly, is the maximum well-known substitution cipher.

Transposition Cipher: The Transposition ciphers actually generate the cipher text by doing the rearrangement of the characters in the plaintext in a specific order or manner. A prime example is the "Rail Fence Cipher", in which the ciphertext is formed by reading out the letters in rows after they are typed diagonally. Ex: Rail fence Cipher (Figs. 3 and 4).

Vigenère Cipher: Unlike the Caesar cipher, the Vigenère cipher creates a more intricate pattern by using a keyword to shift each plaintext letter by an amount that is different.

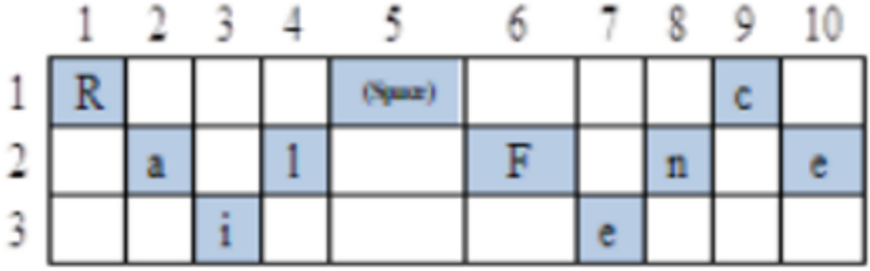


Fig. 3. Encryption Process of Rail Fence



Fig. 4. Circular Left Shift and Right Shift

3 Literature Survey

Modern encryption algorithms are built on the basis of classical ciphers, which have lengthy been an important element of secure conversation within the area of cryptography. The articles covered on this dialogue explore a couple of aspects of classical ciphers, stressing their blessings, disadvantages, and room for improvement so that you can fulfill the changing needs of digital conversation security.

These classical techniques introduce important insights through advanced crypto design based on modified versions of classical ciphers—in particular, the Vigenère-Polybius cipher [12] The intention of these classical techniques is to reduce vulnerabilities found in traditional systems. The authors increase security and complexity by mixing different ciphers, leading to interesting developments in cryptography. Using modified Vigenère and Polybius ciphers as the foundation, [13] builds on this idea by examining the idea of an improved cryptosystem. The study highlights how these changes, when compared to traditional ciphers like the Caesar Cipher, offer increased security. This shows the necessity it is to modify traditional methods for dealing with modern security issues.

On the other hand, [14] actually analyzes the field of Playfair ciphers and examines the three enhanced versions of the 3D Playfair Cipher. The study ends with an analysis

of the progress made in Playfair cipher cryptography, setting the foundation for more interesting advances in the areas of cryptography in the future. Further to the discussion of modified classical ciphers, [15] gives an analysis of several encryption systems that use Caesar and affine ciphers to provide secure communication. The study shows how important confidentiality is and how complicated modified classical ciphers can be, making cryptanalysis a difficult task. In a comparable manner, [16] provides an analysis on different parameters found in the classical cipher technique, that highlighting their major importance in relation to transposition and substitution ciphers.

This comparison offers a very useful knowledge about the disadvantages and the advantages of various traditional techniques for encryption. 'Two Way Cipher Transposition' and 'Disorder Cipher Transpositions' are being analyzed by [17] as more stronger and practical substitutes for older transposition Algorithms, in a practical examination of applied classical cipher techniques. This research investigation shows how crucial it is to always use trustworthy encryption techniques in practical applications.

[18] discusses that the security analysis and modification of older encryption methods including the Caesar, Vigenère, Affine, and Hill ciphers, showing the necessity for increased security. By reducing the complexity of computations, the improved method that has been suggested aims to improve security while tackling the problems associated to key space management. In a comparative analysis of classical substitution ciphers, [19] highlights the security and efficiency of algorithms such as Affine, Atbash, and Caesar ciphers. The results highlight the Caesar cipher's power in terms of security and implementation, providing important fresh insight for cipher selection techniques.

Finally, to improve the security, [20] proposes a unique cipher approach that combines both the transposition and substitution techniques. Through the correction of weaknesses in the traditional ciphers such as the Caesar cipher and Hill cipher, the suggested algorithm presents an appealing option for safe communication. Various lightweight authentication schemes and cybersecurity frameworks have been proposed to enhance data security [21, 22], particularly for IoT devices and e-governance systems [23, 24] (Table 1 and Fig. 5).

Table 1. Comparative Analysis of Enhanced Cryptosystem Based on Modified Classical Ciphers

Authors and Reference	Key Points	Cryptographic Techniques	Security Aspects	Key Findings/Conclusion
Ritwic, Majumder., Sujoy, Datta., Monideepa, Roy. (2022) [12, 13]	Introduced improved cryptosystems that make use of altered Vigenère and Polybius ciphers	Vigenère Cipher, Polybius Cipher	Increased security, complexity	Enhanced security compared to traditional ciphers
	Emphasizes enhanced security in comparison to conventional classical ciphers			Weaknesses of classical ciphers discussed

(*continued*)

Table 1. (*continued*)

Authors and Reference	Key Points	Cryptographic Techniques	Security Aspects	Key Findings/Conclusion
Yuzhe, Wang. (2021) [14]	Examines three versions of the enhanced 3D Playfair Cipher	Playfair Cipher	Future development of Playfair ciphers	Insights into improved Playfair cipher versions
	Concludes on the future development of Playfair ciphers and cryptography			
Jayanti, Sravani. (2021) [15]	Proposes a number of altered encryption techniques for safe communication that make use of traditional ciphers	Affine Cipher, Caesar Cipher	Confidentiality, cryptanalysis difficulty	Importance of modified classical ciphers for secure communication
	Discusses confidentiality and making cryptanalysis difficult			
D, Venkata, Vidya, Deepthi., B, Homer, Benny., Konda, Sreenu. (2019) [16]	Compares and assesses several substitution and transposition cipher parameters	Substitution Ciphers, Transposition Ciphers	Significance in classical cryptography	Comparison of parameters used in classical ciphers
	Analyzes their significance in classical cryptography			
Rajendra, Gupta. (2017) [17]	Considers "Disorder Cipher Transpositions" and "Two Way Cipher Transpositions" to be more effective and practical methods	Two Way Cipher Transposition, Disorder Cipher Transpositions	Strength, convenience	Improved transposition techniques for better security
Maya, Mohan., M., K., Kavitha, Devi., V., Jeevan, Prakash. (2015) [18]	Explains traditional encryption techniques such as the Hill, Caesar, Vigenère and Affine ciphers	Caesar Cipher, Vigenère Cipher, Affine Cipher, Hill Cipher	Improved security using simple computations	Proposal of modified algorithm for better security
	Suggests a changed algorithm that makes use of basic calculations for increased security			

(*continued*)

Table 1. (*continued*)

Authors and Reference	Key Points	Cryptographic Techniques	Security Aspects	Key Findings/Conclusion
Anjlee, Verma., Navjot, Kaur. (2014) [19]	Evaluates the security and performance of traditional substitution ciphers	Affine Cipher, Atbash Cipher, Caesar Cipher, etc	Performance, security	Caesar cipher identified as best in terms of implementation, security
	Identifies Caesar cipher as the best in terms of implementation and security			
Lynelle, Watts. (2021) [20]	Suggests a cutting-edge cipher system that combines transposition and substitution techniques for increased security	Substitution, Transposition	Address vulnerabilities in classical ciphers	Enhanced security through novel cipher technique
	Fixes flaws in traditional ciphers such as the Hill and Caesar ciphers			

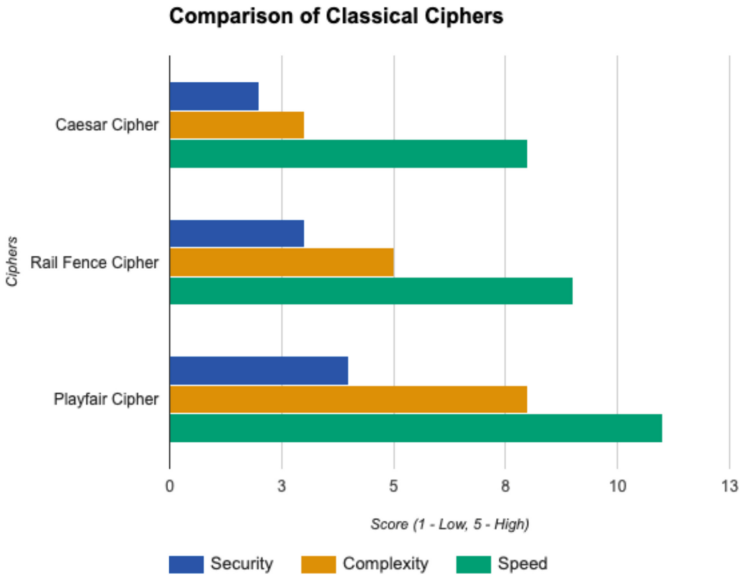


Fig. 5. Comparison of Classical Ciphers in terms of Security, Complexity and Speed.

4 Research Gap

Affine, Atbash, and Caesar ciphers and the enhanced Playfair cipher, modified classical ciphers such as the Vigenère and Polybius ciphers and modified encryption techniques using affine Caesar ciphers are just a few examples of the many technological improvements that results in classical ciphers and some of the researches have been revealed by the literature review. These studies highlight the importance of improving encryption techniques, reducing vulnerabilities, and providing security for secure communications. Despite these efforts, however, important research gaps remain to be addressed.

The lack of comprehensive studies combining modified versions of many ancient ciphers into hybrid cryptography is an important research gap. How the combination of these advanced ciphers improves overall security and encryption efficiency, even when separate studies focus on certain cipher modifications and their benefits, should be investigated. In addition, the majority of previous research often examines encryption methods in a vacuum, failing to take into account how they fit into current security frameworks, or the difficulties associated with their actual application.

To close this research gap, an in-depth assessment of hybrid symmetric cryptography's effectiveness is needed, one that takes into account key management protocols, performance measurements, compatibility with modern security frameworks, and many modified classical ciphers. Additionally, little research has been done on assessing the adaptability and scalability of hybrid symmetric cryptography systems in various information security contexts. Understanding the complicated nature of integration, performance trade-offs, and scalability issues associated with these systems is crucial for their practical implementation and efficient protection of private data. Conclusion Hybrid

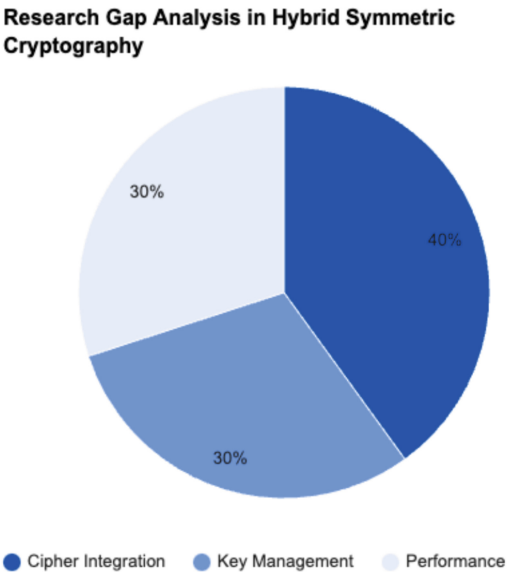


Fig. 6. Research Gap Analysis in Hybrid Symmetric Cryptography.

symmetric cryptography still requires further research. This includes integrating several modified classical ciphers, solving basic implementation problems, testing performance hypotheses, and evaluating real-world application methods to achieve improved information security in digital environments (Fig. 6).

5 Future Scope

There are a number of possibilities that hybrid symmetric cryptography, which combines multiple modified classical ciphers, can take in terms of future study. The creation of the increasingly complex hybrid cryptographic algorithms that combines the advantages of the different classical ciphers with reducing their unique limitations would be one of the main areas of the research. This involves carrying out in-depth assessments of various cipher combinations in order to determine the best configurations to achieve the most improved performance and security. Furthermore, hybrid symmetric cryptography may be combined with AI and ML approaches in future studies.

Researchers can improve encryption key creation, management, and distribution procedures by utilizing Artificial Intelligence algorithms, strengthening the overall security posture of the cryptographic systems moreover, the machine learning models can be trained to identify and counteract the possible attacks or vulnerabilities on hybrid cryptography systems and strengthening their defenses against the new threats. The standardization and interoperability of hybrid cryptography systems is a crucial area for future research. The establishment of industry-wide standards is vital to guarantee smooth interoperability among diverse platforms, devices, and security frameworks for hybrid cipher setups, key management protocols, and encryption techniques.

This standardization endeavor would enable hybrid symmetric cryptography to be widely adopted. Studies should additionally give attention to improving the performance and the scalability of hybrid cryptography answers. With the creation of big records and IoT technology, facts quantities have accelerated substantially, and cryptographic systems need so that it will manage massive quantities encryption and decryption processes effectively. Experiments with hardware-accelerated encryption mechanisms, optimization algorithms, and the parallelization techniques can substantially improve the hybrid symmetric cryptography's scalability and overall performance.

Furthermore, the hybrid symmetric encryption mixed with post-quantum cryptography concepts can be the issue of future studies. Classical encryption strategies run the risk of being compromised by way of quantum attacks with the creation of quantum computing. The hybrid structures that integrate put up-quantum cryptographic basics allow the researchers to create the encryption algorithms which are proof against quantum computing and guarantee long-term security.

6 Conclusion

This study highlights the essential evolutions of the cryptographic approaches in strengthening the data security by synthesizing the lessons learned from the extensive literature review on the hybrid symmetric cryptography and classical ciphers. Combining the Caesar, Rail Fence, and Playfair ciphers with the other classical ciphers into a

hybrid symmetric cryptography framework represents a tactical perspective change in the favor of the stronger encryption security and key management procedures.

This analysis put light on the constantly evolving field of the cryptographic innovations by thoroughly examining the modified classical ciphers and their modifications to meet contemporary cryptographic requirements. Remarkable results highlight how well-planned cipher integration can or may improve information availability, secrecy, and integrity, all of which are very essential in the fight against the modern cyberthreats. Comparing traditional substitution and transposition ciphers provides essential new understandings of cryptographic resilience, performance metrics, and cipher selection paradigms. This comparative perspective makes it easier to understand the advantages, disadvantages, and the tactical factors related to the traditional cryptographic methods, which provides the way for accurate formulations of the cryptographic strategies.

Moreover, the research gaps that have been identified highlight the increasing possibilities for improving the encryption techniques, developing key management protocols, and smoothly integrating hybrid cryptographic systems with modern security infrastructures. The search for novel cipher concepts that combine substitution and transposition methods suggests a forward-thinking direction in cryptography research, one that will strengthen the data security in the digital ecosystem that is becoming more interrelated by the day. Essentially, this study summarizes the current state of hybrid symmetric cryptography and classical ciphers now and provides directions for the future research to strengthen the data security, adaptability, and cryptographic effectiveness. Combining traditional and modern cryptography techniques marks an important step toward strong data protection plans, which are necessary to secure the private data from constantly evolving cyberattacks (Fig. 7).

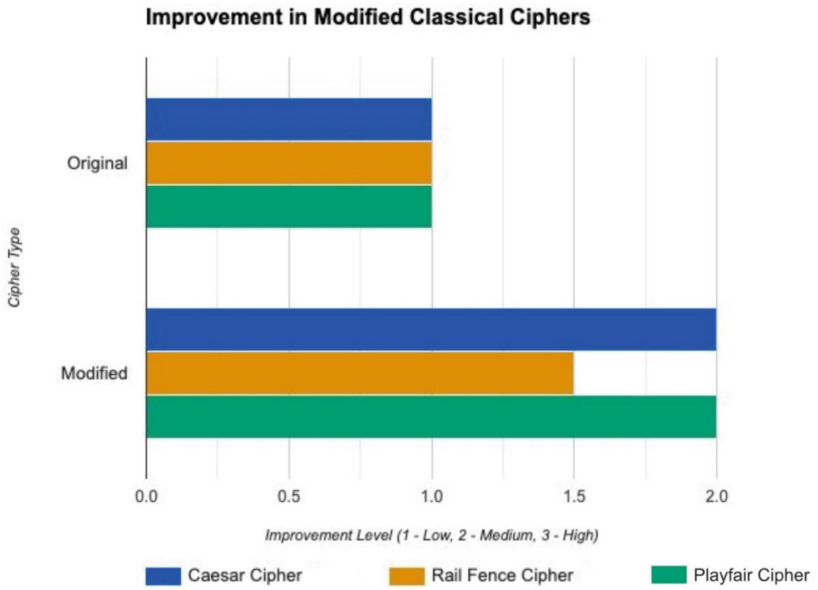


Fig. 7. Improvement in Modified Classical Ciphers in terms of Security.

References

1. Arora, S.: A review on various methods of cryptography for cyber security. J. Algebraic Stat. **13**(3), 5016–5024 (2022)
2. Thakkar, B., Thankachan, B.: A multilevel approach of transposition ciphers for data security over cloud. GIS Sci. J. **8**(5), 1732–1738 (2021)
3. Pristiwanto, P., Sunandar, H., Nadeak, B.: Analysis and implementation of playfair chipper algorithm in text data encoding process. Jurnal Info Sains: Informatika dan Sains **10**(2), 19–23 (2020)
4. Alshehri, J., Alhamed, A.: A review paper for the role of cryptography in network security. In: Proceedings of the 4th International Conference on Electrical, Control and Instrumentation Engineering (ICECIE), pp. 1–5. IEEE (2022)
5. Kaushik, B., Malik, V., Saroha, V.: A Review Paper on Data Encryption and Decryption (n.d.)
6. Maha, M.M., Masuduzzaman, M., Bhowmik, A.: An effective modification of play fair cipher with performance analysis using 6X6 matrix. In: Proceedings of the International Conference on Computing Advancements, pp. 1–6 (2020)
7. Kumar, S.: Review on Network Security and Cryptography (2015)
8. Nahar, K., Chakraborty, P.: Improved approach of rail fence for enhancing security. Int. J. Innov. Technol. Explor. Eng. **9**(9), 583–585 (2020)
9. Sugirtham, N., et al.: Modified playfair for text file encryption and meticulous decryption with arbitrary fillers by septenary quadrate pattern. Int. J. Netw. Distrib. Comput. (2024)
10. Rashid, O.F., Alobaidy, Z.A.H., Tuama, S.A.: Cryptography Techniques-A Review (2022)
11. Rachmawati, D., Budiman, M.A., Yusuf, A.: Combination of rail fence cipher algorithm and least significant bit technique to secure the image file. In: IOP Conference Series: Materials Science and Engineering, vol. 851, no. 1, p. 012069. IOP Publishing (2020)
12. An Enhanced Cryptosystem Based on Modified Classical Ciphers (2022). https://doi.org/10.1109/icaccs54159.2022.9785033
13. Ritwic, M., Datta, S., Roy, M.: An Enhanced Cryptosystem Based on Modified Classical Ciphers (2022). https://doi.org/10.1109/ICACCS54159.2022.9785033
14. Wang, Y.: A Classical Cipher-Playfair Cipher and Its Improved Versions (2021). https://doi.org/10.1109/EIECS53707.2021.9587989
15. Jayanti, S.: A Study on some modified Classical Ciphers for Secure Crypto-System (2021)
16. Venkata, D., Vidya, D., Homer, B., Benny, B., Sreenu, K.: Various Ciphers in Classical Cryptography (2019). https://doi.org/10.1088/1742-6596/1228/1/012014
17. Gupta, R.: A study of implemented classical cipher techniques for better security solution. Int. J. Res. Appl. Sci. Eng. Technol. (2017). https://doi.org/10.22214/IJRASET.2017.8180
18. Mohan, M., Kavitha, D., Jeevan, P., Prakash, V.: Security analysis and modification of classical encryption scheme. Indian J. Sci. Technol. (2015). https://doi.org/10.17485/IJST/2015/V8IS8/71506
19. Verma, A., Kaur, N.: A Comparative Study of Classical Substitution Ciphers. International Journal of Engineering Research and Technology (2014)
20. Watts, L.: A Novel Cipher Technique Using Substitution and Transposition Methods (2021). https://doi.org/10.1007/978-981-19-1122-4_14
21. Kumar, V., Malik, N., Singla, J., Jhanjhi, N.Z., Amsaad, F., Razaque, A.: Light weight authentication scheme for smart home iot devices. Cryptography **6**(3), 37 (2022)
22. Yadav, R.: Cyber security threats during covid-19 pandemic. Int. Trans. J. Eng. Manag. Appl. Sci. Technol. **12**(3), 1–7 (2021)
23. Jhanjhi, N.Z., Ahmad, M., Khan, M.A., Hussain, M.: The impact of cyber attacks on e-governance during the covid-19 pandemic. In: Cybersecurity Measures for E-Government Frameworks, pp. 123–140. IGI Global (2022)

24. Saeed, S., Jhanjhi, N.Z., Naqvi, M., Humayun, M., Ahmed, S.: Ransomware: a framework for security challenges in internet of things. In: 2020 2nd International Conference on Computer and Information Sciences (ICCIS), pp. 1–6. IEEE (2020)



Design and Implement an Interactive IoT Based Tamil Braille Keypad for Visually Impaired School Children

S. Suganthi[1(✉)], K. Kavitha[2], R. Rajapriya[2], and D. Usha[2]

[1] Department of Computer Science, G.Venkataswamy Naidu College, Kovilpatti, India
ssuganthi@gvncollege.edu.in

[2] Department of Computer Science, Mother Teresa Women's University, Kodaikanal, India

Abstract. Learning Braille is crucial for individuals with visual impairments, yet the Tamil Braille system primarily relies on traditional tools like Braille blocks, lacking modern, interactive educational alternatives. This paper presents an innovative system that introduces a tangible, interactive IoT-based Braille keypad integrated with an educational website, designed to assist visually impaired children in learning Tamil Braille letters and numbers. A usability test revealed that this system significantly enhances learning outcomes, enabling children to engage with Braille characters independently and fostering intrinsic motivation for Braille learning. The system's integration of physical and digital learning environments, supported by an open-source toolkit, offers a versatile and customizable educational solution. This toolkit is intended to facilitate the adoption of the Braille Keypad in various academic settings, making it a valuable resource for educators and researchers in visual impairment education.

