2025 Tenth International Conference on Science Technology Engineering and Mathematics (ICONSTEM) | 979-8-3315-6187-1/25/$31.00 ©2025 IEEE | DOI: 10.1109/ICONSTEM65670.2025.11374838

Adaptive Phishing Threat Identification and Classification Using Hybrid ML Techniques in Cyberspace

G.Suvetha, T.Jaya*, V.Rajendran

Assistant Professor, Department Of ECE, Vels Institute of Science, Technology Advanced Studies (VISTAS), Chennai, Tamilnadu, India.

Email id: gsuvetha.se@vistas.ac.in, jaya.se@vistas.ac.in, director.ece@vistas.ac.in

Abstract- Phishing attacks are becoming a more prevalent danger in the realm of cybersecurity, targeting individuals and organizations to obtain sensitive personal and financial information through fraudulent means. With the continuous advancement of phishing techniques, traditional detection methods similarbans and rule basedstructuresare finding it difficult to effectively counter the ever-changing tactics used by attackers. This paper reviews a broad range of ML algorithms applied to phishing detection, highlighting their effectiveness, limitations, and potential challenges in practical applications. It also identifies promising areas for future research, with an emphasis on improving classification accuracy, reducing false positives, and developing adaptive detection models that can enhance cybersecurity defences in real-time. The proposed ensemble machine learning process such as Random Forest and CNN obtains 97% accuracy and also reduced error rate by 5%. The testing results highlights proposed technique provides better efficiency in terms higher accuracy, and minimal computational overhead which formulated it appropriate for real-time phishing identification

Keywords—Phishing, Machine Learning, CNN, Classification, Cybersecurity, Phishing Identification.

I. INTRODUCTION

Phishing attacks are a continuing and growing cyber threat that utilizes social engineering to mislead users forexposing theirprivatedata [20]. These threats can ariseviadissimilar channels i.e. email, websites, and social media, and oftenentail impersonating genuine entities to get user faith. Given the latentsignificances of phishing like identity theft and financial defeat, designing an efficientidentificationsystems are vital. Though, conventional phishing discoverytechnique i.e.bans and heuristic rule createdmethods, scuffle to preserve withhigh-speed-evolving techniques utilized by intruders. Blacklists are often restricted by their trust on previously identified phishing URLs, which cannot considered for new and adaptive phishing strategy [1].

To deal with these drawbacks, machine learning (ML) technique has consideredsuch asreliableso-lutionaimed at phishingprediction.ML algorithms can find out patterns and recognize anomalies, formulating them appropriate for identifying phishing attempts that diverge from distinctive online behaviour. Latestinnovations in ML, for instance ensemble learning and deep neural networkhave validatedthe potential outperformstate of the arttechniquesviaobtaininggreateridentification accuracy and adaptability to new hazards [3], [5], [7] ML algorithms can investigate a broad range of features like URL characteristics, website metadata and email information's, facilitating more robust and accurateclassification of phishing attacks [10].

This paper describes a broad analysis of ML-based techniques for phishing recognition using different algorithmic concepts and their function in predicting phishing attempts across various environments [8]. Figure. 1 describes growing phishing threats analysis from 2020-2023. Besides to that, it explains the current difficulties involved during the phishing identification processes i.e. handling big datasets, balancing finding accuracy and false positives, and obtaining real-time identification capability. As well, this paper finds areas for potential research with investigation of novel feature selection, optimization concept, and hybrid systems that can further increases the performance of phishing identification in an ever-evolving threat environment [9]–[27].

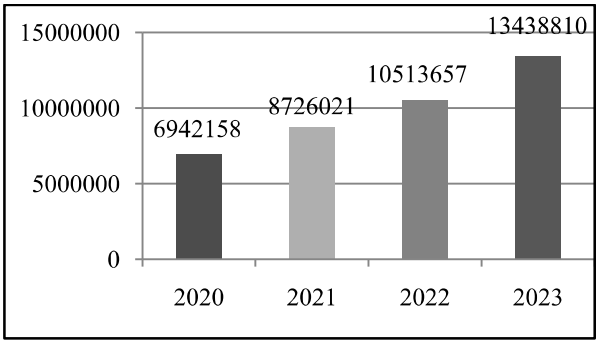

Figure 1. Growing phishing threats from 2020-2023

Overview of Phishing Techniques

Phishing attacks can acquire in diverse types, each leveraging dissimilar algorithmic concept to mislead users. This section discusses several key phishing techniques with significant references.