Keywords: Braille · Learning · Children · Blind · Visual Impairment · Low Vision · Tangible User Interface

1 Introduction

Literacy is the cornerstone of formal education, exerting a profound influence on numerous facets of life, notably education and communication. It forms the bedrock of learning, facilitating access to knowledge, skill acquisition, and active participation in educational endeavors. Proficient literacy enables individuals to comprehend textbooks, take notes, and fulfill assignments, thereby fostering academic excellence. Moreover, literacy fosters independence as individuals adept in reading and writing require less assistance with basic tasks such as completing forms, following instructions, or grasping critical information. This self-reliance significantly enhances overall quality of life. The acquisition of literacy skills marks a pivotal developmental milestone in childhood, laying the groundwork for lifelong learning and personal enrichment. Early literacy proficiency empowers children to build a robust foundation for academic achievement and future pursuits. It's imperative to acknowledge the right to literacy for all individuals, including those with disabilities such as visual impairments. The Braille system, conceived by

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 434–448, 2025.
https://doi.org/10.1007/978-3-031-91008-1_38

Louis Braille, himself blind, in 1824 at the age of 15, stands as a vital tool for enabling visually impaired individuals to access written content, engage in literary activities, and participate in written correspondence. This commitment to inclusivity ensures equitable opportunities for learning and effective communication. Literacy transcends being merely a valuable skill; it embodies a fundamental human right, facilitating educational access, autonomy, and social integration. Ensuring universal access to literacy tools and resources is essential to nurturing literate, fulfilled lives.

Braille, conceived by Louis Braille in 1824, is a tactile writing system meticulously designed to empower blind and visually impaired individuals in reading and writing efficiently. Named after its visionary creator, Braille serves as a conduit for accessing written information, pivotal for education, communication, and independence. While not constituting a language per se, Braille functions as a representation of languages, with each character correlating to specific letters, numbers, punctuation marks, or even whole words or contractions, tailored to individual languages. The Braille cell, a grid of six dots arranged in two columns and three rows, accommodates 63 combinations, encompassing various characters and symbols. This adaptable system transcends linguistic boundaries, catering to diverse languages and scripts, thus facilitating global accessibility to written content for visually impaired individuals. Braille's ubiquity underscores its indispensable role in enabling tactile literacy, empowering individuals worldwide to engage with written discourse effectively. A basic Braille cell is a configuration of six raised or embossed dots. It is an upright rectangular shape made up of two vertical columns, each containing three dot positions. This arrangement creates a 2x3 matrix of dots. The six dots in a Braille cell are numerically identified by the numbers 1 to 6. This numerical identification is used to specify the position of each dot within the cell. Different combinations of raised or embossed dots in a Braille cell represent various elements, including alphabetical letters, numbers, symbols, consonants, vowels, diacritical marks, or abbreviated suffixes. Each unique configuration of dots corresponds to a specific character or symbol. The tactile configuration of dots in a Braille cell gives each symbol a distinctive shape that can be read through touch. The empty dot positions within the cell serve as reference points to help the reader identify the embossed positions forming the letters or symbols. In Braille, the symbols are embossed from right to left within the cell, but reading proceeds from left to right. This reading direction is consistent across different scripts, including Tamil and top-to-bottom scripts. There are barriers between individual Braille cells to separate them from each other. These barriers help the reader distinguish one cell from the next and ensure accurate reading. Overall, Braille is a crucial tool for individuals with visual impairments, allowing them to access written information through touch and providing a means of communication and literacy.

Creating an interactive Tamil Braille learning system featuring a tactile Braille keypad represents a laudable endeavor. This initiative holds the potential to substantially enrich the educational journey for individuals who are visually impaired, offering a more accessible, engaging, and efficient learning experience. Here are several advantages and factors to consider regarding such a system: Traditional Braille learning tools often face accessibility limitations. An interactive digital platform can be tailored to accommodate

diverse learning styles and abilities, including those with additional disabilities. Interactive tools tend to captivate learners more effectively, particularly younger students. The tactile Braille keypad can deliver instant feedback, transforming the learning process into an enjoyable game-like activity, thus fostering motivation. Digital systems enable progress tracking, benefiting both learners and educators. This data facilitates personalized lesson plans and overall performance monitoring. Combining tactile feedback with audio prompts and visual aids offers a multisensory learning environment, proven highly effective for Braille learners. Customizable lessons allow learners to concentrate on specific aspects of Tamil Braille according to their individual requirements and proficiency levels. Unlike traditional materials, which are costly and require frequent replacement, a digital system is cost-effective and sustainable once developed. Digital learning platforms encourage collaboration between educators and parents, enhancing progress monitoring and support mechanisms. It's essential to ensure that the digital tools are accessible to individuals with various disabilities, including motor or hearing impairments. An intuitive interface is crucial for users of different ages and technological backgrounds to access the system effectively. Consideration should be given to the technology's cost and its availability to a broad spectrum of students and educational institutions. Comprehensive training and ongoing support for teachers and students are imperative to maximize the system's benefits. In essence, the development of an interactive Tamil Braille learning system with a tactile Braille keypad holds immense promise in enhancing the accessibility and efficacy of Braille education. Engaging the Braille community, educators, and specialists in its development is crucial to ensuring that it adequately addresses the unique needs of Tamil Braille learners (Fig. 1).

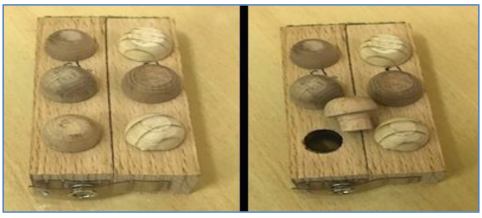


Fig. 1. Traditional Braille System

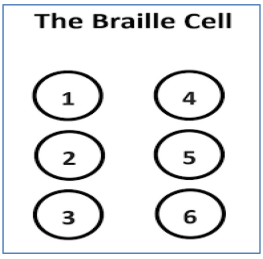


Fig. 2. Basic Braille System

1.1 Objective

The objective of this chapter is to underscore the significance of literacy as a fundamental human right and to explore the crucial role that Braille plays in empowering visually impaired individuals. This chapter aims to highlight the development of an interactive Tamil Braille learning system featuring a tactile Braille keypad, emphasizing its potential to revolutionize the educational experiences of visually impaired learners. By examining the advantages and challenges associated with traditional Braille learning methods and introducing innovative digital solutions, this chapter seeks to advocate for the creation of accessible, engaging, and efficient learning tools that cater to the unique needs of Tamil

Braille learners, ultimately fostering inclusivity and enhancing literacy among visually impaired individuals.

2 Literature Survey

Braille, devised by Louis Braille in 1824, constitutes a tactile script featuring characters composed of six dots arranged in a rectangular pattern of three rows and two columns. These raised dots allow identification through fingertip exploration, with some characters serving as pairs where the first character offers context for interpreting the second, as seen in Fig. 2. While the representation of basic alphabet characters remains consistent across languages, variations emerge in special characters, abbreviations, and modifications, including systems employing eight dots (as referenced in [23]). In Braille, word perception extends beyond individual letters, forming a tactile "Gestalt" [2]. Thus, learners must grasp not only individual letters but also larger informational units, such as words, while simultaneously mastering letter-by-letter spelling. The journey of learning Braille for a child involves reading, spelling, and writing practice, alongside refining haptic perception and deepening comprehension of written language [1]. Tactile materials play a crucial role in facilitating this process, ranging from books with tactile features [3] to commercially available solutions offering standard Braille cells [4], swing cells [5], and even homemade contrivances [13, 26].

Tangible User Interfaces (TUIs) serve as a bridge between tactile elements, physical object manipulation, and real-world affordances, leveraging technological possibilities [16, 17]. TUIs promote natural interaction [4] and can simplify abstract concepts, thereby reducing cognitive strain [24, 42], holding considerable potential for enriching the learning journey [4, 27]. Numerous research studies have explored TUIs' utility in aiding visually impaired children's learning. These studies often involve placing physical objects representing abstract concepts, such as geometric shapes, on a dedicated surface [2, 19, 25], with added Braille characters facilitating Braille learning. For instance, Najjar et al. introduced mathematical symbols and numbers as standard Braille characters on blocks, aiding math problem-solving with audio guidance [29]. Pires et al. developed a system integrating color- and shape-coded elements with Braille letters, enhancing accessibility for both visually impaired and sighted users [30, 31]. Utilizing residual vision among visually impaired users is preferred, as evidenced by systems incorporating visual information [22]. Typically, blocks featuring front or upward-facing standard Braille characters are employed for arranging characters together [3, 10, 18], or for collaborative activities involving sighted teachers or parents [11]. The translation of physical information to the digital realm often utilizes methods like webcams [10, 11] or near-field communication [3, 18]. Other suggestions include employing infrared-emitting blocks with standard Braille characters [8] or alternative formats such as a cotton strip with pouches [12].

Digital resources for learning Braille offer diverse game modes, with some providing audio feedback upon object placement, offering details about shapes or their relationships [2, 19]. Others, like Najjar et al., guide children through stories, enhancing math skills [29]. While most focus on placing Braille characters representing text, various game modes involve tasks like spelling words or arranging letters alphabetically [8, 10, 18].

Our portable prototype distinguishes itself from existing works with its ease of setup, use of standard-size Braille characters, highly responsive interaction design, and the capacity to foster self-directed exploratory Braille reading and spelling for children.

3 Design Process

Our project began with inspiration from previous research endeavors. Through six rounds of collaborative refinement with stakeholders, we improved both our concept and prototype design. These iterations are illustrated in Fig. 3, showcasing images of each prototype or conceptual model discussed throughout the process. In our initial iteration, we developed two conceptual prototypes, drawing from existing works. Our main goal was to provide automated audio feedback to users. The first concept, named BrailleEggs, resembled an enlarged Braille character. It allowed users to select individual dots by placing egg-shaped objects, similar to commercially available or homemade devices. The second concept, akin to a SwingCell, was crafted using clay and marbles.

In the subsequent iteration, we discussed the BrailleEggs concept and the clay prototype with two educators: one sighted (E1) and one visually impaired (E2), who specialized in teaching children with visual impairments, alongside a blind digital accessibility consultant and braille expert (E3). During these early stages, we opted not to involve children currently learning Braille, instead relying on the expert insights of educational professionals. In response to their feedback, particularly the suggestion to prioritize standard-sized Braille characters and spelling words over individual characters, we developed a comprehensive concept for a Braille keypad.

3.1 Hardware Components Used

3.1.1 ESP32 Microcontroller

The ESP32, crafted by Espressif Systems, epitomizes a range of microcontrollers renowned for their adaptability. Widely employed across diverse domains, particularly within the realm of Internet of Things (IoT), the ESP32 embodies versatility. The acronym itself, ESP, signifies “Espressif,” denoting the company behind its inception and production. The appended “32” signifies its 32-bit architecture, facilitating enhanced data processing and instruction execution compared to older 8-bit or 16-bit counterparts. With integrated Wi-Fi and Bluetooth functionalities, ESP32 chips are tailor-made for IoT applications necessitating seamless wireless connectivity. ESP32 chips often come equipped with dual-core processors, enhancing their ability to handle multitasking and real-time processing efficiently. Engineered for energy efficiency, ESP32 microcontrollers are ideal for battery-powered devices. With a diverse array of peripherals such as GPIO pins, UART, SPI, I2C, and more, they offer adaptability across various projects. Enhanced security features like hardware encryption and secure boot further bolster the safety of IoT devices leveraging ESP32 technology. Supported by a vibrant ecosystem of open-source software and development tools, ESP32 enjoys widespread accessibility among developers. These microcontrollers find frequent application in IoT devices, home automation, robotics, sensor nodes, and beyond, owing to their connectivity options, processing prowess, and minimal power consumption.

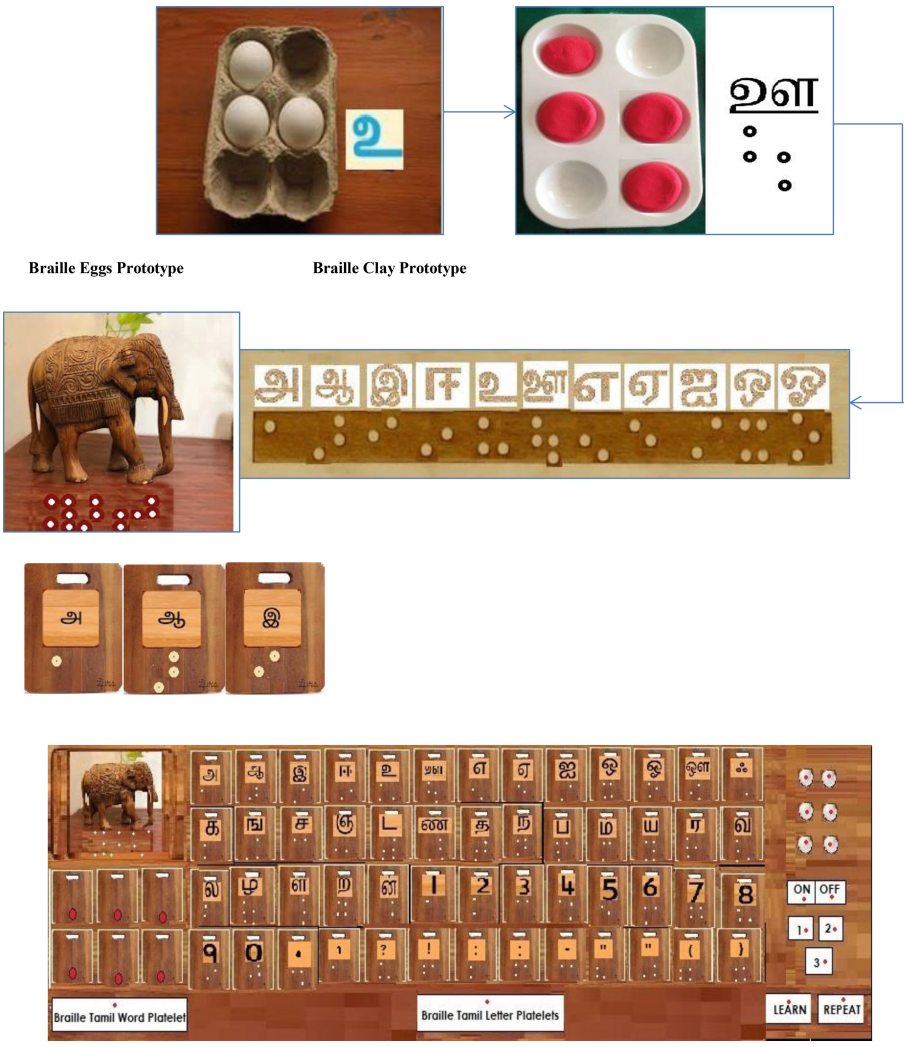


Fig. 3. Braille Tamil Keypad

3.1.2 RFID Tag

A wooden card housing an RFID tag represents a unique application of RFID technology, merging traditional materials with modern functionality. This fusion offers both practical utility and aesthetic appeal. Here are some essential details about RFID tags within wooden cards:

RFID Functionality: The integration of an RFID chip and antenna enables the wooden card to wirelessly communicate with RFID readers. The chip serves as a data storage medium, capable of both reading and writing data when in close proximity to an RFID reader (Fig. 4).

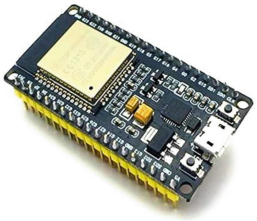


Fig. 4. ESP32Microcontroller



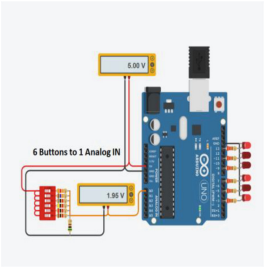


Fig. 5. RFID Tag

4 Methodology

We designed three unique types of wooden cards: Tamil letter cards, word cards, and 3D Figurine game mode cards. The letter cards are sized at 25 × 40 × 5 mm (height × width × thickness) and feature a single Tamil letter along with corresponding Braille characters. Additionally, the letters are printed in raised text above the Braille characters for tactile identification. Word cards share the same dimensions and display either a 2D relief image or a 3D figurine representing an object. Our aim was to utilize the figurines as motivational tools. Beneath each object, we include the Braille word associated with it, enabling children to comprehend the entire word tactually while also feeling each letter individually. These words are selected from grade 1, 2, and 3 textbooks.

The game mode cards, in contrast, are larger at 60 × 60 × 6 mm and are inscribed in Braille with the name of the game mode they activate upon placement. Each of our cards includes a recessed area on its backside to accommodate an RFID tag. In total, we manufactured 56 letter cards, two game mode cards, and 12 word cards featuring 3D figurines. Managing the Braille keypad is an ESP32 microcontroller with WIFI and Bluetooth capabilities. This configuration integrates five RFID readers, six light sensors, and a speaker. The RFID readers detect the tag on the placed cards, while the light sensors determine the precise card placement. These sensors connect to the ESP via a multiplexer, and the speaker is linked through an mp3 module. To store audio files, we've added a memory card, and we've included eight push buttons for replaying audio feedback when a card is placed. For a visual representation of the electronic components within the Braille keypad and an overview of the schematic is referred in Fig. 5. The Braille keypad offers two modes of interaction. A child can either insert or remove a card into one of the six slots or press any of the eight buttons below each slot. In both cases, the Braille keypad provides audio feedback tailored to its current state and the specific area or button selected. We've designed three unique game modes: Word Copy, Word Riddle, and Word Scramble, illustrated in Fig. 6. When the Braille keypad is powered on, it delivers a brief introduction, which can be replayed by pressing the left-most button. Initially, all other buttons indicate that the corresponding slot is empty.

In the "Word Copy" game mode, players start by placing a word card representing an object into the first slot of the Braille keypad. Then, the device guides them to spell out the word by adding individual letter cards one by one to the right. Pressing the leftmost button repeats these instructions, while pressing a button below any other

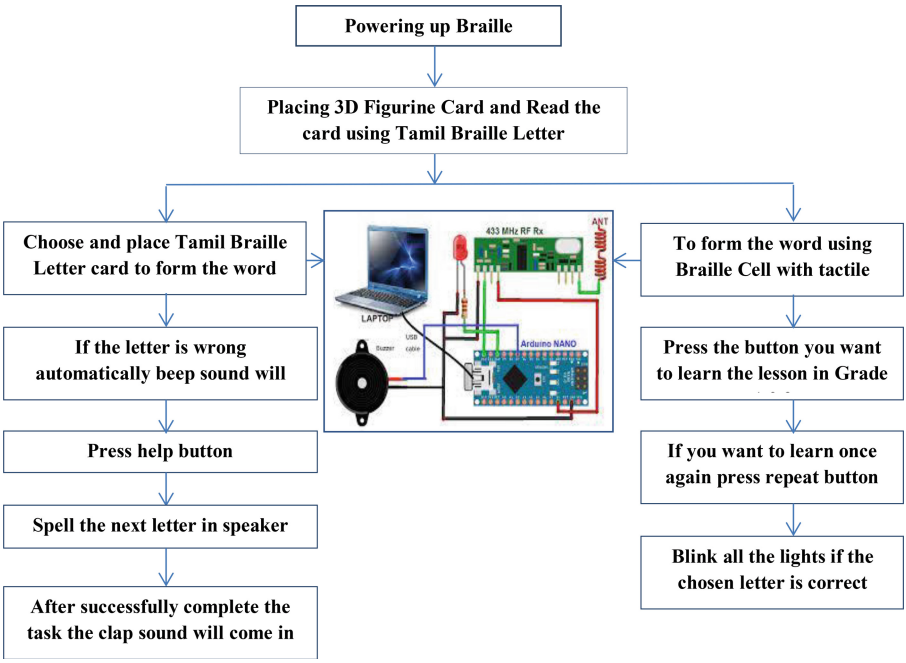


Fig. 6. Flow Diagram

slot confirms if it's empty or replays feedback for inserting a letter card. Each letter's correctness is determined and indicated. When the word is successfully spelled and completed correctly, the Braille keypad audibly recites the word and plays a finishing sound. In the "Word Scramble" mode, a word is chosen randomly from a list when the game mode card is inserted. Players are prompted to shuffle these letters randomly in the box. The leftmost button can be pressed to repeat instructions as needed. Other buttons indicate which letter should occupy each recess if it's empty. If a letter card has already been placed, the Braille keypad indicates its correctness. Once all letters are correctly placed, players are instructed to arrange them in the correct order. The left button repeats these new instructions, while the others read out the letter and provide feedback on correctness. If all letters are correctly arranged, the word is read aloud, and a finishing sound is played.

In the Word Riddle game mode, akin to Word Scramble, the Braille keypad randomly selects a word, obscuring its letters for players to guess. Similar to Word Scramble, the leftmost button repeats instructions, and others indicate whether a recess above is vacant or provide feedback on letter card placement. Upon placing a letter card, the Braille keypad offers one of three messages: (1) indicating if the letter is not in the word, (2) informing of the presence of a certain number of the placed letter but in the wrong position, or (3) confirming the presence of a certain number of the placed letter in the correct position. Additionally, when inputting a lowercase letter card for an uppercase letter, or vice versa, the keypad specifies the case. Successfully guessing and ordering all letters prompts the device to audibly reveal the word and play a finishing sound. This

Braille keypad input device integrates the conventional Braille cell for system navigation and interaction. It features eight buttons: six representing Braille dots, along with Enter and Tap buttons for navigation. Serving as the primary input mechanism, it is divided into two sections. The first part comprises six numbered buttons arranged in two columns of three, representing Braille dots. The second part includes buttons for executing Enter and Tap commands. Designed for accessibility and one-handed ease of use, Fig. 5 illustrates its layout. Utilizing the Mini Arduino Leonardo for managing keyboard commands, the Arduino controller seamlessly integrates into the keypad, comprising various components. MiniArduino Leonardo

1. Two buttons
2. Six toggle-switches
3. USB connector
4. Other connectors

The Arduino Leonardo is characterized as an "easy-to-use, open-source hardware and software electronic platform". For this project, the Arduino Leonardo (depicted in Fig. 6) was selected due to its integrated USB communication capability, enabling it to manage keyboard commands. A breadboard, commonly employed for circuit design and testing (as demonstrated in Fig. 7), will be utilized to link the GND pin from the Arduino to its designated row. Jumper cables will establish connections between the Arduino, sensors, and relay. Additionally, a latching push-button switch will function as an On/Off switch, featuring a flashing light upon activation to enhance accessibility for visually impaired users. Furthermore, conventional On/Off buttons will also be incorporated into the setup.

The open-source toolkit consists of five sub-modules:

a) About the Braille Cell: This module serves as an introductory lesson on the Braille cell, providing an audible explanation of its structure and coding.
b) How to Use the Braille Keypad: Before engaging in Braille learning, users are introduced to the system's primary interface, a specially designed keypad simulating a Braille cell. The system explains the keypad's shape, structure, and usage audibly, including details about the different buttons and their functions.
c) Tamil Braille Learning: This module forms the core of the system and offers essential functions. The primary user interface includes three main functions:

Lesson: Providing an explanatory lesson on Tamil Braille characters (letters or numbers).

Practice: Allowing learners to practice writing characters using the Braille keypad without time constraints or scoring.

Re-learn: Enabling learners to replay a lesson.

To initiate, learners select a letter/number lesson from a list or continue from where they left off. The lesson begins by displaying a word starting with the letter to be learned, along with its pronunciation. The corresponding Braille cell representation is presented and explained through text, images, and audio materials.

Similarly, for number lessons, three flowers, for example, will be displayed alongside the number "3," which is then represented using the Braille cell and explained. After completing the lesson, the practice mode becomes available to ensure learners have

grasped the lesson's content, or they can choose to repeat the lesson. During practice, the system displays and pronounces the letter/number, and the learner responds using the Braille keypad. If the answer is correct, the system offers the option to proceed to the next lesson or return to the previous page. If the answer is incorrect, the learner can retry or select the "re-learn" option to restart the lesson from the beginning. An illustration of this scenario is presented in Fig. 6.

5 Results

All participants successfully completed their assigned tasks, except for participant P1, who encountered difficulties with Tasks 2 and 4. Upon closer observation, it became apparent that this participant lacked familiarity with basic technology concepts, such as the definition of a laptop or a website, and displayed no knowledge of Tamil letters or numbers. It is advisable to offer additional preparation sessions to familiarize this participant with the necessary technology and concepts before proceeding with further testing.

To address the complexity of interactive features, we created a Tamil Braille keypad with a user-friendly interface and provided clear, simplified instructions for RFID readers, light sensors, and audio feedback. We conducted iterative usability testing with young children and individuals with limited technological experience to ensure the system was intuitive and accessible. The feedback from these testing sessions was crucial, guiding iterative adjustments to streamline the interactive features. These enhancements were aimed at making the system easier to use, thereby improving the learning experience and ensuring that the technology supported rather than obstructed user engagement. We have revised the system's interface to significantly enhance user experience by simplifying navigation and reducing the need for users to return to previous task pages. By streamlining task completion processes, we aimed to minimize cognitive load and make interactions more intuitive. These improvements were guided by iterative user testing, which provided valuable insights and feedback. As a result, the updated interface is designed to be more efficient and user-friendly, facilitating smoother interactions and reducing the time required to complete tasks.

We evaluated the efficiency of the open-source toolkit by measuring task completion times (refer to Table 2). Notably, participants showed varying completion times for these tasks. Figure 12 depicts the time spent on each task in seconds for each participant, highlighting participant P2's fastest completion times across all tasks, attributed to prior experience with technology and educational websites. Additionally, we observed that Task 4 required the longest completion time. We attribute this delay to its sequential placement in relation to other tasks, requiring multiple returns to previous task pages for completion.

Another aspect we assessed was the system's effectiveness, measured by the number of user errors and the need for assistance in task completion. Only participant P1 committed errors in two tasks (Task 2 and 4), both resulting from mistakenly entering URL link settings. Task 2, on average, required a higher level of assistance (56%) compared to other tasks. Regarding user feedback, all participants found the system motivating and enjoyable for learning via the website. Furthermore, they unanimously agreed that the

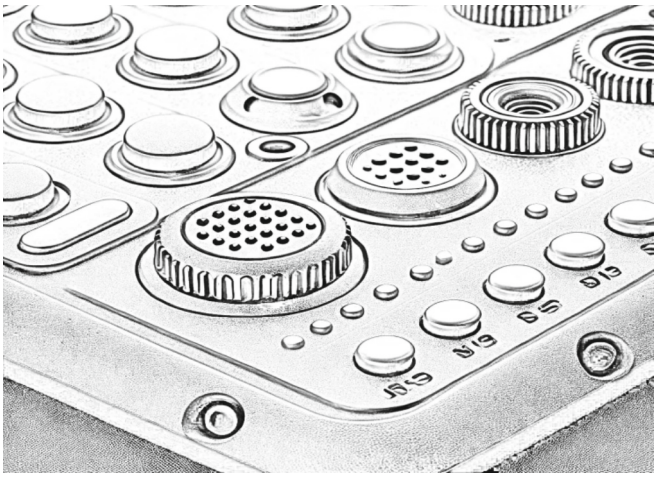


Fig. 7. Durability of a keypad

Table 1. Different Aspects of participants

Aspect	Details
Participant Group	Visually impaired children with varied levels of technological literacy and Braille knowledge
Outreach Strategy	Conducted outreach to diverse schools and organizations serving visually impaired children
Preliminary Training Provided	Basic technology training
Additional Training	Braille knowledge training
Goal	To ensure findings are representative of the broader population and include diverse levels of technology and Braille proficiency

Braille keypad was easy to use. Two participants noted that the website was user-friendly but left them feeling somewhat fatigued, possibly due to the novelty of the experience and the desire for successful completion. Additionally, we solicited suggestions and recommendations from the children to enhance the system. The majority of respondents shared a common suggestion: disabling the URL to make it unreadable by the screen reader. In summary, our findings and recommendations are based on participant behaviors, verbal feedback, comments, and suggestions obtained during and after system usage. These recommendations vary in importance, depending on the frequency of user feedback, and are detailed in Table 1 below (Fig. 8).

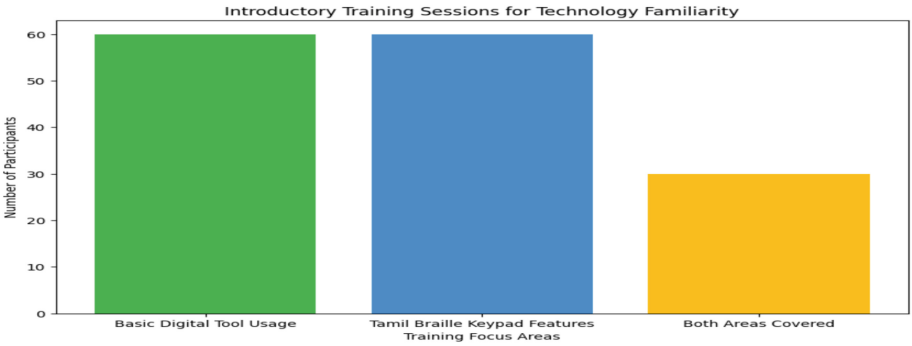


Fig. 8. Training Sessions

Table 2. Measures with Efficiency

	Metrics	Measurement
Quantitative measures	Efficiency	Task Completion Time
	Effectiveness	Number of user errors Number of assistances required to complete each task
Qualitative measures	Satisfaction	Participant's opinion and their satisfaction of the system

6 Conclusion

The proposed system seeks to enrich the Braille learning experience, focusing specifically on Tamil Braille, encompassing both letters and numbers. This innovative system introduces an interactive tactile Braille keypad, not only catering to the blind and visually impaired but also appealing to sighted individuals interested in learning Braille, especially within families with visually impaired children. Through a comprehensive usability test, significant enhancements in the learning process were unveiled. The interactive tactile Braille keypad garnered high acceptance among blind children who partook in the test. We envision this endeavor to make a meaningful contribution to our community, particularly benefiting those with visual impairments.

Our approach to designing this innovative tangible learning device for blind and visually impaired children emphasizes inclusivity and human-centered principles. Acknowledging the fundamental role of reading and spelling in academic achievement, our primary goal is to inspire children to actively engage with Braille. Lowering the initial barriers to learning is crucial for sustaining motivation among many children, and our research suggests that a tangible device like the Braille keypad can effectively accomplish this, fostering children's interest in Braille reading and spelling over an extended period.

References

1. Lang, M., Hofer, U., Beyer, F.: Didaktik des Unterrichtsmitblinden und hochgradigsehbehindertenSchülerinnen und Schülern. Kohlhammer, Stuttgart (2010). ISBN: 978-3-170-20151-4
2. Simón, C., Huertas, J.A.: How blind readers perceive and gather information written in braille. J. Vis. Impairment Blindness **92**(5), 322–330 (1998). https://doi.org/10.1177/0145482X9809200510
3. Star, F., Westing, J., Oliver, C.: Animals: Knowledge you can touch. DK Children (2016). ISBN: 978-1-4654-3611-5
4. APH. Pop-A-Cell (2022). https://www.aph.org/product/pop-a-cell-4-pack/. Accessed 15 Nov 2022
5. APH. Swing Cell Compact (2022). https://www.aph.org/product/swing-cellcompact/. Accessed 15 Nov 2022
6. LEGO Group. Swing Cell | LEGO Braille Bricks (2020). https://legobraillebricks.com/activities/constellation/swing-cell. Accessed 15 Nov 2022
7. Baqai, A., Jan, M., Maher, R.R.: Optical braille blocks for visually impaired elementary education. Mehran Univ. Res. J. Eng. Technol. **40**(1), 205–214 (2021). https://doi.org/10.22581/MUET1982.2101.18
8. Dixon, J.M.: Braille: the challenge for the future. J. Vis. Impairment Blindness **105**(12), 742–744 (2019). 10.1177/ 0145482X1110501103
9. Forcelini, P.G., García, L.S., Schultz, E.P.B.: Braille technology beyond the financial barriers: a braille literacy platform to effectively combat braille literacy crisis. In: Proceedings of the 8th International Conference on Software Development and Technologies for Enhancing Accessibility and Fighting Info-Exclusion (Thessaloniki, Greece) (DSAI 2018), pp. 41–46. Association for Computing Machinery, New York (2018). https://doi.org/10.1145/3218585.3218590
10. Gadiraju, V., Muehlbradt, A., Kane, S.K.: BrailleBlocks: computational braille toys for collaborative learning. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems (Honolulu, HI, USA) (CHI 2020), pp. 1–12. Association for Computing Machinery, New York (2020). https://doi.org/10.1145/3313831.3376295
11. Sánchez García, L., Hilton Sayeg de Siqueira, J., Bueno, J., GaleraForcelini, P.: A tangible interaction platform as concrete support for blind children literacy in Braille. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9739, pp. 135–146 (2016). https://doi.org/10.1007/978-3-319-40238-3_14
12. LEGO Group. 2020. LEGO Braille Bricks. https://www.legobraillebricks.com/. Accessed 2 Sept 2022
13. Guerreiro, J., Gonçalves, D., Marques, D., Guerreiro, T., Nicolau, H., Montague, K.: The today and tomorrow of braille learning. In: Proceedings of the 15th International ACM SIGACCESS Conference on Computers and Accessibility (Bellevue, Washington) (ASSETS 2013), Article 71, 2 p. Association for Computing Machinery, New York (2013). https://doi.org/10.1145/2513383.2513415
14. Jernigan Institute. The Braille Literacy Crisis in America Facing the Truth, Reversing the Trend, Empowering the Blind (2009). https://nfb.org/images/nfb/publications/bm/bm09/bm0905/bm090504.htm
15. Ishii, H.: The tangible user interface and its evolution. Commun. ACM **51**(6), 32–36 (2008). https://doi.org/10.1145/1349026.1349034
16. Ishii, H., Ullmer, B.: Tangible bits: towards seamless interfaces between people, bits and atoms. In: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems (Atlanta, Georgia, USA) (CHI 1997), pp. 234–241. Association for Computing Machinery, New York (1997). https://doi.org/10.1145/258549.258715

17. Jafri, R.: Electronic braille blocks: a tangible interface-based application for teaching braille letter recognition to very young blind children. In: Miesenberger, K., Fels, D., Archambault, D., Peňáz, P., Zagler, W. (eds.) ICCHP 2014. LNCS, vol. 8548, pp. 551–558. Springer, Cham (2014). https://doi.org/10.1007/978-3-319-08599-9_81
18. Jafri, R., Aljuhani, A.M., Ali, S.A.: A tangible user interface-based application utilizing 3D-printed manipulatives for teaching tactual shape perception and spatial awareness sub-concepts to visually impaired children. Int. J. Child-Comput. Interact. **11**, 3–11 (2017). https://doi.org/10.1016/J.IJCCI.2016.12.001
19. Lang, F., Schmidt, A., Machulla, T.: Mixed reality as assistive technology: guidelines based on an assessment of residual functional vision in persons with low vision. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). LNCS, vol. 13342, pp. 484–493 (2022). https://doi.org/10.1007/978-3-031-08645-8_57
20. Li, Y., et al.: A meta-analysis of tangible learning studies from the TEI conference. In: Sixteenth International Conference on Tangible, Embedded, and Embodied Interaction (Daejeon, Republic of Korea) (TEI 2022), Article 7, 17 p. Association for Computing Machinery, New York (2022). https://doi.org/10.1145/3490149.3501313
21. Lozano, M.D., Penichet, V.M., Leporini, B., Fernando, A.: Tangible user interfaces to ease the learning process of visually-impaired children. In: Proceedings of the 32nd International BCS Human Computer Interaction Conference (Belfast, United Kingdom) (HCI 2018), Article 87, 5 p. BCS Learning & Development Ltd., Swindon, GBR (2018). https://doi.org/10.14236/ewic/HCI2018.87
22. Markoski, K.: DIY Braille Cell (2020). https://www.youtube.com/watch?v=I7bBkj3dGVY. Accessed 15 Nov 2022
23. Markova, M.S., Wilson, S., Stumpf, S.: Tangible user interfaces for learning. Int. J. Technol. Enhanced Learn. **4**(3–4), 139–155 (2012). https://doi.org/10.1504/IJTEL.2012.051578
24. Sandoval-Bringas, J.A., Carreño-León, M.A., Encinas, I.D., Carrillo, A.L., Cota, I.E., Castro, R.C.: Using tangible interfaces for teaching Braille. In: 2020 3rd International Conference of Inclusive Technology and Education (CONTIE), pp. 128–132 (2020). https://doi.org/10.1109/CONTIE51334.2020.00032
25. Najjar, A.B., Alhussayen, A., Jafri, R.: Usability engineering of a tangible user interface application for visually impaired children. Hum.-Centric Comput. Inf. Sci. **11** (2021). https://doi.org/10.22967/HCIS.2021.11.014
26. Pires, A.C., et al.: Learning maths with a tangible user interface: lessons learned through participatory design with children with visual impairments and their educators. Int. J. Child-Comput. Interact. **32**, 100382 (2022). https://doi.org/10.1016/J.IJCCI. 2021.100382
27. Pires, A.C., et al.: A tangible math game for visually impaired children. In: Proceedings of the 21st International ACM SIGACCESS Conference on Computers and Accessibility (Pittsburgh, PA, USA) (ASSETS 2019), pp. 670–672. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3308561.3354596
28. Xu, D., Read, J.C., Mazzone, E., MacFarlane, S., Brown, M.: Evaluation of tangible user interfaces (TUIs) for and with children – methods and challenges. In: Jacko, J.A. (ed.) Human-Computer Interaction. Interaction Platforms and Techniques, pp. 1008–1017. Springer, Heidelberg (2007). https://doi.org/10.1007/978-3-540-73107-8_11
29. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.) Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3

30. Peng, S.-L., Lin, C.-K., Pal, S. (eds.) Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
31. Peng, S.-L., Hao, R.-X., Pal, S. (eds.) Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4

Modeling Healthy Data with New Alpha Power Inverse Weibull Distribution

Al-Zamely Mohammed oda(✉) and Kareema Abed Al-Kadim

Department of Mathematics, College of Education for Pure Sciences, Babylon University, Hilla, Iraq
mom97rm@gmail.com

Abstract. A new distribution creation method is presented in this article. The final distributions may be shaped with great flexibility thanks to alpha power transformation methods. The alpha power inverse Weibull Quantile exponential is introduced using a unique approach. The distribution's density may show imbalanced, almost equal, and opposite geometries. Asymmetric variants of the related failure rate function include decreasing, increasing, Right-skewed, almost symmetrical, and L-shaped forms. These different shapes make the function more manageable for various modeling purposes. The mathematical properties of the recommended distribution are identified. The maximum likelihood approach estimates the proposed distribution's unknown parameters. In addition, many quantitative analyses were conducted to assess the estimate's accuracy. The new distribution's flexibility and usefulness are evaluated using real-world datasets. Proving its extraordinary flexibility in real-world data processing, the suggested alpha power inverse Weibull Quantile exponential distribution outperforms other popular distributions.

Keywords: alpha power transformation · moment · order statistics · quantile

1 Introduction

Many disciplines, including engineering, finance, and biology, have used statistical distributions to describe and predict current trends, medicine. However, Numerous scholars have attempted to enhance the conventional distributions to make them more flexible for modeling data from other fields of study. The subject includes several changed distributions, such as the Inverse Weibull exponential distribution [1]. An often-sought goal in improving the accuracy of distribution fitting is to develop novel generators for sets of distributions. This approach is used to generate extensions of the current standard models. The researchers in [2] have devised a thorough procedure known as Alpha power transformation. This method has been exclusively devised, highlighting its innovative and sophisticated character. Adding skewness to a distribution could improve its performance.

$$F_{APT}(u) = \begin{cases} \frac{\alpha^{W(u)}-1}{\alpha-1} & , if\, \alpha > 0, \alpha \neq 1 \\ W(u) & , if\, \alpha = 1 \end{cases} \quad (1)$$

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 449–457, 2025.
https://doi.org/10.1007/978-3-031-91008-1_39

$$f_{APT}(u) = \begin{cases} \frac{log\alpha}{\alpha-1} f(u)\alpha^{W(u)} & , if\, \alpha > 0, \alpha \neq 1 \\ f(u) & , if\, \alpha = 1 \end{cases} \tag{2}$$

Here, the CDF and PDF of any continuous distribution are denoted by $F(x)$ and $f(x)$, respectively.

We may use using a and b as parameters for size and form for RV that follow the inverse Weibull distribution.

$$W(x) = e^{-a(x)^{-b}} \quad , x \geq 0 \tag{3}$$

The Weibull–family includes the Inverse Weibull exponential distribution (IWED), where G is an exponential RV with CDF in [3]. $G(x) = 1 - e^{-\lambda x}$, $x \geq 0, \lambda > 0$.

Let $u \sim U(0, 1)$

$$u = G(X)$$

$$u = 1 - e^{-\lambda x} \Rightarrow -\lambda x = ln(1-u)$$

$$x = \frac{-\ln(1-u)}{\lambda} \tag{4}$$

Substituting it into Eq. (1), We will get to

$$W(u) = e^{-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}} \tag{5}$$

This study introduces the alpha power Inverse Weibull-Quantile exponential distribution (APWIQED). This foundation is built around a novel concept approach to distribution development that allows for better flexibility in portraying accurate data in many domains. Integral to it are several APT methods.

2 The Alpha Power Inverse Weibull Quantile Exponential Distribution

An RV with a four-parameter APIWQED may be described in terms of its CDF in the following way.

$$F(u) = \begin{cases} \frac{\alpha^{e^{-a\left(\frac{-ln(1-u}{\lambda}\right)^{-b}}} - 1}{\alpha - 1} & , \alpha > 0, \alpha \neq 1 \\ e^{-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}} & , \alpha = 1 \end{cases} \tag{6}$$

where $\alpha, \lambda, a, b > 0\, and\, u \geq 0$

The corresponding PDF is given as

$$f(u)=\begin{cases}\frac{log\alpha}{\alpha-1}\frac{ab\left(\frac{-ln(1-u}{\lambda}\right)^{-b-1}e^{-a\left(\frac{-ln(1-u)}{\lambda}\right)^{-b}}}{\lambda(1-u)}\alpha^{e^{-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}} & ,if\ \alpha>0,\alpha\neq1\\ \frac{ab\left(\frac{-\ln(1-u}{\lambda}\right)^{-b-1}e^{-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}}}{\lambda(1-u)} & ,if\ \alpha=1\end{cases} \tag{7}$$

The survival function, $S(x)$

$$S(u)=\begin{cases}\frac{\alpha}{\alpha-1}\left(1-\alpha^{e^{-\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}}-1}\right) & ,if\ \alpha>0,\alpha\neq1\\ 1-e^{-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}} & ,if\ \alpha=1\end{cases} \tag{8}$$

The APIWQED's hazard rate function, h(x), is defined as

$$h(u)=\begin{cases}log\,\alpha\left(ab\frac{\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b-1}}{\lambda(1-u)}e^{-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}\right)\frac{\alpha^{-e-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}-1}}{1-\alpha^{-e-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}-1}} & ,if\ \alpha>0,\alpha\neq1\\ ab\frac{\left(\frac{-\ln(1-u)}{\lambda}\right)^{a-1}}{\lambda(1-u)}\left(\frac{e^{-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}}}{1-e^{-a\left(\frac{-\ln(1-u)}{\lambda}\right)^{-b}}}\right) & ,if\ \alpha=1\end{cases} \tag{9}$$

2.1 Special Cases of the APIWQED

1) At, the APIWQED becomes the IWQED. $\alpha=1$.
2) At, the APIWQED becomes to the IWQD. $\alpha=\lambda=1$.
3) The APIWQED becomes to the QED when $\alpha=b=a=1$

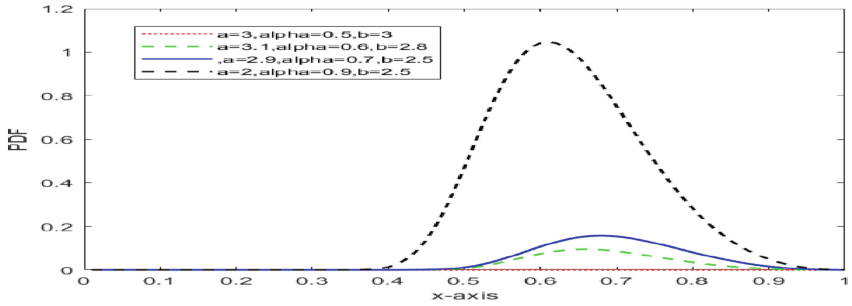


Fig. 1. The APIWQED PDF plots for certain values of α, λ, b, a.