Email-based Phishing

Phishing emails aim to trap recipients through acting as to be trustworthy sources, planning to steal private information [5] [22]. These emails often include connections to malicious websites or demand users to give personal data frankly.

Website-based Phishing

These attacks depend on fake websites similar to genuine ones, aspiring to trap users into revealing their private information [2] [14]. Attackers often utilize identical domain names or logos to construct their websites appear reliable [16].

Spear Phishing and Social Engineering Attacks

Targeted threats which utilize personalized Information to acquire the trust of particular persons [4]. This phishing employs social engineering concepts to inspire an intelligence of urgency or legitimacy.

Emerging Phishing Techniques

Fig. 2 below shows categories of phishing detection.Current model utilize advanced digital systems to make more believable phishing threats [6] [12]. This incorporates the utilization of social media and instant messaging policies in which attackers exploit the trust built within social networks [18].

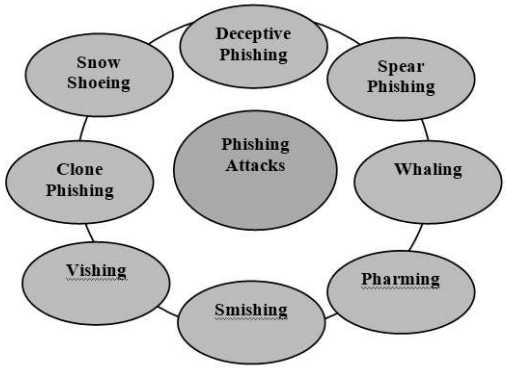

Figure 2. Types of phishing attacks

Machine Learning Algorithms in Phishing Detection

This segment examines the main machine learning algorithms applied in phishing attacks, grouped into distinct categories based on their learning approaches[21].Fig. 3 explains machine learning techniques for phishing detection.

Supervised Learning Techniques

- **Decision Trees**: Simple rule-based model ideal for classifying phishing websites and URLs【1】.
- **Support Vector Machines (SVM)**: Effective for identifying phishing websites based on specific feature sets【4】.
- **Random Forests (RF)**: Combines multiple decision trees, reducing overfitting and improving classification accuracy【2】.

Unsupervised Learning Techniques

- **K-Means Clustering**: Groups phishing patterns when labelled data is unavailable
- **Autoencoders**: Commonly used for anomaly detection in phishing emails【3】.

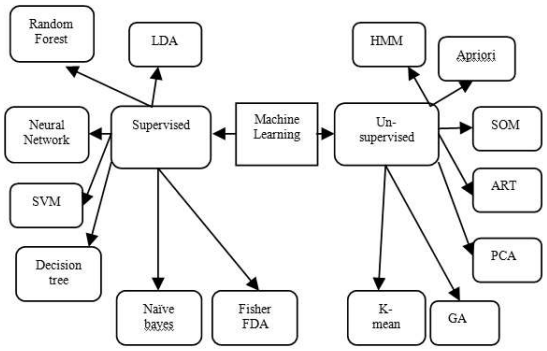

Figure 3. Machine Learning (ML) Techniques for phishing detection

Ensemble Learning

- Ada-Boost and Gradient-Boosting: Chain weak classifiers to strengthen phishing detection and reduce errors【1】【7】.