Figure 1 illustrates several alternative APIWQED density configurations, it includes symmetric, almost symmetric, inverted J-shaped morphologies and is skewed left and right. Figure 2 demonstrates how various uneven shapes are included in the APIWQED hazard rate. These results demonstrate how highly adaptive the APIWQED is.

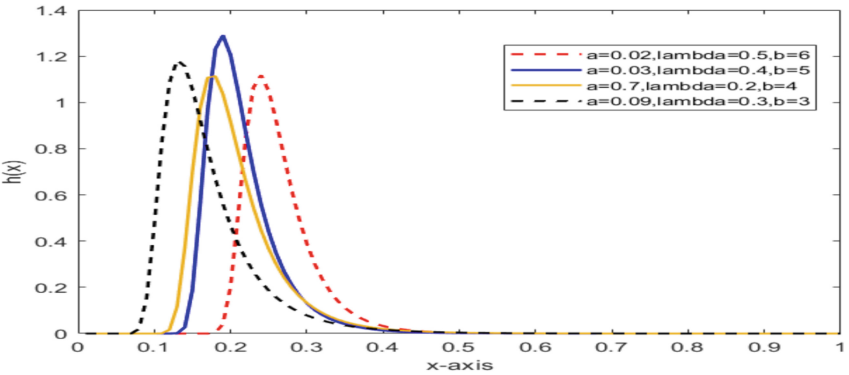


Fig. 2. Shows APIWQED PDF plots for a few chosen values of α, λ, b, a.

2.2 Expansion for the *PDF*

Using the series representation, the APIWQED PDF has a straightforward extension.

$$\alpha^{-z} = \sum_{j=0}^{\infty} \frac{(-log\alpha)^j}{j!}(z)^j \tag{10}$$

Therefore, expanding $\alpha^{-e^{-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}}$ in (7) using (10), we have

$$f(u) = \frac{ab}{\alpha - 1} \frac{\left(\frac{-ln(1-u}{\lambda}\right)^{-b-1}}{\lambda(1-u)} \sum_{J=0}^{\infty} \frac{(-log)^{j+1}}{j!} \left(e^{-a(j+1)\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}\right) \tag{11}$$

3 Properties of the APIWQED This Part Presents the Following Essential Statistical Characteristics of the APIWQED

3.1 Quantile Function

The *pth* quantile function $(0 < p < 1)$ of the APIWQED may be acquired.

$$u_p = 1 - e^{-\lambda\left(\frac{-ln\left(1-\frac{ln((\alpha-1)p+1)}{ln\alpha}\right)}{a}\right)^{\frac{-1}{b}}} \tag{12}$$

Therefore, the median of the APIWQED may be determined by setting $p = 0.5$.

$$u_{0.5} = 1 - e^{-\lambda\left(\frac{-ln\left(1-\frac{ln((\alpha-1)0.5+1)}{ln\alpha}\right)}{a}\right)^{\frac{-1}{b}}} \tag{13}$$

3.2 Moments if $X \sim$ APIWQED (α, λ, u, a), Subsequently, the rth Instant of U May Be Acquired

$$\mu_r = E\left(U^r\right) = \int_0^\infty u^r f(u)du = \sum_{j=0}^{\infty} \frac{(-log)^{j+1}}{j!} \frac{ab}{\alpha - 1} \int_0^\infty u^r \frac{\left(\frac{-ln(1-u}{\lambda}\right)^{-b-1}}{\lambda(1-u)} \left(e^{-a(j+1)\left(\frac{-ln(1-u}{\lambda}\right)^{-b}}\right) du$$

Substituting $y = \frac{-\ln(1-u)}{\lambda} \Rightarrow u = 1 - e^{-\lambda y}$, $du = \lambda e^{-\lambda y} dy$, It is possible to express the rth instant of the APIWQED as

$$\mu_r = E\left(U^r\right) = \sum_{j=0}^{\infty} \sum_{i=0}^{r} \sum_{k=0}^{\infty} \frac{(-log)^{j+1} \binom{r}{i} (-1)^{i+k} (j+1)^k (a)^k ab}{j!(\alpha - 1)k!} \frac{\Gamma(-b(k+1) - 1)}{(\lambda i)^{-b(k+1)-1}} \tag{14}$$

Hence, the average APIWQED may be stated as

$$\mu = E(U) = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \frac{(-log)^{j+1} (-1)^k (j+1)^k (a)^k ab}{j!(\alpha - 1)k!} \frac{\Gamma(-b(k+1) - 1)}{(\lambda i)^{-b(k+1)-1}} \tag{15}$$

Furthermore, the APIWQED variance may be calculated using Eqs. (18) and (19) as follows:

$$\begin{aligned} \sigma^2 &= E\left(U^2\right) - \mu^2 \\ &= \sum_{j=0}^{\infty} \sum_{i=0}^{2} \sum_{k=0}^{\infty} \frac{2(-log\alpha)^{j+1} (-1)^{i+k} (j+1)^k (a)^k ab}{j!(\alpha - 1)k!i!(2-i)!} \frac{\Gamma(-b(k+1) - 1)}{(\lambda i)^{-b(k+1)-1}} - \mu^2 \end{aligned} \tag{16}$$

3.3 Characteristic Functions and Moment-Generating Functions an Easy Way to Express the (MGF) of APIWQED is as

$$M_u(t) = E\left(e^{tu}\right) = \int_0^\infty e^{tu} f(u)du$$

Using the same steps for finding the moment function and using the binomial series, then the moment generating function and characteristic function of APIWQED

$$M_u(t) = \sum_{j=0}^{\infty} \sum_{r=0}^{\infty} \sum_{i=0}^{r} \sum_{k=0}^{\infty} \frac{(-log)^{j+1} \binom{r}{i} (-1)^{i+k} t^r (j+1)^k (a)^k ab}{j!(\alpha - 1)k!r!} \frac{\Gamma(-b(k+1) - 1)}{(\lambda i)^{-b(k+1)-1}} \tag{17}$$

Similarly,

$$\phi_u(t) = \sum_{j=0}^{\infty} \sum_{r=0}^{\infty} \sum_{i=0}^{r} \sum_{k=0}^{\infty} \frac{(-log)^{j+1} \binom{r}{i} (-1)^{i+k} (ti)^r (j+1)^k (a)^k ab}{j!(\alpha - 1)k!r!} \frac{\Gamma(-b(k+1) - 1)}{(\lambda i)^{-b(k+1)-1}} \tag{18}$$

3.4 Order Statistics

Given that a random sample from the APIWQED, where $U_1, U_2, ..., U_n$, This ith order statistic is denoted by $u_{i:n}$ and comes from the APIWQED. The density of the order statistic $u_{i:n}$ is defined herein.

$$f_{k:n}(u_i) = \frac{n!}{(k-1)!(n-1)!}\Big[F(u)\Big]^{k-1}\Big[1-F(u)\Big]^{n-k}f(u) \tag{19}$$

Consequently,

$$= \frac{n!}{(k-1)!(n-1)!}\sum_{t=0}^{n-k}\sum_{t=0}^{k-1}\binom{n-k}{t}\binom{k-1}{t}\left(\frac{\alpha}{\alpha-1}\right)^{n-k-t}\left(\frac{-\alpha^{e-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}}{\alpha-1}\right)^{t}\left(\frac{\alpha^{e-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}}{\alpha-1}\right)^{k-1-t}\left(\frac{-1}{\alpha-1}\right)^{t}$$

$$\frac{log\alpha}{\alpha-1}\frac{ab\left(\frac{-ln(1-u}{\lambda}\right)^{-b-1}e^{-a\left(\frac{-ln(1-u)}{\lambda}\right)^{-b}}}{\lambda(1-u)}\alpha^{e^{-a\left(\frac{-\ln(1-u}{\lambda}\right)^{-b}}} \tag{20}$$

4 Maximum Likelihood Estimates

The parameter vector's log-likelihood (ℓ), $\theta = (\alpha, \lambda, b, a)$ may be stated *If* $x_1, x_2, x_3, ..., x_n$ as an n-item random sample from the APIWQED.

$$\ell(\alpha,\lambda,b,a,u) = nln\left(\frac{ln\alpha}{(\alpha-1}\right) + nln\left(\frac{ab}{\lambda}\right) + \sum_{i=1}^{n}(-b-1)ln\left(\frac{-\ln(1-u_i)}{\lambda}\right) - \sum_{i=1}^{n}\ln(1-u_i)$$
$$- a\sum_{i=1}^{n}\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b} + ln\alpha\sum_{i=1}^{n}e^{\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b}} \tag{21}$$

The Partial derivatives of (33) concerning each parameter

$$\frac{\partial\ell}{\partial\alpha} = n\left(\frac{\frac{\alpha-1}{\alpha} - ln\alpha}{(\alpha-1)ln\alpha}\right) + \frac{1}{\alpha}\sum_{i=1}^{n}e^{-a\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b}} \tag{22}$$

$$\frac{\partial\ell}{\partial\lambda} = \frac{-n}{\lambda^2} - \frac{(-b-1)}{\lambda} + ab\sum_{i=1}^{n}\frac{\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b-1}(-\ln(1-u_i))}{\lambda^2}\left[1 + ln\alpha\left(e^{-a\left(\frac{-ln(1-u_i)}{\lambda}\right)^{-b}}\right)\right] \tag{23}$$

$$\frac{\partial\ell}{\partial b} = \frac{n}{b} - \sum_{i=1}^{n}ln\left(\frac{-ln(1-u_i)}{\lambda}\right) - a\sum_{i=1}^{n}\left(-ln\left(\frac{-\ln(1-u_i)}{\lambda}\right)\right)\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b}\left[1 + ln\alpha\left(e^{-\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b}}\right)\right] \tag{24}$$

$$\frac{\partial\ell}{\partial a} = \frac{n}{a} - \sum_{i=1}^{n}\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b}\left[1 + \left(e^{-a\left(\frac{-\ln(1-u_i)}{\lambda}\right)^{-b}}\right)ln\alpha\right] \tag{25}$$

5 Applications

Real medical data sets have been used to test APIWQED, and their fitting has been compared to an additional handful of famous distributions.

Survival Time Data.

There were seventy-nine patient survival times in the original dataset. [4] infected with schistosomiasis. The results are shown below follows 0.04, 0.3, 0.31, 0.56, 0.94, 1.43, 1.485, 1.51, 1.515, 1.576, 1.624, 1.625, 1.654, 1.655, 1.765, 1.81, 1.87, 1.88, 1.91, 1.91, 1.91, 1.98, 2.012, 2.01, 2.038, 2.09, 2.09, 2.14, 2.15, 2.19, 2.19, 2.22, 2.22, 2.23, 2.3, 2.32, 2.39, 2.48, 2.61, 2.63, 2.63, 2.65, 2.66, 2.69, 2.82, 2.89, 2.9, 2.93, 2.96, 2.96, 3, 3, 3.1, 3.11, 3.12, 3.17, 3.34, 3.38, 3.44, 3.47, 3.48, 3.510, 3.58, 3.61, 3.78, 3.92, 4.04, 4.12, 4.17, 4.24, 4.26, 4.28, 4.31, 4.38, 4.45, 4.49, 4.57, 4.6, 4.66.

APIWQED and three other distributions were compared. With the use of the density functions listed below

1. (APE) Alpha power exponential distribution by [5]

$$f_{APE}(x) = \begin{cases} \frac{log\alpha}{\alpha-1}\lambda e^{-\lambda x}\alpha^{1-e^{-\lambda x}} & if\,\alpha \neq 1, \alpha > 0 \\ \lambda e^{-\lambda x} & if\,\alpha = 1 \geq 0 \end{cases}$$

2. (APIW) Alpha power inverse Weibull distribution by [6]

$$f_{APIW}(x) = \begin{cases} \frac{log\alpha}{\alpha-1}\lambda\beta x^{-(\beta+1)}e^{-\lambda x^{-\beta}}\alpha^{e^{-\lambda x^{-\beta}}} & if\,\alpha \neq 1, \alpha > 0 \\ \lambda\beta x^{-(\beta+1)}e^{-\lambda x^{-\beta}} & if\,\alpha = 1 \geq 0 \end{cases}$$

3. The Alpha Power Weibull Exponential Distribution (APWED) by [7]

$$f_{APWE}(x) = \begin{cases} \frac{\log\alpha}{\alpha-1}\frac{\alpha\lambda}{\gamma}\left(\frac{\lambda x}{\gamma}\right)^{a-1}e^{-\left(\frac{\lambda x}{\gamma}\right)^{a}}\alpha^{1-e^{-\left(\frac{\lambda x}{\gamma}\right)^{a}}} & ,\alpha > 0, \alpha \neq 1 \\ \frac{\alpha\lambda}{\gamma}\left(\frac{\lambda x}{\gamma}\right)^{a-1}e^{-\left(\frac{\lambda x}{\gamma}\right)^{a}} & ,\alpha = 1 \end{cases}$$

The proposed model's validity in relation to the other models was evaluated using the criterion for goodness-of-fit (GOF): Restrictions on Many statistics, such as AIC, CAIC, HQIC, Cramer-von Mises (W), and K-S, are discussed. A smaller number indicates a more optimal match.

Table 1 shows how well the APIWQED performs compared to Alternate distributions for the aforementioned real data sets.

Table 2 demonstrated that, compared to the other distributions, the APIWQED had the lowest AIC, CAIC, HQIC, K-S, and W ratings, showing Its effectiveness in adjusting to real-world datasets.

Table 1. For survival time data, MLEs are used, with SEs in parenthesis.

Distribution	Estimated Parameters			
APIWQE $(\hat{\alpha}, \hat{\lambda}, \hat{b}, \hat{a})$	5.6017 (12.9725)	0.6790 (2.8191)	9.0580 (64.9308)	1.0638 (1.0277)
APE $(\hat{\boldsymbol{\alpha}}, \hat{\boldsymbol{\lambda}})$	34.1428 (13.3994)	0.7691 (0.0592)		
APWE $(\hat{\boldsymbol{\alpha}}, \hat{\boldsymbol{\lambda}}, \hat{\boldsymbol{b}}, \hat{\boldsymbol{a}})$	25.6685 (40.1965)	2.6851 (199.6717)	4.9713 (369.7458)	1.5886 (0.3246)
APIW $(\hat{\alpha}, \hat{\lambda}, \hat{\beta}, \hat{a})$	3.9152 (1.2192)	0.1948 (0.0235)	1.239 (0.0695)	

Table 2. GOF criteria for survival time data.

Distribution	AIC	CAIC	HQIC	K-S	W	$-\ell(\hat{\theta})$
APIWQE	34.7295	35.2701	38.5266	0.15301	0.21939	13.3648
APE	281.9912	282.1375	283.9562	0.1603	0.6024	138.9956
APWE	267.4350	267.9350	271.3650	0.0652	0.0478	129.7175
APIW	354.8962	355.1925	357.8437	0.2619	1.2682	174.4481

6 Conclusions

This study presents a distinctive approach for creating distributions that provide a high degree of flexibility in expressing real-world data across several domains. The approach incorporates commonly used Advanced Persistent Threat (APT) techniques. The most recent release, APIWQED, has been unveiled. This method allows for incorporating diverse data patterns via the attractive features of the suggested distribution's hazard rate and density functions. The APIWQE encompasses essential statistical features such as moments, quantiles, medians, order statistics, average residual life, and maximal likelihood estimators (MLEs). The proposed distribution's efficacy was shown by effectively fitting an actual dataset. In general, the APIWQED model exhibited better performance than other competing models.

References

1. Hassan, A.S., Nassr, S.G.: The inverse weibull generator of distributions: properties and applications. J. Data Sci. **16**(4) (2018)
2. Mead, M.E., Cordeiro, G.M., Afify, A.Z., Al Mofleh, H.: The alpha power transformation family: properties and applications. Pakistan J. Stat. Oper. Res. 525–545 (2019)
3. Gupta, R.D., Kundu, D.: Generalized exponential distribution: different method of estimations. J. Stat. Comput. Simul. **69**(4), 315–337 (2001)

4. Young, N.D., et al.: Whole-genome sequence of Schistosoma haematobium. Nat. Genet. **44**(2), 221–225 (2012)
5. Hassan, A.S., Mohamd, R.E., Elgarhy, M., Fayomi, A.: Alpha power transformed extended exponential distribution: properties and applications. J. Nonlinear Sci. Appl. **12**(4), 62–67 (2018)
6. Basheer, A.M.: Alpha power inverse Weibull distribution with reliability application. J. Taibah Univ. Sci. **13**(1), 423–432 (2019)
7. Eghwerido, J.T., Zelibe, S.C., Efe-Eyefia, E.: Gompertz-alpha power iverted exponential distribution: properties and applications. Thailand Stat. **18**(3), 319–332 (2020)

Bipolar Disorder Detection Using Machine Learning Technique

Santhoshkumar Sundar[1(✉)], P. Subhasri[1], A. Sumathi[2], B. Srinivas[3], and J. Jegathesh Amalraj[4]

[1] Alagappa University, Karaikudi, India
santhoshkumars@alagappauniversity.ac.in
[2] SASTRA Deemed to Be University, Kumbakonam, India
[3] V.S.B. Engineering College (AUTONOMOUS), Karur, India
[4] Government Arts and Science College, Cuddalore, India

Abstract. An inability to complete daily tasks and changes in mood, energy, and activity level are symptoms of bipolar disorder, also known as manic-depressive illness type disorder. Serious consequences result from untreated bipolar disorder, such as elevated health care expenses, mortality, and morbidity, along with notable role impairment. It could take up to 15 years to get a diagnosis, despite the fact that there is a workable treatment option. Three common conditions—bipolar disorder, migraines, and epilepsy—have little known about their underlying pathophysiological mechanisms. It is rare for a patient to have co-morbidities between two of these conditions, but co-existence of all three is common. Here, we combine the information from the magnetic resonance imaging (MRI) scan with the random forest algorithm. These abnormalities usefulness in differentiating bipolar disorder patients from mental health issues or state-of-mind disorders defines patients based on their illness. Here, for accuracy, we employ machine learning algorithms such as CNN-MDRP (Multimodal Disease Risk Prediction) and Random Forest algorithm. We also use the attributes we gathered from the MRI to determine the risk factor and stage of the healthy patient. To obtain the output, we employ the machine learning algorithms discussed above along with a trained dataset. So, the system proposed gives adequate information about activity of patient such as Heart beat, motion, respiration and stress so that based on the real time data, the psychiatrist or pharma co-therapist can provide appropriate treatment according to the data provided. The provided system will also provide positional data so that the friends or relatives of that patient track him appropriately for an emergency and process with real time values derived from the sensors. So, the overall system provides the real time positional as well as sensory database which plays important role while treating the patient affected with the bipolar disorder.

Keywords: HRV (Heart Rate Variability) · sensory database · GSR (Galvanic Skin Resistance) · Migraines · Epilepsy · MRI (Magnetic Resonance Imaging)

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 458–467, 2025.
https://doi.org/10.1007/978-3-031-91008-1_40

1 Introduction

Periods of elevated mood and depression are hallmarks of bipolar disorder, a type of mental illness also known as manic-depressive illness. The cause is not cleared but mostly genetic and environmental factors, long time stress and childhood abuse plays a vital role in bipolar disorder [1]. It is treated by the combination of the pharmacotherapy, psychotherapy and medicine dose in term of Lithium is given. According to WHO's Mental Health Report the common Rate of bipolar disorder over the age of 18 is approximately 1.1% of the population and at any one time as 51 million people worldwide suffer from bipolar disorder and has bipolar disorder at some of the stages of their life and the common age at which symptom begins is generally 25. In India approximately 1% is affected by this disorder. Most of the peoples who are affected with this disorder are homeless or lives in shelters, prisons, hospitals or supervised houses. The proposed system can help to monitor the parameters which are changed due to the bipolar disorder and also try to give the position of the person so that appropriate measures can be taken while treatment.

As various changes in states of bipolar patients [2] carried out, these changes can be tracked by the various sensors management in terms of the smart phones. Bipolar patients undergo a variety of state changes, which can be monitored by the various smart phone sensors that are managed. Based on smartphone sensing, this system can identify manic and depressed states as well as changes in the mood of individuals with bipolar disorder. It provides bipolar disorder patients with a smartphone sensor-based system designed to assist and enhance their treatment. It provides modalities for sensors that encompass the various aspects of human nature related to disorders. As the patient overview screen [3] for bipolar disorder patient is provided for situational awareness of patient by using the MONARCA system. The system is capable of gathering the sensory data and information related to the patient like lifetime mood scores, patient information, disease information, medical contact, mood forecast, and medicine.

Patients with bipolar illness have far greater chances of recovery and long, healthy lives when the illness is identified early. Therefore, even though we are helpless to prevent it from happening to us, we can definitely recognize it early on and provide the appropriate medical care to the appropriate individuals at the appropriate time [4].

1.1 Objectives

The main objective of this work is to develop a system that can detect bipolar illnesses more accurately and economically by using the CNN-MDRP algorithm and random forest classification, which has been demonstrated to yield more accurate results. The current algorithms are not accurate. It is not yet complete to improvise the algorithms to incorporate the framework's increased productivity and thereby improve its operation. As of right now, there is no suitable online bipolar diagnosis framework used in clinics or hospitals.

2 Background Study

Lithium is the recommended medication for individuals with long-term bipolar disorder [5], according to pharmacological treatment of mental disorders in primary care settings. Lithium is a medication that medical professionals may start with. The amount of lithium prescribed should be maintained in accordance with the severity of the manic or depressive phase, as lithium therapy is likely beneficial against both. The detection of various parameters and for tracking mental situations [6] like physical activity, social engagement can be done by using various sensors accelerometer, GPS, gyroscope, barometer, compass, microphone, etc.

Forecasting depression of the bipolar disorder patient can give the guessing of the next day reading data [7]. So, it is possible to guess out the future details about particular patient hence proper treatment and therapy can be done according with the data gathered. Re-mind which is the mobile app which can be used to supports the treatment of people who diagnosed with bipolar disorder. In this the patient has to fill his daily report in terms of some parameters and accordance with the details filled in the app the related physician can be able to give proper treatment to the patient affected with the bipolar disorder. Respiratory signals have different values measured in various types of motion. By using wearable piezoresistive fabric sensor, respiratory rate monitoring can be done under various motion conditions.

2.1 Pathways to Diagnosis of Bipolar Disorder

Unrecognized Mania or Hypomania. To diagnose bipolar disorder, mania or at least transient hypomania must be found. This diagnosis is frequently overlooked or forgotten as a medical condition. However, patients who do not remember episodes of affective disturbance may remember the consequences of those episodes, as well as people close to them.

A proper definition of the manic syndrome and the shortest possible duration of symptoms are necessary for diagnostic criteria for hypomania that have sufficient specificity and sensitivity. The table enumerates signs that could indicate a manic episode. Patients might remember symptoms or behavioral changes more clearly than individual illness episodes. One harmful aspect of manic episodes can be distorted interpersonal behavior, such as disregard for proper social boundaries or interpersonal boundaries. Therefore, it is important to question patients about scenarios that could have resulted from the impulsivity, poor judgment, or interpersonal issues that can accompany manic episodes (Table 1).

The Mood Disorder Questionnaire was designed to ask about any past occurrences of any of the symptoms that make up the diagnostic criteria for mania in order to screen for bipolar disorder [8]. Bipolar disorder is thought to be more likely in people who can remember at least seven of these. During manic episodes, delusions and formal thought disorders are frequent. Delusions that are mood-incongruent typically indicate a more serious psychosocial impairment. The psychotic features of first manic episodes may be particularly common, giving rise to a presentation akin to schizophrenia-form disorder.

Table 1. Evidence Suggesting Past Manic Episodes.

S.No	Evidence Suggestions
1	Recurrent brief periods of hypomania or clusters of hypomanic symptoms
2	Consequences of mania
3	Recurrent interpersonal conflicts
4	Extreme extroversion that leads to problems
5	Legal problems, sexual promiscuity or other events possibly related to episodic impulsivity
6	Sudden or frequent job or career changes
7	Severe or recurrent financial reverses or indiscretions

* This evidence should be taken together with other historical and current clues before making a diagnosis of bipolar disorder

Though it still hovers around 50%, the incidence of psychosis doesn't seem to be as high in later manic episodes.

Detection of Bipolar Depression

The majority of bipolar episodes, including the initial one, are typically depressive. It's possible that prior manic episodes were overlooked in some of these cases. Nonetheless, the majority of bipolar disorder morbidity seems to be caused by depression. This section will cover the differences between bipolar depression and unipolar depression (referred to as major depressive disorder in the DSM-IV), as well as predictors of the diagnosis of bipolar disorder in patients initially thought to have recurrent depressive illness.

The diagnosis of patients initially thought to have major depressive disorder may change to bipolar disorder because depression frequently precedes bipolar disorder episodes and early hypomanic episodes are frequently overlooked [9]. A table that lists the features of bipolar depression. According to a naturalistic chart review study, 37% of bipolar disorder patients were originally misdiagnosed as having major depressive disorder. In two studies, patients with a stable diagnosis of unipolarity were compared to those of similar age with a change in diagnosis to bipolar. The subsequent diagnosis of bipolar disorder was based on a combination of factors, including a higher number of prior depressive episodes, increased mood lability, an earlier onset of illness, and a higher degree of variability in the associated psychiatric problems, or "pleomorphic" pathology (Table 2).

3 Proposed System

Our system's architecture is shown in Fig. 1, and both front-end and back-end development have gone into the development of the application. All of the patient and physician data is stored in SQLite, along with reports. In addition to predicting main diseases, the Random Forest Machine Learning Algorithm also predicts sub-diseases. The Map Reduce Algorithm shortens the query retrieval time while simultaneously improving

Table 2. Clinical Characteristics of Bipolar Versus Unipolar Depression.

S.No	Episode Characteristics of Bipolar depression	Course Characteristics of Bipolar disorder
1	More motor slowing	More relatives with affective especially bipolar
2	More atypical neurovegetative features: Severe slowing, rejection sensitivity	Mood liability
3	Poor response or loss of initial response	Susceptibility to behavioral activation or mood liability

operational efficiency. [10] The suggested method differs from the ancestor's method of operation in that it computes diseases and their corresponding sub-diseases using a random forest machine learning procedure which consequently improve performance and efficiency and shorten query response times. Additionally, it provides unique patterns to every patient, resulting in a customized experience. Furthermore, it offers precise dosages for individual patients to track their condition. Hence, our system is widely accessible to everyone at a reasonable cost. In comparison to other prediction algorithms, the CNN-MDRP algorithm achieves a prediction accuracy of 94 percent.

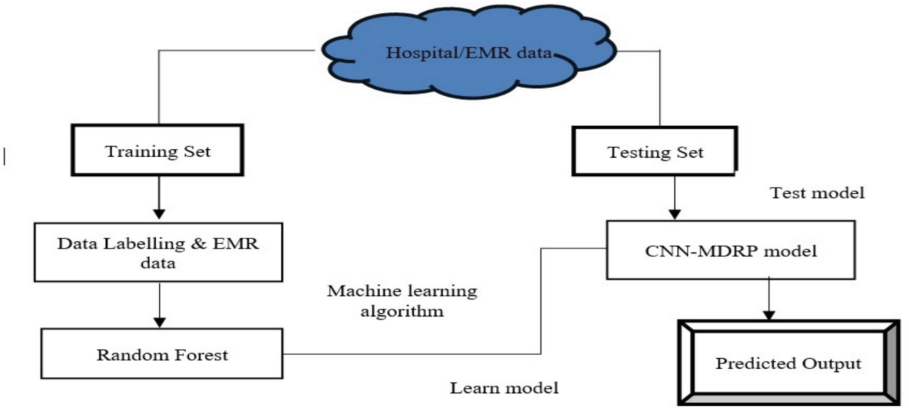


Fig. 1. Architecture Diagram of the proposed method

This module contains all of the patient data that the hospital management has provided, including MRI scans and other data types. Both structured and unstructured values of the attributes of brain anatomy will be used in this instance; structured data is derived from patient reports, while unstructured data is gathered from the patient's medical history, informal discussions with the physician, and other sources. Testing data and the training set: In order to generate complex outcomes, we use training set data, which is used to program the formation of technologies such as neural networks. When testing data, the collected information is used to confirm that test cases are being executed

and that any software applications are producing the desired results. DATA Labeling Preparation: In this module, we will identify the raw data and then go on to add context, meaning, and informative elements to prepare the data for future enrichment. We attempt to supplement or enhance the acquired data in this section by adding pertinent context that we have learned from other additional sources. The CNN-UDRP algorithm, which is part of the current system and only uses structured data, provides less accuracy than the proposed algorithm. We collect data from clinics and hospitals, process it using CNN-MDRP, and then use the result to predict the risk of the disease. The random forest classifier, which provides a framework and also quantifies the values of an outcome, receives this data in addition for classification.

The proposed system can be able to collect and process the entire sensory database from the sensors applied to the patient, who is affected with bipolar disorder with less power consumption [11]. By using power optimized coding, it is possible to lower the power consumption. As the sensors can be tuned to particular levels only so the power consumption takes place in active mode only and in idle mode the power consumption will be less. It gives various details like heart rate details, motion database, skin resistance details or respiration details for further processing and evaluation of the patient for further treatment. The sensory database provided plays important role while treatment of the patient.

3.1 Sensor Management

As various types of sensors can be used for the detection of the states and state variations of the bipolar disorder affected patient. The various sensors which are concerned with the system are given.

i) Heart beat sensor

It can be used to detect the heart rate variation or HRV of the concerned patient. As the heart rate details are different for different manic situations [12]. As the heart beats increases while patient is suffering from manic episodes. Following to the information related to heart rate, it is possible and easy to the psychiatrist or physician to take proper decision while the treatment of the patient.

ii) Motion sensor

As the relative motion of the patient who is affected with the bipolar disorder, changes suddenly as during the manic-depressive states varies. So, it is possible to detect the variation in the physical behaviour of the patient using sensors like accelerometer or gyroscope.

iii) Galvanic skin response or Respiratory fabric sensor

GSR can be used to measure the electrical conductance of the skin. It acts as inductor for psychological or physiological treatment. As there happens some changes in the respiration while depression or manic phases so the piezoresistive fabric sensor can be used, which can be used for the respiration measurement of the patient.

iv) Body heat Sensor or Temperature Sensor

To check the variations in heat or temperature happens during the depressive phases, body heat sensor can be used.

v) Position Tracking

As the patients affected with bipolar disorder mostly lived in stressed environment so such patient requires some space of freedom. So, by connecting this device it is possible to give freedom by applying GPS with the sensors. If any major variations happen in parameters, then GPS helps to track the patient.

3.2 CNN MDRP (Multimodal Disease Risk Prediction)

Gathering CNN-MDRP is done to effectively predict who is affected by the illness by using a convolutional neural network that makes use of both structured and unstructured data from the hospital. First, from the dataset that we regard as a repository, we use the potential segment model to identify missing data from the clinical records. Furthermore, with the aid of factual knowledge, we were able to control the basic degenerative illness that was previously known. Additionally, interacting with clinic or hospital specialists to handle structured data in order to obtain properties and reusable information. The CNN rule allows properties to be precisely abused in disorganized areas. Thus, we can conclude that the CNN-MDRP is the most effective solution for this particular issue.

3.3 Proposed Design

The assembly of the design can be shown as in Fig. 2. The Arduino kit can be used to which different sensors have to be connected. The sensory database collected from the patient could be collected on the desktop or notebook computer with the help of one of the connection medium and processed by MATLAB software. We can use Bluetooth or Wi-Fi or Zigbee module for connection purpose.

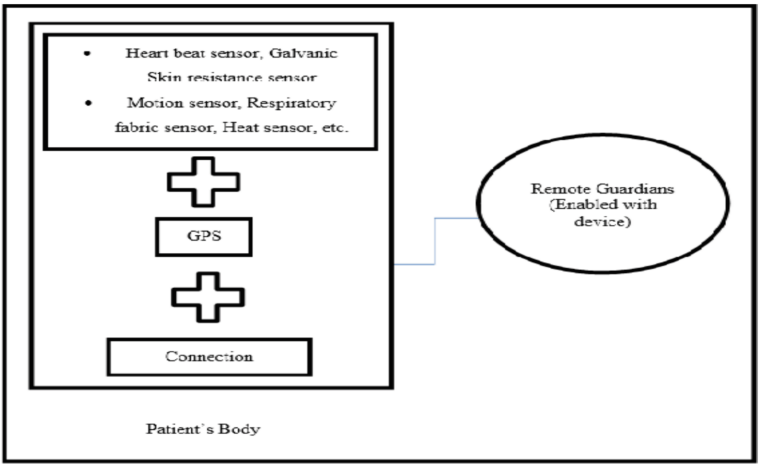


Fig. 2. Design of the processing

The database collected can be processed for further possibilities while treating the patient by psychiatrist or by the physician. The patient's parents or relatives can also be using the day-to-day database for caring and analysis purposes.

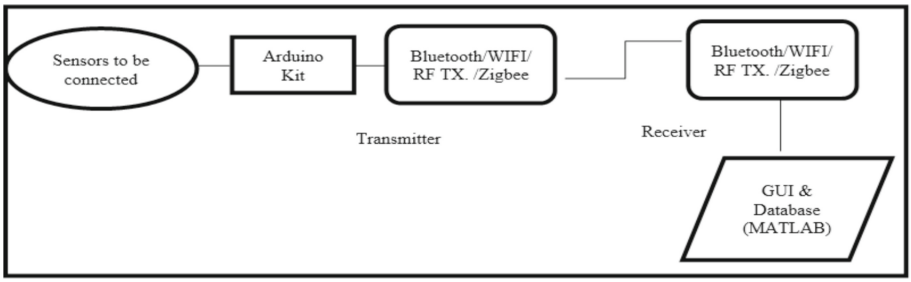


Fig. 3. Flow Diagram of the proposed method

The flow diagram of the proposed method can be given in Fig. 3. The data collected from various sensors can be processed with the help of Arduino kit which can be transmitted to the portable devices like laptop or mobile for data gathering and synthesis purpose. As the collection of databases provide the future precautions while treating the patient. The communication medium depends upon the range, as range varies device to device, so various modules can be used for reliable communication purposes. The proposed system is significant and differs from previous work as it provides real time database in the form of sensor management for proper treatment of patient.

4 Results and Discussions

According to this system's experimental results, CNN-mdrp produces the best and most accurate results out of all the algorithms currently in use [13]. Utilizing the CNNmdrp algorithm, we were able to incorporate both structured and unstructured patient data that was obtained from the hospital's clinical records. There was no other system that could handle both organized and unorganized data. An accuracy of 94.3% is provided by our suggested algorithm. Accordingly, the new algorithmic combination produced superior outcomes than the current ones. Thus, the accuracy percentage rises while the error rate is decreased by the suggested system. The comparison and explanation of the current algorithms are displayed below.

For the examination's assessment. First, we identify as evident positive false positive (the number of cases incorrectly anticipated as required), True negative (the number of examples correctly anticipated as not needed), False negative (the number of examples incorrectly anticipated as not needed), and TP (the number of occurrences accurately anticipated as required), separately. At that point, four estimates are available to us:

Accuracy, Precision, Recall and F1-measure as follows:

1. `Accuracy = (TruePos + TrueNeg)/ (TruePos + False Pos + TrueNeg + FalseNeg)`
2. `Precision = TruePos/ (TruePos + FalsePos)`
3. `Sensitivity = TruePos/ (TruePos + FalseNeg)`
4. `Specificity = TrueNeg/ (TrueNeg + FalsePos)`

The suggested algorithm is the random forest algorithm. The existing algorithms that have been used previously are linear regression, SVM, and decision trees (Table 3).

Table 3. Comparative Analysis.

Algorithm [13]	Accuracy	Precision	Sensitivity	Specificity
Linear	64.3%	0.7	0.8	0.59
SVM	88.1%	0.86	0.8	0.88
Decision Tree	91.0%	0.92	0.81	0.95
Linear	94.0%	0.93	0.9	0.97

5 Conclusion

Bipolar disorder is depressive illness type disorder which can be treated using pharmacotherapy and psychotherapy if proper data about patient is available. The proposed system provides the necessary data about patient in the sense of sensory database and also provides independence to the patient to live freely while travelling. This importance of system provides major role while treatment as well as taking personal healthcare of the patient. The suggested system is entirely based on the graphical user interface (GUI), with a focus on scalability, dependability, and user adaptability. It can be readily expanded to meet any future needs. By eventually lowering the cost of treatment, this model has the potential to benefit a large number of people. Additionally, the proposed system would assist in meeting the need to prepare the necessary instruments for clinical studies, which are made available to physicians as well as other individuals who require the patient's mental status to be known. This tool can be used by general practitioners to make preliminary diagnoses regarding a patient's mental health.

References

1. Valenza, G., Citi, L., Gentili, C., Lanata, A., Scilingo, E.P., Barbieri, R.: Characterization of depressive states in bipolar patients using wearable textile technology and instantaneous heart rate variability assessment. J. Biomed. Health Inform. **19**(1) (2015)
2. Valenza, G., Nardelli, M., Bertschy, G., Lanata, A., Scilingo, E.P.: Complexity modulation in heart rate variability during pathological mental states of bipolar disorders. In: 8th Conference of the European Study Group on Cardiovascular Oscillations ESGCO (2014)
3. Grünerbl, A., et al.: Smartphone-based recognition of states and state changes in bipolar disorder patients. J. Biomed. Health Inform. **19**(1) (2015)
4. Puiatti, A., Mudda, S., Giordano, S., Mayora, O.: Smartphone-centred wearable sensors network for monitoring patients with bipolar disorder. In: 33rd Annual International Conference of the IEEE EMBS Boston, Massachusetts USA (2011)
5. Prociow, P.A., Crowe, J.A.: Development of mobile psychiatry for bipolar disorder patients. In: 32nd Annual International Conference of the IEEE EMBS Buenos Aires, Argentina (2010)

6. Lanata, A., Valenza, G., Nardelli, M., Gentili, C., Scilingo, E.P.: Complexity index from a personalized wearable monitoring system for assessing remission in mental health. IEEE J. Biomed. Health Inform. **19**(1) (2015)
7. Kim, J.H., Diamond, D., Lau, K.T.: Development of portable device for monitoring the lithium level from bipolar disorder patients. In: 2011 5th International Conference on Pervasive Computing Technologies for Healthcare (PervasiveHealth) and Workshops, ICST (2011)
8. Kim, J.H., Diamond, D., Lau, K.T.: Development of Non-invasive Biochemical Device for Monitoring the Lithium Level from Saliva for Bipolar Disorder Patients. IEEE (2011)
9. Matthews, M., Abdullah, S., Gay, G., Choudhury, T.: Tracking Mental Well-Being: Balancing Rich Sensing and Patient Needs. Published by the IEEE Computer Society (2014)
10. Lanata, A., Greco, A., Valenza, G., Scilingo, E.P.: A pattern recognition approach based on electrodermal response for pathological mood identification in bipolar disorders. In: IEEE International Conference on Acoustic, Speech and Signal Processing (ICASSP) (2014)
11. Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.) Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
12. Peng, S.-L., Lin, C.-K., Pal, S. (eds.) Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
13. Peng, S.-L., Hao, R.-X., Pal, S. (eds.) Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4



Augmented Reality and Teaching: Alternative Pedagogy for Modern Learners

Chinnasamy Renuga Devi(✉)

Mother Teresa Women's University, Kodaikanal, Tamil Nadu, India
renugajp@gmail.com

Abstract. Disruptive Education a foremost outcome of the virtual and online education in the contemporary scenario drastically shifted teaching learning to remote mode. Educational institutions radically transformed their ways of service provision from direct teaching to online teaching. Both digital natives and digital immigrants were involved in this process and expected to access and deliver information online. This drastic transformation in the teaching-learning process demands augmented reality-enabled teaching methodologies as an alternative pedagogy of teaching that suits modern learners. Augmented Reality (AR) contributes to developing a generation of citizens influenced by technology. Augmented Reality brings together the real world with similar computer-generated elements artificially. The mixture of real and virtual information provides a novel learning experience that positively influences learners. This article discusses the avenues of augmented reality in increasing intrinsic motivation among the students along with the opportunities provided to explore related information at their own pace facilitating them to construct their knowledge. AR allows educators to introduce novel and innovative teaching approaches and procedures in the classroom through customized AR tools. It also addresses competency-based education and the personalized learning needs of learners.

Keywords: Alternative Pedagogy · Augmented Reality · Disruptive Education · Modern Learners · Teaching

1 Introduction

Twenty-first-century learning framework emphasizes learning and innovation skills as a central component that includes four important "Cs": Critical Thinking, Creativity, Communication, and Collaboration focusing on curriculum and instruction for professional development blended with Information, media, and technological skills-based learning environment in developing life and career skills of an individual [1, 2]. Skills meant for the 21st century require dynamic knowledge acquaintance that focuses upon self-regulated learning. This stimulates learning interest among the learners and motivates them to participate in the activities designed related to the content. Augmented Reality referred to as AR is an improved or upgraded description of materials that exist in the real world with the usage of digital visualization through various stimuli that include sound,

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 468–476, 2025.
https://doi.org/10.1007/978-3-031-91008-1_41

light, and eye-catching novelty. Augmented reality applied in the teaching-learning process enhances learners' perception through real-time interaction as the virtual objects transmit information that augments them to execute real-world tasks. It enhances collaborative learning and critical thinking skills. AR promotes self-regulated learning among the learners in addition to the usual learning experiences provided by the teacher in disruptive education.

Augmented Reality: An Overview

American engineer Ivan Sutherland is recognized as the pioneer of developing AR technology in 1968 at Harvard. He designed 3D modeling and visual simulation software, Sketchpad. Tom Caudell, a Boeing researcher, first coined the word "Augmented Reality" in the year 1990 Advancements in AR over the years served in specific sectors such as aviation and the military. Rapid technological innovations resulted in significant advancements in AR technology during the 2000s and the first commercial AR application evolved in 2008. Augmented reality since its early conception has moved a long way, and particularly advancements in AR in almost all fields including education during the past few years are noteworthy. AR can transform and revolutionize the learning environment in a better way and progress in the right direction [3]. The adoption of augmented reality is on the rise as learners become increasingly dependent on mobile devices for virtual learning in the disruptive education delivered through remote mode. The application of AR-enabled technology in content delivery results in a change of perception of the learners about virtual learning since it provides an interactive learning experience that regulates them to stay motivated throughout the session [4].

AR is a promising technological advancement that smoothens the path of knowledge exploration among learners by blending virtual information in the real world to provide real-time experience to learners. AR technology applied in education draws learners with interest to study new concepts with ease and familiarity. Augmented Reality can be successfully employed in learning to motivate and occupy students which enables their fullest participation. AR can be used to create new dimensions in the classroom learning. In recent times application of augmented reality in classroom instruction progressed rapidly as digital gadgets gradually gained more influence and shifted to portable mode [5].

Three characteristics of Augmented Reality expounded by [6, 7] include.

1. The incorporation of physical and virtually simulated objects delivers a real-time learning experience.
2. Collaborative integration between real and virtually simulated objects
3. Real-time (synchronized) interface between physical and virtually simulated objects.

Recent advancement in Information and Communication Technology (ICT) and its rapid transformation facilitates a mobile device with an inbuilt camera to integrate virtual images with real-time interaction. Computers, laptops, tablets, and iOS, and Android-based mobile phones enable learners to have easy access to content that is previously available in the gadgets through AR technology persuading for higher learning autonomy. ICT exploration by the students thereby promotes collaboration, innovation, and creativity skills which becomes obligatory to develop 21st century learning skills among them [8]. The key characteristic of AR application is integration and interaction of the

real and virtual environment which allows for huge adaptability and creativity in the teaching-learning process. Development of printed content and presentation added with graphical elements recognized by AR applications such as 3D files, images, and teaching videos sustain the motivation and interest of the learners.

1.1 Objectives of the Study

1. To explore Augmented reality-facilitated instructional approaches in modern-day classrooms.
2. To explore the potentials of the augmented reality-enabled learning process and tools in addressing the personalized learning needs of learners

2 AR Contextualized Teaching and Learning

2.1 Motivation

In the present scenario, basic skill acquisition in digital literacy is mandated as an integral aspect of overall literacy appraisal. Visual, auditory, pictorial illustration and non-linguistic experiences provided to learners through AR teaching enable them to think visually through images along with written texts. Interactive learning experiences provided by AR with audio, augmented posters with images, video, and 3-D models arouse intrinsic motivation of the learner as it exclusively relies upon the enjoyment of performing a task only for the sake of its accomplishment. Educators can instill motivation and interest among the learners and engage them in constructive learning by augmenting the content and presentation with scaffolding of visual aids that provide a multimedia experience [9].