Neural Network and Deep Learning

Fig. 4 reveals phishing detection process using deep learning

- **Convolutional Neural Networks (CNNs)**: Analyses structures from emails and websites to detect phishing attempts【3】.
- **Recurrent Neural Networks (RNNs)**: Detects phishing attempts based on sequenced data, such as emails【4】

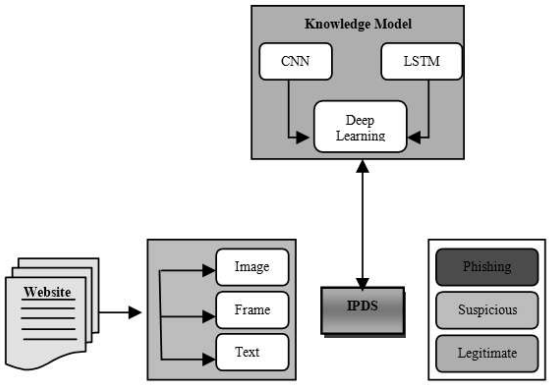

Figure 4. Phishing detection using deep

Learning (CNN and LSTM)

Methodology:

The RF algorithm leverages bagging (bootstrap aggregating) to create a diverse set of decision trees, each trained on random subsets of the dataset. Fig. 5 explainsrandom forest process forphishing detection. Each tree independently predicts whether a URL or webpage is phishing or legitimate based on selected or chosen characteristics, URL length, keyword presence, and domain attributes. Final classification is based on majority vote amongst the trees, enhancing both accuracy and reliability. [1], [7].

Advantages:

- **High Accuracy**: RF can obtain highest classification accuracy through combiningseveral weak classifiers output significantly by decreasing variance and boosting efficiency compared to individual decision trees [1], [9].
- **Feature Importance**: RF delivers insights into feature prominence, agreeing researchers to categorize which characteristics contribute maximum to phishing detection, aiding in feature selection and model interpretability [26].
- **Robustness to Noise**: The model's ensemble nature makes it less sensitive to noise and outliers in the data, enhancing its generalization capabilities [27].

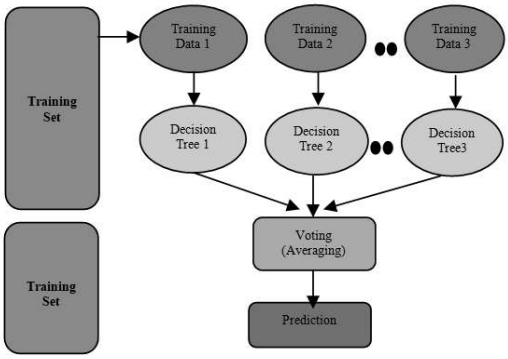

Figure 5. Random forest phishing detection

Disadvantages:

- **Computational Complexity**: Training multiple decision trees can be computationally intensive, especially with large datasets, which may impact real-time detection capabilities [13].
- **Interpretability**: Although RF can indicate feature importance, the overall decision-making process remains less transparent than simpler models, making it challenging for security analysts to understand the rationale behind specific predictions [28][32].

Convolutional Neural Networks (CNNs) in Phishing Detection

CNNs have been effectively applied in phishing detection, particularly in analysing visual data from web pages and email content. CNNs excel at identifying intricate patterns and features in data, making them suitable for detecting phishing attempts based on visual cues.Fig. 6depictsCNN process forphishing detection.

Methodology: CNNs use multiple layers of convolutional filters to capture and extract features from raw input data. In phishing detection, CNNs can analyse screenshots of webpages or the content of phishing emails, identifying visual similarities with legitimate sites. It typically includes convolutional layers, pooling layers, and completely connected layers, culminating in a SoftMax layer for classification. [3], [15].

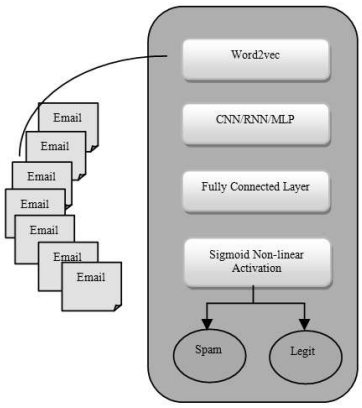

Figure 6. CNN Phishing Detection

Advantages

- **Automatic Feature Extraction**: CNNs can learn significant features from data which is helpful for phishing identification [29].
- **High Performance**: CNNs have shown superior performance in image recognition tasks, leading to higher accuracyidentifying phishing sites that attempt to mimic legitimate ones [17]
- **Scalability**: CNNs can handle high datasets efficiently, creating them appropriate for real-time phishing detection applications [30].