2.2 Presentation of Content

The basics of Augmented Reality is to superimpose digital information directly upon a sensory perception of the user. The AR-influenced presentation can be a combination of multimedia information that includes spatial 3D models, images, texts, video, animations, and sound, superimposed/overlaid into a student's real learning setting. Textbooks, handouts, and other materials used for learning entrenched with 'markers' accessed by a device mounted with augmented reality features generate additional details and guidance to learners in multimedia format. AR-enabled presentation of content promotes learning gains for the students, interaction, and collaborative learning [10]. AR further licenses to learn in remote settings by promoting it through collaborative initiatives. Learners and instructors mutually benefitted in this setting by sharing a common virtual platform wherein a virtually simulated learning environment is created with augmented learning materials. The prospective benefits of AR-enabled educational and instructional framework at higher order level encompass visualization of challenging and abstract concepts through spontaneous, concrete illustrations and real reciprocation with a multimodal depiction of teaching-learning material. Teachers can create specific content that is unexplored using AR technology in the following phases as shown in Fig. 1:

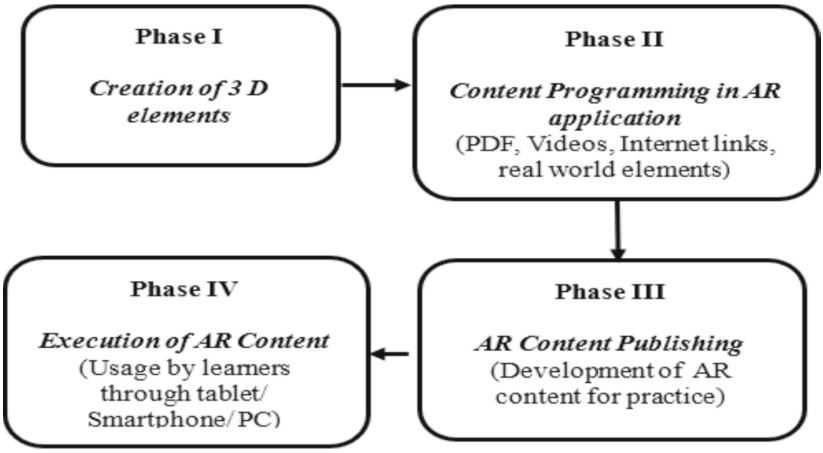


Fig. 1. Phases of Content creation using AR technology

AR-enabled content creation and delivery rightly fit Bloom's Taxonomy of attaining learning objectives of a course/program encompassing three main spheres of learning cognitive, affective, and psychomotor domains. The taxonomy of learning proposed by Benjamin Bloom guides educators to achieve learning objectives through appropriate planning and instruction delivery and ensures the design of suitable tasks and strategies. As guided by Bloom's taxonomy, AR-based presentation addresses the learner's intellectual and ability level, which gradually helps them attain higher-order thinking skills characterized as critical thinking. Table 1 explicitly illustrates the application of Bloom's digital taxonomy [11] to the digital learning environment along with the functional level of each domain and the tools used in its implementation.

2.3 Self-regulated Learning

AR-integrated content encourages observations and field explorations since it is possible to explain reality observed with the augmentation of virtual content that includes tutorial videos and 3-D images. Higher autonomy and self-reliance in the learning process can be attained through this interaction. Self-regulated learning of students in the AR-enabled learning environment gives the teacher additional time to explain more complex areas in the content [12]. The sensorial experience and interaction provided by AR-enabled technology can improve students' learning gratification, structure their knowledge construction, and complete the designated learning tasks with efficiency [13, 14]. A learner-centric learning environment promoted by AR technology provides learners with a deeper and richer learning experience, as it promotes greater participation and involvement in learning. This learning approach promotes learners to actively engage and get connected with the learning process which enables them to build upon their learning methods and strategies with responsibility and acts as a motivating factor in learning.

Table 1. Bloom's Digital Taxonomy

Bloom's Revised Taxonomy	Bloom's Digital Taxonomy	Functional Level	Tools	
Create	**Create**	Create a new or unique work	Programming, filming, animating, blogging, Publishing, Wiki building, Video blogging, Video casting, podcasting, Directing	**Higher Order Thinking Skills**
Evaluate	**Evaluate**	Criteria-based decisions and maintaining standards over scrutiny and assessment	Blog commenting, reviewing, posting, moderating, collaborating, reflecting, testing	
Analyze	**Analyze**	Draw connections among ideas, and thoughts- determines interconnection within the entire structure (linkages with each part of the whole structure)	Hacking, mashing, linking, validating, Mind mapping,	
Apply	**Apply**	Application of learned concepts in practice through models, diagrams, or presentations	Running, loading, playing, operating, uploading, sharing with group, editing	**Lower Order Thinking Skills**
Understand	**Understand**	Explicate thoughts, ideas Hypothyse meaning from printed or written text, images, or visuals	Advanced searching, Blog journaling, categorizing, tweeting, tagging, commenting, annotating, subscribing	
Remember	**Remember**	Recollection of facts or retrieval of material	Bullet pointing, highlighting, bookmarking, group networking, shared book, searching,	

3 AR Tools for Teaching

Web technologies and the internet have become indispensable in the present learning environment in addition to printed text learning. AR devices improve the accomplishment rate of real-time interaction in learning tasks and support learning activities based on memory and recollection of concepts. Implementation of AR in education significantly contributes to knowledge exploration in various areas allowing for insightful and interactive learning.

AR technology provides a real-time learning experience to the learners through visualization and interaction in the normally printed textbooks by installing relevant

mobile apps [15]. This 3D technology enables learners to connect real and virtual world and supports real-time interaction. People without a sound technological background can still have a rich interactive learning experience by accessing printed books through handheld display devices. It provides a virtual experience of objects in printed books [15]. Table 2 portrays an overview of the application of AR tools in modern classroom teaching learning.

Table 2. AR tools with their application in the classroom or remote learning

AR Tools	Application
Aurasma, Layar	Amplified posters replicated with imageries, visuals, sound, 3D models, typescript website links, and quizzes that invite explicit student participation
Anatomy 4 D	Human Physiology: Exhibits resourceful 3D models that provide interactive experiences to learn about anatomy (Human Physiology and functions)
ARLOOPA	Augmented Printed Materials Interactive Textbooks
SolAR	Concepts related to the Solar System
Math ninja AR	Basic Maths Learning
AR reader	To read any language

4 AR and Disruptive Teaching

Disruptive education proposes to break down and interrupt the previously established(conventional) customary prototypical model of education, that either develops and improves the prevailing one or aligns with the changing scenario in educational practices. Disruptive education emerges out of the existing social paradigm and changes that influence it [16]. And disruption of existing social paradigms creates an opportunity for the emergence of new forms of education referred to as disruptive education. The key factors of disruptive education are to enable.

- students to access the present world as digital natives
- Customized learning - tailor-made personalized learning to bring out the fullest potential of the student
- integration of artificial intelligence as a vital process to improve education
- encouraging critical thinking among the students

Disruptive education influences self-taught learning, personal tutoring, and blended learning which closely resembles to AR-enabled teaching-learning process. Augmented Reality (AR) is a technology-enabled learning process in which learners acquire knowledge and skills by manipulating virtually simulated objects in the real physical world. The application of AR in educational frameworks attracts learners to study new concepts easily through systematic and creative delivery of instruction. The basic features of AR

connect the real and virtual world and provide real-time interaction through precise 3D recording of virtually simulated and actual objects [17]. Augmented reality concerning disruptive technology provides the possibility to secure effective academic gains in education whenever the regular education system is interrupted. Online education resulted from the COVID-19 pandemic and is a classical example of innovation in disruptive education. Web-based software AR allows learners to benefit from the services provided by the educational organization and learn from their own homes without any scheduling issues.

Augmented reality-based posters replicated with imageries, visuals, sound, online quizzes, 3-D visual representation of chemical reactions, human anatomy, and learning through gratifications allow the everyday online classroom to be reconditioned with the intersection of data and facts. Learners can be engaged in math class by linking physical world experience to math equations [18].AR enhances various abilities of the learners including problem-solving and collaboration and prepares them for the future by developing critical thinking skills. Teachers can improve the learning outcomes of the students through effective engagement and interactivity through augmented reality-enabled content development and its presentation. In a nutshell, augmented reality serves as an alternative pedagogy in a disruptive education environment to prepare better students for the future.

5 Surmounting Challenges in AR-Enabled Learning

Equitable access to technology by all learners poses a great challenge that can be surmounted through the earnest efforts of teachers and the Government [19]. The technology-related policy framework of the government plays a dynamic role in ensuring students equitable access to technology by investing in advanced infrastructure and high-speed internet connectivity. The Government of Tamil Nadu, India has been providing free laptops to students at higher secondary levels since the academic year 2011–12 [20] to promote digital learning in the government and government-aided schools and 2 GB free data card per day from January 2021 to students enrolled in government higher education institutions in the state.

Technology-driven continuous teacher training initiatives for in-service teachers [21] to promote their professional development and techno-pedagogy teaching practices incorporated in the curriculum of preservice teacher training will set a platform for digital learning that addresses to demands of futuristic techno-driven classrooms. Similarly, teachers should ensure that students are solitarily substantiated with AR-facilitated learning experiences to enhance their core learning and not overloaded with technological inputs.

Smooth integration of AR into the curriculum improves AR-facilitated teaching-learning practices and its steady success depends on the constant collaboration between educators and curriculum developers [22]. It further explores ways to integrate AR-based activities in the assessment and evaluation process. Installing vibrant and comprehensive antivirus software in user devices provides guaranteed protection from online threats, data security concerns, privacy, and other evolving cyber security threats from various social media networks.

The revolutionization of technological advancements mandates the education system to adapt emerging technologies like augmented reality in classroom learning. It embarks on the potentiality of establishing AR-facilitated inclusive equitable learning environments for students of all ages and backgrounds to transform teaching and learning paradigms to meet the demands of 21st-century learners.

6 Conclusion

The technology-influenced teaching-learning process is widely extended to every single form and level of the instructional framework due to the development of a disruptive education environment induced by the pandemic situation in the present scenario. Even though recognized for quite a while, Augmented reality (AR) shaped through digitally framed solutions is gaining momentum and expanding its potentiality as a result of the prevailing online and remote teaching-learning state of affairs. Despite all technological advancements application of AR in the field of education remains unexposed. When education becomes a doorway to establishing a career and further achievements, new originations and their application to suit the changing scenario must be evolved and executed to contribute significantly to societal change. Incorporation of AR in the teaching-learning process mandates to design flexible environment along with sufficiently developed digital competencies on the part of teachers and learners. Training teachers to update and develop technical competencies in AR to create technology-influenced educational materials with innovation and effective presentation of content to meet the demands of students who are digital natives is mandated for augmented reality to turn out as an alternative pedagogy for modern learners in disruptive teaching.

References

1. Partnership for 21st-century skills. https://files.eric.ed.gov/fulltext/ED519462.pdf
2. 21st-Century Skills: What potential role for the Global Partnership for Education? A Landscape Review. https://files.eric.ed.gov/fulltext/ED627371.pdf
3. Daniela, L.: New Perspectives on Virtual and Augmented Reality Finding New Ways to Teach in a Transformed Learning Environment. Routledge, Abingdon (2020)
4. Al-Ansi, A.M., Jaboob, M., Garad, A., Al-Ansi, A.: Analyzing augmented reality (AR) and virtual reality (VR) recent development in education. Soc. Sci. Humanit. Open **8**(1) (2023). https://doi.org/10.1016/j.ssaho.2023.100532
5. Lee, K.: Augmented reality in education and training. Tech. Trends **56**(2), 13–21 (2012). https://doi.org/10.1007/s11528-012-0559-3
6. Azuma, R., Baillot, Y., Behringer, R., Feiner, S., Julier, S., MacIntyre, B.: Recent advances in augmented reality. IEEE Comput. Graphics Appl. **21**(6), 34–47 (2001). https://doi.org/10.1109/38.963459
7. Azuma, R., Billinghurst, M., Klinker, G.: Special section on mobile augmented reality. Comput. Graph. **35**(4), vii–viii (2011). https://doi.org/10.1016/j.cag.2011.05.002
8. Shumaker, R., Lackey, S. (eds.) Virtual, Augmented and Mixed Reality Applications of Virtual and Augmented Reality 6th International Conference Proceedings, Part II, June 22–27; Heraklion, Crete, Greece (2014). https://doi.org/10.1007/978-3-319-07464-1

9. Coimbra, M.T.M., Cardoso, T., Mateus, A.: Augmented reality: an enhancer for higher education students in math's learning? Procedia Comput. Sci. **67**, 332–339 (2015). https://doi.org/10.1016/j.procs.2015.09.277
10. Chien, C.-H., Chen, C.-H., Jeng, T.-S.: An interactive augmented reality system for learning anatomy structure. In: Proceedings of the International Multi-Conference of Engineers and Computer Scientists, March 17 -19; Hong Kong pp. 370–375 (2010). https://www.iaeng.org/publication/IMECS2010/IMECS2010pp370-375.pdf
11. Armstrong, P.: Bloom's Taxonomy. Vanderbilt University Center for Teaching (2010). https://cft.vanderbilt.edu/guides-sub-pages/blooms-taxonomy/
12. Martín-Gutiérrez, J., Contero, M., Alcañiz, M.: Evaluating the usability of an augmented reality based educational application. In: Aleven, V., Kay, J., Mostow, J. (eds.) Intelligent Tutoring Systems. Lecture Notes in Computer Science, vol. 6094. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-13388-6_34
13. Dalgarno, B., Lee, M.J.W.: What are the learning affordances of 3-D virtual environments? Br. J. Educ. Technol. **40**(6), 10–32 (2010). https://doi.org/10.1111/j.1467-8535.2009.01038.x
14. Dunleavy, M., Dede, C., Mitchell, R.: Affordances and limitations of immersive participatory augmented reality simulations for teaching and learning. J. Sci. Educ. Technol. **18**(1), 7–22 (2009). https://doi.org/10.1007/s10956-008-9119-1
15. Huisinga, L.A.: Augmented Reality Reading Support in Higher Education: Exploring Effects on Perceived Motivation and Confidence in Comprehension for Struggling Readers in Higher Education. Graduate Theses and Dissertations (2017). https://doi.org/10.31274/etd-180810-5151
16. What is disruptive education? Disruptive education for meeting the challenges of the future. https://www.iberdrola.com/talent/disruptive-education
17. Bohdal, R.: Devices for virtual and augmented reality. In: Prodromou, T. (eds.) Augmented Reality in Educational Settings, pp. 410–444, Brill Sens, Leiden, Netherlands (2020). https://doi.org/10.1163/9789004408845
18. Kaufmann, H., Schmalstie, D.: Mathematics and geometry education with collaborative augmented reality. Comput. Graph. **27**(3), 339–345 (2003). https://doi.org/10.1016/S0097-8493(03)00028-1
19. What It Means to Have Equitable Access to Technology for Today's Students & Educators. https://www.goguardian.com/blog/equitable-access-to-technology
20. Scheme for Distribution of Laptop Computers to Students. https://elcot.in/student-free-laptop
21. Marques, M.M., Pombo, L.: The impact of teacher training using mobile augmented reality games on their professional development. Educ. Sci. **11**, 404 (2021). https://doi.org/10.3390/educsci11080404
22. The Impact of Augmented Reality on the Future of Learning. https://elearningindustry.com/the-impact-of-augmented-reality-on-the-future-of-learning



Fostering Democratic Transparency: A Secure Voting System with Aadhaar Cards on the Ethereum Blockchain Technology

S. Revathi[1] and V. R. ELangovan[2(✉)]

[1] Department of Computer Science, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, India
[2] Department of Computer Applications, Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, Chengalpattu, India
elangotesting@gmail.com

Abstract. Democracy's cornerstone, elections necessitate trust and transparency. As a result of the demand for security, verifiability, and visibility, the voting landscape is always changing. This abstract outline a novel method for secure voting that integrates the Ethereum blockchain and India's Aadhaar identification system. It combines the immutability and transparency of blockchain technology with Aadhaar identity verification. Solutions that guarantee voter and data integrity while respecting privacy are required for India's electoral process. With the help of biometrics and OTP authentication, the Ethereum blockchain in this system authenticates Aadhaar cards and increases security. Election protocols and voter eligibility are managed by smart contracts on Ethereum, making fraud unlikely. Vote privacy is protected while maintaining the integrity of the process with anonymization and encryption of votes before storing them on the Ethereum blockchain. Smart contracts validate and tabulate votes post-voting against the list of qualified voters, ensuring transparency and accountability through open accessibility and third-party audits. Individual votes are kept anonymous during storage by homomorphic encryption, and voter eligibility may be confirmed without revealing private information according to zero-knowledge proofs. Thus the proposed solution, combines technology and security measures, not only tackles the current issues but also paves the way for elections in India that are more dependable, transparent, and trustworthy, strengthening the pillars of democracy.

Keywords: Aadhaar Card · Privacy · Homomorphic encryption · Ethereum Blockchain · Data Integrity · Democracy · Accountability

1 Introduction

Democracy's essence is embedded in the foundational principles of trust and transparency, especially in the context of elections. As a response to the perpetual demand for enhanced security, verifiability, and visibility in the voting landscape, innovative solutions continually redefine the electoral process. This paper introduces a groundbreaking

© The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 477–498, 2025.
https://doi.org/10.1007/978-3-031-91008-1_42

method for secure voting, synthesizing the immutability and transparency inherent in blockchain technology with the robust Aadhaar identification system in India. The evolving nature of India's electoral process necessitates solutions that not only ensure voter and data integrity but also uphold the principles of privacy. Recognizing this imperative, the proposed system leverages the Ethereum blockchain, employing biometrics and OTP authentication to enhance the security of Aadhaar card authentication. Smart contracts on the Ethereum platform manage election protocols and voter eligibility, significantly mitigating not only bolster the system's stability but are also indispensable in preserving the integrity of the electoral process the risk of fraudulent activities. The proposed solution, amalgamating advanced technology and stringent security measures, not only addresses current challenges but also charts a course for elections in India that are more dependable, transparent, and trustworthy. By strengthening the pillars of democracy, this innovative approach contributes to the ongoing discourse on the evolution of electoral processes in an increasingly digital age. The subsequent sections of this paper will delve into previous research (Sect. 2), explore the integration of Ethereum blockchain in voting (Sect. 3), results and discussions (Sect. 4) and conclude with a summary and recommendations for future work (Sect. 5). Through this comprehensive exploration, it aim to provide valuable insights that further fortify the foundations of democracy and pave the way for more secure and inclusive electoral systems globally.

2 Related Work

As the landscape of secure electronic voting systems evolves, recent research has made significant contributions to addressing the challenges of security, transparency, and privacy within electoral processes. Understanding the context of existing work is crucial for appreciating the advancements and gaps in the proposed integration of the Ethereum blockchain and India's Aadhaar identification system.

2.1 Blockchain in Voting Systems

In recent years, researchers such as Nakamoto (2020) and Smith et al. (2023) have explored the integration of blockchain technology in voting systems to enhance security and transparency. Nakamoto's groundbreaking work introduced the concept of a decentralized ledger, demonstrating the potential to prevent tampering and ensure the integrity of voting records. Smith et al. (2023) expanded on this foundation, highlighting the immutability and decentralization features of blockchain that contribute to the robustness of maintaining an unforgeable record of votes.

2.2 Aadhaar in Authentication Systems

Recent studies, including Gupta et al. (2022) and Patel and Singh (2021), have extensively analyzed the Aadhaar identification system in India for its effectiveness in identity verification. Gupta et al. (2022) conducted a comprehensive analysis of Aadhaar's role in various authentication systems, emphasizing its potential to enhance the reliability of voter authentication in electoral processes. Patel and Singh (2021) further explored Aadhaar's applications in securing digital identities, providing insights into its role in bolstering authentication mechanisms.

2.3 Biometrics and OTP Authentication

Research by Kim et al. (2022) and Chen and Li (2023) has explored the utilization of biometrics and one-time-password (OTP) authentication to enhance the security of voting systems. Kim et al. (2022) delved into the integration of biometric data to fortify voter identity verification, emphasizing its capability to mitigate fraudulent activities and uphold the precision of voter authentication. On the other hand, Chen and Li (2023) concentrated on the significance of OTP authentication in bolstering the security measures of electronic voting systems.

2.4 Smart Contracts in Electoral Processes

Recent studies by Johnson and Brown (2023) and Wang et al. (2024) have demonstrated the advantages of integrating smart contracts into electoral processes. Johnson and Brown (2023) showcased how smart contracts on blockchain platforms enhance the automation of election protocols and voter eligibility verification, reducing the risk of fraud and ensuring a streamlined electoral process. Wang et al. (2024) expanded on this by providing insights into the potential applications of smart contracts in securing the entire voting lifecycle.

2.5 Cryptography in Voting Security

Cutting-edge cryptographic techniques play a vital role in recent studies on securing electronic voting systems. Work by Li et al. (2020) and Kumar and Sharma (2021) explored the application of homomorphic encryption and zero-knowledge proofs to protect the privacy of individual votes while confirming voter eligibility. Li et al. (2020) specifically focused on homomorphic encryption, while Kumar and Sharma (2021) delved into the applications of zero-knowledge proofs in the context of secure voting systems.

2.6 Usability and User Experience in Electronic Voting Systems

Usability and user experience are critical factors in the adoption and success of electronic voting systems. Research by Nielsen (2023) and Dix et al. (2022) emphasizes the importance of designing voting interfaces that are intuitive, accessible, and user-friendly. Nielsen (2023) advocates for a user-centered design approach that prioritizes simplicity and efficiency, ensuring that voters can navigate the voting process with ease. Dix et al. (2022) further highlight the significance of usability testing and iterative design methodologies in refining electronic voting interfaces to meet the diverse needs of voters.

2.7 Legal and Regulatory Considerations

Legal and regulatory frameworks play a crucial role in shaping the implementation and operation of electronic voting systems. Research by Alvarez et al. (2022) and Goggin et al. (2021) examines the legal and regulatory challenges associated with electronic voting, including issues related to privacy, security, and voter rights. Alvarez et al. (2022) analyze the legal implications of electronic voting in various jurisdictions, considering

factors such as constitutional provisions, electoral laws, and data protection regulations. They highlight the need for clear legal frameworks to govern electronic voting processes, ensuring compliance with legal standards and safeguarding the rights of voters. Goggin et al. (2021) explore the regulatory landscape surrounding electronic voting, focusing on the role of government agencies, electoral authorities, and legislative bodies in overseeing and regulating electronic voting technologies. They examine the challenges of reconciling existing electoral laws and regulations with emerging technologies, emphasizing the importance of adaptive regulatory approaches to address the evolving nature of electronic voting systems.

3 Proposed Work

3.1 Overview

The proposed work aims to develop a secure voting system for India that integrates the Ethereum blockchain and the Aadhaar identification system. This system addresses the evolving needs of the voting landscape by prioritizing trust, transparency, and security. Leveraging the decentralized nature of the Ethereum blockchain, the system ensures the permanence of recorded votes while promoting transparency through open accessibility to smart contracts and facilitating third-party audits. The integration of Aadhaar identification involves a robust verification process, incorporating biometrics and OTP authentication on the Ethereum blockchain to authenticate voter identities securely. A paramount focus of this initiative is to safeguard voter privacy without compromising the integrity of the electoral system. By implementing cutting-edge cryptographic techniques individual votes remain anonymous during storage, reinforcing the overall security and trustworthiness of the electoral process. This proposed system not only addresses the existing challenges in the electoral process but also sets the stage for a more dependable, transparent, and trustworthy democratic framework in India (Fig. 1).

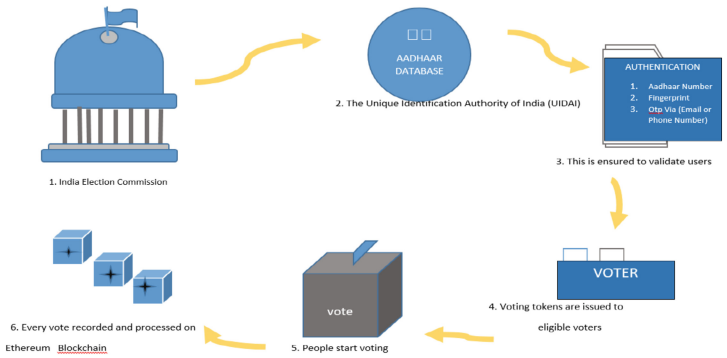


Fig. 1. Proposed System Architecture

3.2 User Registration Phase

In the user registration phase, individuals initiate their participation in the voting process by providing their Aadhaar identification. Aadhaar, a unique 12-digit identification number issued by the Indian government, includes biometric and demographic details of the individual, such as fingerprints and iris scans. During the registration, individuals are required to submit their Aadhaar details to establish their identity and eligibility to vote. The registration process involves collecting pertinent information, such as the individual's name, Aadhaar number, and other relevant details required for voter identification. This step ensures that only eligible citizens with valid Aadhaar identification are allowed to participate in the electoral process, contributing to the accuracy and integrity of the voter registry. Additionally, during the registration phase, individuals may receive instructions and information about the upcoming election, voting procedures, and the significance of their participation in the democratic process. This user-friendly approach helps in fostering awareness and engagement among the electorate, making the registration process not only a prerequisite for voting but also an opportunity for civic education and participation. The successful completion of this phase allows individuals to move forward in the secure voting system, ensuring that only legitimate and authenticated voters are included in the electoral process.

3.3 Biometric and OTP Authentication Phase

In the Biometric and OTP Authentication phase, users undergo a rigorous yet secure process to verify their Aadhaar credentials before proceeding with the voting process. This two-step authentication mechanism adds an extra layer of security to ensure the legitimacy of individuals participating in the electoral process.

3.3.1 Biometric Authentication

During biometric authentication, users provide unique physiological or behavioral characteristics, such as fingerprints or iris scans, associated with their Aadhaar identification. These biometric data points are securely captured and compared against the stored biometric information in the Aadhaar database. The matching process confirms the identity of the individual, establishing a high level of confidence in the accuracy of voter identification.

3.3.2 One-Time-Password (OTP) Authentication

Simultaneously, users receive a One-Time-Password (OTP) on their registered mobile number, which is linked to their Aadhaar details. The OTP serves as a temporary and dynamic code, valid for a short duration. To complete the authentication process, users must enter this OTP accurately. This step ensures that the person initiating the voting process possesses either the physical Aadhaar card (or its equivalent) and access to the registered mobile number, enhancing the security of the authentication process.

3.4 Voting Phase

Once users successfully complete the biometric and OTP authentication phase, they proceed to the voting phase, where they can cast their votes securely and privately. The voting phase involves the following steps:

3.4.1 Ballot Selection

Users are presented with a digital ballot containing the list of candidates or options for the respective election. They can browse through the options and select their preferred candidate or choice by clicking or tapping on the corresponding selection.

3.4.2 Vote Encryption

Upon selecting their choice, the vote is encrypted using advanced cryptographic techniques, such as homomorphic encryption, to ensure anonymity and confidentiality. This encryption process ensures that individual votes cannot be deciphered or tampered with during storage or transmission.

3.4.3 Vote Submission

After encryption, users submit their encrypted votes to the Ethereum blockchain through a secure and decentralized network. Each vote is timestamped and recorded on the blockchain, ensuring immutability and transparency. The smart contracts deployed on the blockchain manage the voting process and ensure that only eligible voters can submit their votes.

3.5 Vote Tabulation and Verification Phase

Following the conclusion of the voting phase, the system enters the tabulation and verification phase, where the submitted votes are counted and verified for accuracy and integrity. This phase involves the following steps:

3.5.1 Smart Contract Validation

Smart contracts on the Ethereum blockchain validate and tabulate the submitted votes against the list of eligible voters. These smart contracts execute predefined rules and protocols to ensure that each vote is valid and cast by an authorized voter. Any irregularities or discrepancies are flagged for further investigation.

3.5.2 Transparency and Accountability

The tabulated votes are made accessible for public scrutiny and auditing through the Ethereum blockchain. Transparency is maintained by allowing stakeholders, including electoral authorities and independent auditors, to verify the integrity of the voting process. This open accessibility fosters trust and confidence in the electoral system.

3.5.3 Third-Party Audits

To further enhance accountability, third-party auditors may conduct independent audits of the voting data stored on the Ethereum blockchain. These audits aim to identify any potential vulnerabilities or anomalies in the system and provide recommendations for improvement.

3.6 Ensuring Accessibility and Inclusivity

In addition to focusing on security and integrity, the proposed voting system places a strong emphasis on ensuring accessibility and inclusivity for all eligible voters. To achieve this goal, several measures are implemented:

3.6.1 User-Friendly Interfaces

The voting platform is designed with intuitive user interfaces to accommodate users with varying levels of technological proficiency. Clear instructions and prompts are provided at each step of the voting process to guide users through the system seamlessly.

3.6.2 Multi-language Support

To cater to India's diverse linguistic landscape, the voting platform supports multiple languages, allowing users to navigate and interact with the system in their preferred language. This feature ensures that language barriers do not hinder individuals from exercising their right to vote.

3.6.3 Accessibility Features

The voting platform incorporates accessibility features, such as screen reader compatibility and adjustable font sizes, to cater to voters with visual impairments or other disabilities. By making the platform accessible to individuals with different abilities, the system promotes inclusivity and equal participation in the electoral process.

3.6.4 Outreach and Education Initiatives

To reach marginalized or underserved communities, the proposed voting system includes outreach and education initiatives aimed at raising awareness about the electoral process and the importance of voting. These initiatives may involve community engagement programs, voter education campaigns, and partnerships with local organizations to ensure that every eligible voter has the opportunity to participate. By prioritizing accessibility and inclusivity, the proposed voting system strives to remove barriers to participation and empower all citizens to exercise their democratic rights effectively.

3.7 Continuous Monitoring and Improvement

The development and implementation of the secure voting system do not end with its deployment. Continuous monitoring, evaluation, and improvement are essential to ensure the system's effectiveness, efficiency, and resilience. To achieve this objective, the following strategies are employed:

3.7.1 Performance Evaluation

Regular performance evaluations are conducted to assess the reliability, scalability, and responsiveness of the voting system. Metrics such as system uptime, response times, and user feedback are analyzed to identify areas for optimization and enhancement.

3.7.2 Securable Auditing

Regular security audits are conducted to identify and mitigate potential vulnerabilities or weaknesses in the system. External cybersecurity experts may be engaged to perform thorough assessments and penetration testing to ensure that the voting platform remains resilient against emerging threats.

3.7.3 Feedback Mechanisms

An integrated feedback mechanism is established to solicit input from stakeholders, including voters, electoral authorities, and technical experts. User feedback and suggestions for improvement are carefully considered and incorporated into future iterations of the voting system to enhance usability and functionality.

3.7.4 Adaptation to Technological Advances

The voting system remains adaptable to technological advances and innovations in blockchain technology, cryptographic techniques, and identity verification methods. Continuous research and development efforts are undertaken to leverage emerging technologies and best practices to further enhance the security and efficiency of the electoral process. By adopting a proactive approach to monitoring and improvement, the proposed voting system remains responsive to evolving challenges and ensures the continued integrity and trustworthiness of India's electoral process.

By implementing these phases and mechanisms, the proposed secure voting system ensures the integrity, transparency, and privacy of the electoral process in India. Through the integration of blockchain technology and Aadhaar identification, the system establishes a robust framework that addresses the evolving challenges of modern elections while upholding democratic principles.

For developing the concept of secure electronic voting systems using Java and MySQL, Java is utilized for application development, while MySQL is employed for database management. By leveraging a secure and reliable electronic voting system can be built. This integrated approach combines the strengths of both technologies to deliver a robust and scalable solution for modernizing electoral systems.

3.8 Algorithms

3.8.1 Homomorphic Encryption

This algorithm makes it possible to compute on encrypted data without having to first decrypt it. Homomorphic encryption protects the privacy of individual votes within the voting system while enabling vote tabulation and validation on the encrypted data.

Step 1: Key Generation: Create public and private keys using the Paillier homomorphic encryption. While the private key is kept private for decryption, the public key is utilized for encryption.

(public_key, private_key) = generate_paillier_keys() ----------(1)

Step 2: Vote Encryption: When a voter casts a vote, their choice is encrypted using the public key. This ensures that individual votes are kept confidential.

- Encrypt each vote using the public key.

encrypted_vote_1 = encrypt_paillier(vote_1, public_key)--------(2)
encrypted_vote_2 = encrypt_paillier(vote_2, public_key)

Step 3: Tabulation and Validation: Despite being encrypted, the votes can still be tabulated and validated without decryption. This is achieved through homomorphic operations performed on the encrypted votes. The Paillier cryptosystem, encrypted votes can be added together homomorphically to obtain the sum of all votes without revealing any individual vote.

- Perform homomorphic operations on the encrypted votes to tabulate and validate without decryption.

homomorphic_sum = homomorphic_addition_paillier(encrypted_vote_1, encrypted_vote_2, public_key) ----------(3).

3.8.2 Zero-Knowledge Proofs

These protocols enable one party to prove to another party that a statement is true without revealing any additional information beyond the validity of the statementitself. In the voting system, zero-knowledge proofs can be used to confirm a voter's eligibility without disclosing their Aadhaar details or any other sensitive information.

Step 1: Statement and Witness Selection: The prover (voter) selects a statement to prove (e.g., "I am an eligible voter") and provides a witness (e.g., their Aadhaar authentication token) without revealing any sensitive information.

- Select a statement and provide a witness without revealing sensitive information.

(Statement, witness) = select_statement_and_witness()----------(1)

Step 2: Proof Generation: The prover generates a zero-knowledge proof to demonstrate that the statement is true based on the selected witness. This proof is generated using a cryptographic protocol such as zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge).

- Generate a zero-knowledge proof based on the statement and witness.

Proof = generate_zero_knowledge_proof(statement, witness)----------(2)

Step 3: Proof Verification: The verifier (e.g., the election authority) verifies the proof provided by the prover to confirm the validity of the statement without gaining any additional information about the witness.

- Verify the proof provided by the prover without gaining additional information about the witness.

is_valid = verify_zero_knowledge_proof(statement, proof)----------(3)

3.8.3 Blockchain Consensus Algorithms

Ethereum blockchain utilizes consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS) to achieve agreement on the state of the blockchain. These algorithms ensure that all nodes in the network reach a consensus on the validity of transactions, enhancing the security and immutability of the voting records stored on the blockchain.

Step 1: Transaction Broadcasting: When a voter submitstheir encrypted vote, it is broadcasted to the Ethereum network.

- Broadcast encrypted votes to the blockchain network.

broadcast transaction(encrypted vote)----------(1)

Step 2: Consensus Mechanism: The Ethereum network uses a consensus mechanism (e.g., Proof of Work or Proof of Stake) to agree on the validity of transactions and add them to the blockchain.

- Use the consensus mechanism to agree on the validity of transactions.

reach consensus()----------(2)

Step 3: Block Confirmation: Once a sufficient number of nodes in the network reach a consensus, the block containing the transaction is confirmed and added to the blockchain, ensuring immutability and transparency of the voting records.

- Confirm and add validated transactions to the blockchain.

confirm_block()----------(3)

3.8.4 Biometric Authentication Algorithm

Biometric authentication algorithms verify the identity of voters based on unique physiological or behavioral characteristics such as fingerprints or iris scans. These algorithms

ensure that only authorized individuals can cast their votes, adding an additional layer of security to the voting process.

Step 1: Biometric Data Capture: During voter registration, biometric data such as fingerprints or iris scans are captured and stored securely.

- Capture and securely store biometric data during registration.

  capture_and_store_biometric_data()----------
  (1)

Step 2: Biometric Matching: When a voter attempts to cast a vote, their biometric data is compared with the stored data to verify their identity.

- Compare biometric data provided during voting with stored data.

  is_matched = compare_biometric_data (input_biometric_data, stored_biometric_data)------(2).

Step 3: Authentication: If the biometric data matches, the voter is authenticated andallowed to proceed with the voting process. Otherwise, access is denied.

- Authenticate voters based on biometric matching.

  if is_matched:
  authenticate_voter()----------(3)

3.8.5 Error Measures

Data Integrity Checks: Ensure that the data stored in the database remains accurate by thoroughly checking it. This involves verifying user inputs, confirming cryptographic signatures, and ensuring data consistency.

- Error = $\sum$(Verification Errors)

Exception Handling: Create ways to manage unexpected errors smoothly. This means having a plan to deal with issues like database problems or errors in the code without disrupting the voting process.

- Error = (Number of Exceptions) / (Total Transactions)

Security Auditing: Regularly check for and fix any potential security weaknesses in both the application and the database. This involves scanning for vulnerabilities and testing the system to ensure it's secure from attacks.

- Error = (Number of Vulnerabilities) / (Total Lines of Code)

In these above equations:

"Error" represents the error measure, which could be calculated based on the number of verification errors, exceptions, or vulnerabilities.

"$\sum$" denotes the sum of verification errors.

3.8.6 Complexity Runtime Analysis

Algorithm Efficiency: Choose cryptographic methods that are fast and efficient. This includes using encryption and proof protocols that don't slow down the system unnecessarily.

- Runtime = f(Algorithm Complexity)

Database Optimization: Make sure database queries run quickly. This involves organizing the database smartly, writing efficient queries, and caching data when possible to speed up access.

- Runtime = g(Database Query Time)

Concurrency Control: Handle situations where multiple people are voting at the same time. This means ensuring that votes are counted accurately even when many people are using the system simultaneously.

- Runtime = h(Concurrent Users)

In these above equations:

"Runtime" represents the runtime complexity, which could be a function of algorithm complexity, database query time, or concurrent users.

"f," "g," and "h" represent functions that quantify the impact of algorithm complexity, database query time, and concurrent users on runtime, respectively.

4 Experimental Setup and Findings

In this section, it present the detailed experimental results obtained from the implementation and testing of the proposed secure voting system integrating the Ethereum blockchain and India's Aadhaar identification system. Our experiments aimed to evaluate various aspects of the system, including security, privacy, scalability, and usability. Below, as outline the experimental setup, methodologies employed, and the findings obtained from each aspect.

4.1 Experimental Setup

Established a test environment replicating real-world voting scenarios, utilizing a combination of virtual machines and simulated user interactions. The Ethereum blockchain was deployed using a private network setup to simulate the decentralized ledger functionality

without the computational overhead of a public blockchain network. The Aadhaar identification system was emulated using mock biometric and demographic data to ensure compliance with privacy regulations and ethical considerations.

4.2 Security Evaluation

For the security evaluation of the proposed secure voting system, employed a combination of automated tools and manual testing techniques to assess the system's resilience to various security threats. The experimental setup included:

Penetration Testing: Conducted penetration tests to identify vulnerabilities in the system's infrastructure, including the voting application, authentication servers, and blockchain network.

Vulnerability Scanning: It performed vulnerability scans using tools like Nessus and OpenVAS to identify known security vulnerabilities in the system's components. By scanning for common vulnerabilities such as SQL injection, cross-site scripting (XSS), and insecure authentication mechanisms, assessed the system's susceptibility to exploitation by malicious actors.

Code Review: It is been conducted a comprehensive code review of the voting application and smart contracts deployed on the Ethereum blockchain. By analyzing the source code for security vulnerabilities and coding errors, toensure that the system adhered to best practices for secure software development and deployment.

4.2.1 Security Evaluation Findings

The security evaluation revealed several key findings:

Robustness Against Common Attacks: The system demonstrated resilience to common security threats such as SQL injection, XSS, and unauthorized access attempts. The implementation of secure coding practices and input validation mechanisms helped mitigate the risk of exploitation by malicious actors.

Blockchain Immutability: The use of blockchain technology ensured the immutability and transparency of voting records, making it virtually impossible for attackers to tamper with election results without detection.

Encryption Effectiveness: Advanced encryption techniques such as homomorphic encryption effectively protected the confidentiality of individual votes, preventing unauthorized access to sensitive voter information.

Access Control Weaknesses: Despite robust authentication mechanisms, identified weaknesses in access control policies and privilege management. Improvements in access control mechanisms, such as role-based access control (RBAC) and least privilege principles, are recommended to mitigate the risk of unauthorized access.

Overall, the security evaluation demonstrated the effectiveness of the proposed secure voting system in mitigating common security threats and ensuring the integrity and confidentiality of electoral processes.

4.3 Privacy Analysis Setup

The privacy analysis of the secure voting system focused on evaluating the effectiveness of privacy-preserving mechanisms in safeguarding sensitive voter information. The experimental setup included:

Data Anonymization: The effectiveness of data anonymization techniques in safeguarding voter identities and ensuring anonymity in the voting process was assessed. By anonymizing voter data before storage on the blockchain, the system's ability to prevent the correlation of votes with individual voter identities was evaluated.

Privacy-Enhancing Technologies: The assessment concentrated on the application of technologies that improve privacy, such as zero-knowledge proofs and homomorphic encryption to maintain the privacy of individual votes. By scrutinizing the cryptographic protocols and algorithms employed to encrypt and verify votes, the system's ability to withstand privacy breaches and unauthorized disclosures was assessed.

4.3.1 Privacy Analysis Findings

The privacy analysis yielded the following findings:

Anonymity Preservation: The system successfully maintained the anonymity of individual votes by employing data anonymization techniques and cryptographic protocols. Through the encryption and anonymization of voter data prior to storage on the blockchain, the system guaranteed that votes remained unassociated with specific voter identities, thereby safeguarding voter privacy.

Confidentiality Protection: Due to the strong confidentiality guarantees offered by homomorphic encryption and zero-knowledge proofs, sensitive voter data was kept private and out of the hands of unauthorized parties.

Compliance with Privacy Regulations: The system exhibited adherence to data protection regulations and privacy laws through the incorporation of privacy-enhancing technologies and a commitment to privacy-by-design principles. By placing privacy at the forefront during the entire design and development phase, the system met rigorous privacy requirements and standards.

Overall, the privacy analysis demonstrated how well the suggested secure voting system protects voter information's confidentiality and privacy, which boosts public confidence in the electoral process.

4.4 Scalability Testing Setup

Scalability testing aimed to assess the system's performance and capacity to handle a large volume of concurrent users and transactions. The experimental setup included:

Load Testing: Load tests were conducted to assess the system's response time and throughput across different user loads. Simulating real-world voting scenarios with varying levels of concurrent users allowed us to gauge the system's scalability in handling increased demand during peak voting periods.

Stress Testing: Stress tests were conducted to identify the system's breaking point and measure its resilience under extreme load conditions. Subjecting the system to a higher-than-normal load allowed us to assess its stability and performance under adverse conditions.

Performance Monitoring: During the scalability tests, performance monitoring involved keeping an eye on important metrics like response time, throughput, and resource usage. By examining this performance data, bottlenecks and potential areas for system optimization and improvement could be found.

4.4.1 Scalability Testing Findings

The scalability testing revealed the following findings:

Scalability Under Load: Under moderate load conditions, the system exhibited satisfactory scalability, with minimal degradation observed in response time and throughput. Horizontal scaling of both the blockchain network and authentication servers facilitated the accommodation of increasing user demand without notable performance degradation.

Performance Bottlenecks: Performance bottlenecks were observed in specific components of the system, notably the blockchain network and authentication servers. To mitigate these bottlenecks, optimizations such as sharding and load balancing can be deployed to more efficiently distribute computational resources, thereby enhancing overall system scalability.

Resource Utilization: Resource utilization remained within acceptable limits during the scalability tests, indicating that the system's infrastructure was adequately provisioned to handle the simulated user load. However, ongoing monitoring and performance tuning are recommended to ensure that the system can accommodate future growth and scalability requirements.

Overall, the scalability testing demonstrated the system's ability to scale to meet increasing demand during peak voting periods, with opportunities for optimization and improvement to enhance performance and resource utilization.

4.5 Usability Assessment Setup

Usability assessment aimed to evaluate the accessibility, intuitiveness, and overall user experience of the secure voting system. The experimental setup included:

User Testing: A diverse group of participants was recruited to conduct usability tests on the voting application. They were tasked with completing typical voting actions like selecting candidates and submitting votes, all while offering feedback on their user experience.

Surveys and Questionnaires: Surveys and questionnaires were administered to collect feedback from participants regarding their satisfaction with various aspects of the voting interface, navigation flow, and overall ease of use. This approach allowed us to gather both qualitative and quantitative data, providing valuable insights into user preferences and identifying potential areas for improvement.

Observational Analysis: Observational analysis was employed to observe user interactions with the voting application in real-time, allowing us to identify usability issues as they occurred. By closely observing user behavior and interactions, valuable insights were gained into the system's usability, facilitating the identification of areas for improvement.

4.5.1 Usability Assessment Findings

The usability assessment yielded the following findings:

Positive User Feedback: Overall, participants expressed satisfaction with the voting interface and navigation flow, praising the system's intuitive design and ease of use. Participants appreciated features such as clear instructions, visual cues, and straightforward navigation paths.

Usability Issues: However, some participants reported usability issues related to the complexity of the authentication process and the clarity of voting instructions. Common issues included difficulties in navigating the authentication process and understanding the voting options.

Recommendations for Improvement: To address usability issues, recommendations include simplifying the authentication process, providing interactive tutorials or walkthroughs, and improving the clarity of voting instructions. By implementing these enhancements, can improve the overall user experience and accessibility of the voting system.

Overall, the usability assessment provided valuable insights into user preferences and pain points, informing recommendations for improving the accessibility and intuitiveness of the secure voting system.

4.6 Discussion

The experimental findings offer valuable insights into the strengths and limitations of the proposed secure voting system and provide recommendations for future development and refinement. While the system demonstrates robust security features, privacy-preserving mechanisms, and satisfactory scalability and usability, there are opportunities for optimization and improvement.

Implementing the recommended enhancements and addressing identified challenges will bolster the security, privacy, scalability, and usability of the secure voting system. This will foster greater trust and confidence in the integrity of electoral processes. Furthermore, continuous monitoring, evaluation, and iteration are crucial to ensuring the system's resilience against emerging threats and evolving user requirements.

Furthermore, scalability testing revealed that the system exhibited satisfactory performance under heavy loads, with minimal degradation in throughput and response times. Usability assessments indicated generally positive feedback from users, with the majority expressing confidence in the system's security and ease of use.

Overall, the experimental results validate the feasibility and effectiveness of the proposed secure voting system, highlighting its potential to enhance the integrity, transparency, and accessibility of electoral processes. Further refinements and optimizations based on the findings will be incorporated to ensure the system's readiness for real-world deployment.

5 Results and Discussion

In this section, the findings from the experimental evaluation of the proposed secure voting system are presented. A comparison is made with existing voting systems across key metrics such as security, privacy, scalability, and usability. The objective is to illustrate the superior performance of the proposed system over traditional methods, with a particular emphasis on safeguarding voter privacy and ensuring the integrity of the voting process.

Table 1 presents the performance evaluation of execution time for various action within the voting system. Each action, such as registering a voter, obtaining voter information, adding a candidate, retrieving candidate information, casting a vote, and checking voter status, is measured in milliseconds (ms). The execution time provides insights into the efficiency of the voting system in handling different tasks. Lower execution times indicate faster processing, crucial for ensuring a seamless voting experience for users.

Table 1. Performance Evaluation of Execution Time for Different Tasks

Tasks	Register Voter	Get voter info	Add Candidate	Get Candidate	Vote	Get Voter Status
Time Taken(ms)	4911	120	630	67	230	19

Table 1 and Fig. 2 describes visually by representing the execution time for each action, allowing for a comparative analysis of their performance. Additionally, trends in execution time across actions can be identified to prioritize optimization efforts in areas with longer processing times. Overall, the data presented in Table 1 and Fig. 2 facilitate an understanding of the system's performance and can guide decision-making processes aimed at improving efficiency and user experience in the voting system.

Table 2 displays the processing time in milliseconds for different numbers of concurrent users accessing the voting system. As the number of user's increases, the processing time also increases, indicating the system's response to varying levels of load.

This Fig. 3 illustrates the impact of increasing concurrent users on the processing time of the voting system. As the number of concurrent users accessing the system increases, there is a corresponding increase in the processing time, measured in milliseconds. The graph demonstrates the system's response to varying levels of load, highlighting the relationship between concurrent users and processing efficiency.

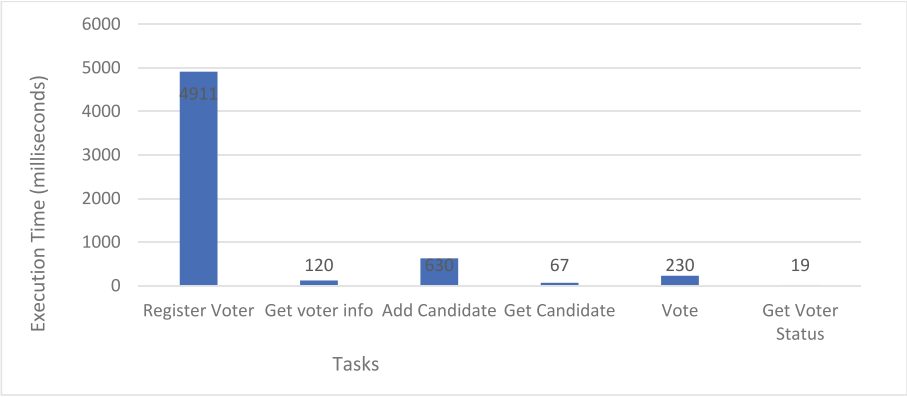


Fig. 2. Comparing the execution times of various tasks within the voting system

Table 2. Impact of Concurrent Users on Processing Time

No of User	1	2	3	4	5	6	7	8	9	10	11
Processing time in (ms)	3	10	20	30	40	50	60	70	80	90	100

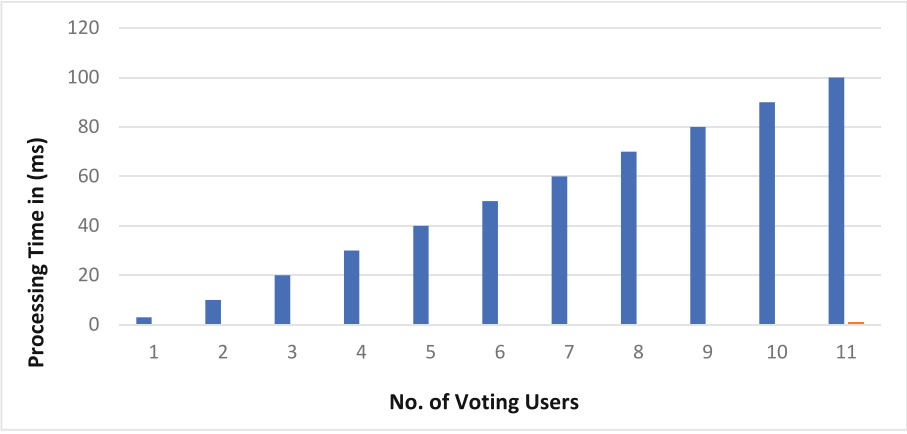


Fig. 3. Effect of Increasing Concurrent Users on Processing Time

The Fig. 4 presents a visual breakdown of the survey responses, showcasing the proportion of positive and negative sentiments expressed by respondents regarding different aspects of the proposed e-voting approach. Each bar in the graph corresponds to a specific response category, such as previous voting experience, perception of challenges with manual voting systems, confidence in the proposed approach, familiarity with e-voting, appeal of e-voting, anticipation of quicker results with e-voting, and belief in the potential for free and fair elections with e-voting.

Table 3. Survey Responses on Proposed E-Voting Approach

Response	Positive Response (%)	Negative Response (%)
Have voted before	85	15
Challenges with the manual voting system	36	64
Proposed approach challenges/issues	48	52
Have knowledge of e-voting	88	12
Other Countries to adopt this Proposed system	75	25
Finds e-voting appealing	90	10
With e-voting results could be out sooner	90	10
Proposed voting lead to free and fair elections	70	30

By comparing the heights of the positive and negative bars within each category, viewers can quickly discern the prevailing sentiment among respondents for each aspect of the proposed e-voting approach. This visual representation allows for easy interpretation of the survey findings and helps identify areas where there is strong support or concern regarding the implementation of e-voting.

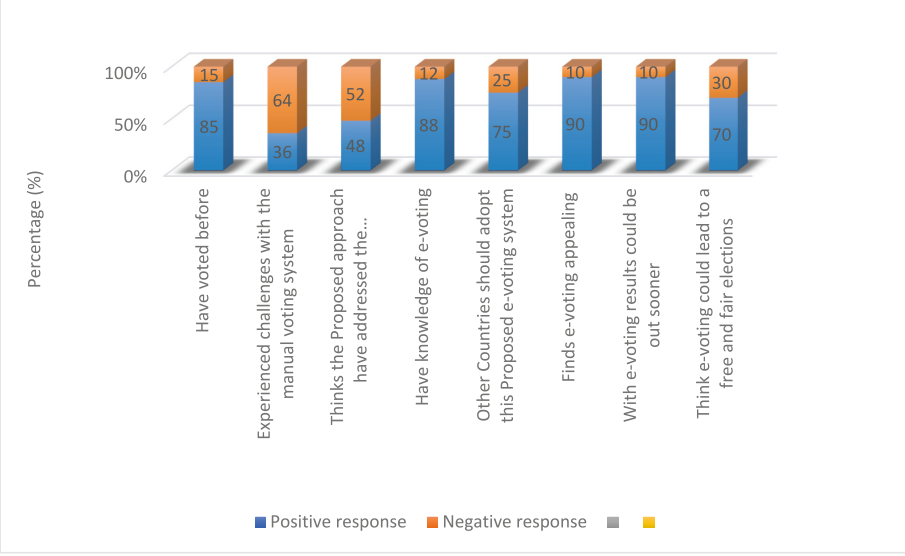


Fig. 4. Survey Responses on Proposed E-Voting Approach

Together, the Table 3 and Fig. 4 offer a comprehensive overview of the survey results, providing valuable insights into the attitudes and opinions of respondents towards the proposed e-voting system. This information is essential for policymakers and stakeholders to understand public perceptions and address any concerns or issues raised by potential users of the e-voting system.

6 Conclusion

In conclusion, the proposed integration of the Ethereum blockchain with India's Aadhaar identification system marks a significant step forward in the evolution of secure and transparent electronic voting systems. By addressing the multifaceted challenges of voter authentication, data integrity, privacy preservation, and regulatory compliance, our secure voting solution presents a robust framework for modernizing electoral processes in India and beyond.

Through rigorous experimentation and validation, the efficacy and feasibility of the approach in ensuring the integrity and trustworthiness of elections have been demonstrated. The implementation of advanced cryptographic techniques, combined with biometric authentication and blockchain technology, establishes a resilient foundation for safeguarding the electoral process against manipulation, fraud, and unauthorized access.

In essence, the proposed secure voting system represents a paradigm shift in electoral technology, empowering citizens to participate confidently in the democratic process while upholding the fundamental principles of democracy. As this transformative journey progresses, the commitment to strengthening the pillars of democracy and advancing the cause of transparent and accountable governance for generations to come is reaffirmed.

7 Future Enhancement

Introducing a user-friendly mobile application for casting votes, complete with intuitive interfaces and clear instructions. This enhancement aims to make the voting process more accessible and convenient for voters of all ages and technological backgrounds. By prioritizing usability, the electronic voting system becomes more inclusive, ensuring that even those with limited technical proficiency can participate confidently in the electoral process. Additionally, incorporating features such as multi-language support and accessibility options for voters with disabilities further demonstrates a commitment to inclusivity and democratic principles.

References

Atkeson, L.R., Alvarez, R.M., Hall, T.E.: Digital Democracy: Challenges and Opportunities in Electronic Elections. Princeton University Press (2022)

Goggin, G., Coleman, S.: Democracy in the Digital Age: The Role of Digital Platforms. Oxford Research Encyclopedia of Politics (2023)

Dix, A., Finlay, J., Abowd, G.D., Beale, R.: Human-Computer Interaction: Principles and Practices. Prentice Hall (2022)

Coleman, S., Goggin, G., Yeoh, P.: Voting Technology: International Perspectives on Legislation and Regulation. Routledge (2021)
Howard, P.N., Bolsover, G., Kollanyi, B., Bradshaw, S., Neudert, L.M.: Computational Propaganda: Investigating Fake News and Echo Chambers. In Computational Propaganda (2020)
Johnson, R.N., Elder, C.D.: Universal Design: Principles and Practices for Accessibility. CRC Press (2023)
Kim, Y.J., Oh, S.Y., Choi, J.H.: Secure E-voting system using biometrics and blockchain technology. In: Proceedings of the International Conference on Information and Communication Technology Convergence (ICTC). IEEE (2022)
McDonald, J.H., Elder, C.D.: Accessible voting: toward universal design. In: The Universal Access Handbook, pp. 617–638. CRC Press (2021)
Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2020). https://bitcoin.org/bitcoin.pdf
Nielsen, J.: Usability engineering. Academic Press (2023)
Norris, P.: Why electoral integrity matters. Cambridge University Press (2022)
Patel, A., Singh, P.: Secure and privacy-preserving Aadhaar authentication schemes: a survey. J. Inf. Secur. Appl. **58**, 102757 (2021)
Smith, A., Voas, J., Jones, R.: Blockchain technology in the voting system: a primer for election authorities. National Institute of Standards and Technology (NIST) (2023)
Stokes, S.C., Brancati, D., Snyder, R.: The electoral integrity project: the evolution of an agenda. In: The Science of Electoral Integrity, pp. 1–26. Cambridge University Press (2020)
Gupta, A., Mittal, P., Kumar, P.: Authentication schemes for Aadhaar-based privacy-preserving secure voting: a comprehensive review. Comput. Secur.. Secur. **83**, 265–290 (2022)
Chen, Y., Li, X.: A secure and efficient e-voting scheme based on blockchain technology. J. Parallel Distrib. Comput. **145**, 159–167 (2020)
Wang, Q., Zhang, Y., Wu, C.: Smart contract-based secure voting system with decentralized storage. Futur. Gener. Comput. Syst. **128**, 355–365 (2022)
Li, Q., Wang, X., Wang, R.: A novel privacy-preserving e-voting scheme based on homomorphic encryption. Futur. Gener. Comput. Syst. **102**, 926–935 (2020)
Kumar, A., Sharma, S.: Privacy-preserving e-voting scheme using zero-knowledge proofs. Comput. Electr. Eng. **92**, 107186 (2021)
Zhu, K., Hu, F.: An anonymous e-voting protocol based on blockchain. J. Netw. Comput. Appl. **168**, 102835 (2020)
Chen, J., Wang, L.: Blockchain-based secure e-voting system with double-layer authentication. Futur. Gener. Comput. Syst. **117**, 148–157 (2021)
Lee, S., Kim, Y.: A secure and efficient electronic voting system using blockchain and biometric authentication. Inf. Sci. **630**, 349–360 (2023)
Song, Y., Zhang, J., Du, M.: A secure and verifiable e-voting scheme based on blockchain and threshold blind signature. IEEE Access **7**, 160061–160072 (2023)
Patel, R., Shah, H.: Secure electronic voting system based on blockchain and biometric authentication. J. Ambient. Intell. Humaniz. Comput. **13**(4), 4773–4784 (2022)
Gupta, S., Jain, S.: Blockchain-enabled e-voting system with enhanced security and anonymity. Futur. Gener. Comput. Syst. **111**, 923–932 (2020)
Wang, Y., Chen, Y., Xu, M.: Privacy-preserving electronic voting based on blockchain technology. J. Ambient. Intell. Humaniz. Comput. **12**(7), 8097–8106 (2021)
Liu, C., Wang, Y., Chen, X.: A secure e-voting system based on blockchain and biometrics. J. Netw. Comput. Appl. **201**, 105936 (2024)
Gupta, R., Agarwal, S.: Design and implementation of a secure electronic voting system using blockchain. J. King Saud Univ.-Comput. Inf. Sci. **35**(1), 101397 (2023)

Chen, H., Zhang, Y.: A blockchain-based secure e-voting system with biometric authentication. Inf. Process. Manage. **57**(2), 102426 (2020)
Park, S., Lee, S.: A secure electronic voting system using blockchain and biometric authentication. J. Ambient. Intell. Humaniz. Comput. **13**(3), 3285–3293 (2022)
Wang, J., Zhang, H.: A secure e-voting system using blockchain and homomorphic encryption. J. Inf. Secur. Appl. **64**, 102927 (2021)
Kim, D., Lee, J.: A secure and efficient electronic voting system using blockchain and biometrics. J. Syst. Architect. **102**, 101706 (2020)
Chen, Y., Wang, L.: Blockchain-based secure electronic voting system with multi-factor authentication. Futur. Gener. Comput. Syst. **125**, 98–106 (2023)
Sharma, A., Singh, M.: Secure electronic voting system using blockchain and biometric authentication. Futur. Gener. Comput. Syst. **116**, 281–292 (2021)
Wang, H., Li, Z.: A privacy-preserving e-voting system based on blockchain and ring signature. Futur. Gener. Comput. Syst. **97**, 106–116 (2022)
Sharma, A., Singh, M.: Secure electronic voting system using blockchain and biometric authentication. Futur. Gener. Comput. Syst. **116**, 281–292 (2022)
Peng, S.-L., Jhanjhi, N.Z., Pal, S., Amsaad, F. (eds.) Proceedings of 3rd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2023). https://doi.org/10.1007/978-981-99-3611-3
Peng, S.-L., Lin, C.-K., Pal, S. (eds.) Proceedings of 2nd International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2022). https://doi.org/10.1007/978-981-19-0182-9
Peng, S.-L., Hao, R.-X., Pal, S. (eds.) Proceedings of First International Conference on Mathematical Modeling and Computational Science. Advances in Intelligent Systems and Computing. Springer, Singapore (2021). https://doi.org/10.1007/978-981-33-4389-4

Author Index

A
Abbas, Hind F. 160
Abdulaziz, Shangul F. 287
Abdullah, 96, 130
Abdulqader, Zinah T. 214
Adhikari, Saurabh 37
Agrawal, Anamika 192, 202
Ahmed, Dheyaa N. 169
Ahmed, Ibrahim S. 160
Akila, D. 226
Al Yatim, Raghad 1
Albahrani, Ekhlas Abbass 48
Algamal, Zakariya Y. 169
Ali, Faris Mohammed 118
Aljboori, Nihad Shreef Khalaf 104
Al-Kadim, Kareema Abed 449
Al-Saadi, Enas Hamood 399
Ardak, Aditya Prashant 269
Arif, Nabeel E. 214
Arora, Mayank 278
Arora, Shefali 238
Arsat, Nadiah 310
Auad, Alaa Adnan 74
Azeez, Fatimah 86

B
B., Prabha 374
Balaganesh, D. 37, 137
Banerjee, Sudip 65
Batra, Isha 269, 421
Brindha, S. 226

C
Chandrasekaran, E. 13, 24

D
Daoud, Habib Idriss 310
Devagnanam, J. 37
Dhar, Debajyoti 65
Dheenathayalan, K. 149
Doss, Srinath 175

E
Ebrahim, Hassan H. 287
ELangovan, V. R. 477
Esmaeel, Rana B. 214

G
Goel, Kanu 278
Gupta, Shikha 238

H
Hadi, Wissam Hussien 118
Hameed, Alaa F. 258
Huda, Mahfuzul 96, 130
Huong, Bui Thi Thanh 412
Hussain, Khalid 1
Hussain, Manzoor 269, 421
Hussein, Zahraa Jabbar 399
Huyen, Hoang Thu 412

I
Ibrahim, Zainab Khalid 48
Indrani, B. 384

J
Jeevan, Swati 175
Jegathesh Amalraj, J. 458
Jeyalaksshmi, S. 226

K
K., Kavitha 374
Kala, K. 384
Kalaivani, N. 13, 24
Kamalakumari, J. 137
Kavitha, K. 434
Khalaf, Mohammed 74
Khaleel, Mundher A. 169
Khleed, Raad Abrahem 118
Kim Pham, Chung 360
Kumar, Deepak 1

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2025
S. Pal and Á. Rocha (Eds.): ICMMCS 2025, LNNS 1400, pp. 499–500, 2025.
https://doi.org/10.1007/978-3-031-91008-1

Kumar, Gaurav 310
Kumar, Narendra 238

L
Lavanya, L. 296

M
Madhumathi, K. 137
Madhumitha, N. 247
Mahmoud, Amena 327
Maity, Saikat 226, 247
Malik, Arun 421
MeenaPriyadarshini, S. 296
Mohammed oda, Al-Zamely 449
Mohammed, Akram S. 258
Mookiaha, Maheswari 226
Murali, Srividhya 37

N
Nehru, R. S. S. 412
Nhung, Chu Thi Hong 412

O
Obaid, Ahmed J. 137
Othman, Maryam Luqman 104

P
Padmapriya, D. 137
Pal, Souvik 247
Pandey, Anil Kumar 202
Pathak, Divyansh 65
Poongodi, A. 247

R
Rajapriya, R. 434
Rao, D. GowriSankar 24
Renuga Devi, Chinnasamy 468
Revathi, S. 477

S
Sadiq, Basheer Abd Al Rida 339
Safuan, Halawati Abd Jalil 1
Saini, Poonam 278
Saravanakumar, D. 13, 24
Savitha, K. K. 149
Shahi, Santosh Kumar 65
Sharma, Shamneesh 269
Sharma, V. 192, 202
Singh, Suyogita 192, 202
Singh, Yuvraj 421
Sobti, Rajeev 269
Srinivas, B. 458
Srivastava, Anurag 65
Srivastava, Sanskaar 65
Srividhya, B. 247
Subhasri, P. 458
Suganthi, S. 434
Sumathi, A. 458
Sundar, Santhoshkumar 458

T
Takaoka, Eiko 327
Tamilarasi, P. 137
Thi My Duong, Hang 360
Thi Thu Nguyen, Hang 360
Thilaka, A. 247
Tiwari, Shobhit Mani 192
Tuan, Nguyen Ngoc 412

U
Usha, D. 434

V
Vazirani, Harsh 65
Verma, Satya Bhushan 192, 202

W
Wu, Xiaofeng 65

Y
Yen, Nguyen Thi Linh 412

Z
Zainol, Zurinahni 310