Disadvantages:

- **Data Requirements**: CNNs require considerable amounts of categorized training data to achieveefficiently, which can be a barrier in phishing detection where labelled data may be scarce [19][21].
- **Computational Demand**: Training CNNs can be resource-intensive, necessitating powerful hardware and considerable time [31].

II. Literature Review

Numerous studies have investigated machine learning methods for phishing finding. Kalabarige [1] introduced a hybrid feature selection method based on boosting and a multi-layer stacked collective model expressively enhancing detection accuracy. However, this model risks over-fitting if improperly tuned. Madisetty [2] proposed an ensemble of neural networks for spam detection on Twitter, which excels at handling large-scale data but demands considerable computational resources. Sahingoz [3] developed a deep learning-based system which extracts features from raw data for effective phishing detection but depends heavily on training data quality. Do [4] presentstaxonomy on various deep learning algorithms for reviewing performance of phishing.

Andrade's [5] describes the significance of understanding user actions, though hard to combine with technical architectures. Ghaleb [6] explains credit card fraud discoveryby utilizing GANs and random forests, demonstrating how GANs handle datasets to get better fraud identification accuracy. Rao [7] utilized a multilayer ensemble concept for better phishing identification whichgives robustness but results in overfitting. Vrbančič [25] examines datasets for finding phishing website, showing the value of timely information.Indrasiri [9] implements a robust flexible classifier algorithm which can efficient but may also overfit with extra layers.

Moreover that, Balogun [10] applied Logistic Model Tree for URL phishing finding. Kulkarni [11] presented a phishing landscape identification process with better accuracy. Tamal [27] described feature optimization in phishing discovery to get better efficiency.However, computational cost was more. Mjahidi [13] examined email behaviours to predict phishing and malware-based phishing threats.Khurma [28] utilizedSalp Swarm Optimization to discover the phishing and thusboosting speed however potentially restricting generalizability to new phishing activities. Abawajy [15] designed a multi-tier system for widespread phishing recognition, though its complexity makes implementation very difficult.Parvathapuram[31], [32] describes detection investigation of URL attack in SDR systems and phishing website discovery using Swarm intelligence with deep learning.

CHALLENGES AND LIMITATIONS

Phishing identification model handlefew challenges and constraints as follows,

- **Imbalanced Datasets :** Phishing datasets are repeatedly warped with higher number of benign samples than phishing ones, which result in biased systems [5].
- **Feature Selection :** Finding the most vital features is difficult because attackers repetitively utilized to avoid identification [7].
- **Real-time Detection :** Machine learning concept must be utilized to work in real-time for timely attack recognition [1].
- **Interpretability :** The complex characteristic of deep learning concepts often results to problems

in understanding their decision-making systems. [4].

III. Future Research Directions Adversarial Machine Learning

Research must concentrate on utilizing machine learning concepts that resilient against phishing attacks which can mislead them [6].

Explainable AI (XAI) for Phishing Detection
Describing machine learning system process can assist security analysts understand and faith the discovery process, thus boosting the reliability of phishing identification performance [27].

Hybrid Models
Integrating existing algorithms with machine learning concepts can increase recognition accuracy and diminish false alarms, thus achieving cybersecurity. [25].

Privacy-preserving Machine Learning
Designing a technique for identifying phishing attack is crucial problem to be resolved for cybersecurity. This characteristic will become more and more significant as privacy regulations evolution [13].

IV. Proposed Workflow

The workflow is segregated into three key phases: pre-processing, feature selection, and categorization. The architecture diagram of phishing identification and classification are illustrated in Fig. 7.

Pre-processing
During this task, data cleaning and normalization are done. The ANF is utilized to deal with missing information, take away noise, and normalize the dataset. This process make sure that the dataset is appropriate for further examination through based on interrelated features, thus raising performance and minimizing the complexity [1], [3].

Feature Extraction
Here, Machine Learning Texture Random Forest (MLTRF) is utilized to choose more significant features from the pre-processed data.

- Lexical features: describes URL length and occurrences of unique characters.
- Content-based features: represents features of the email or website.
- Domain-specific attributes: depicts domain age and reputation [1], [4], [6].

The feature extraction is vital in finding concealed patterns and anomalies interrelated with phishing attacks [2], [3].

Classification
The final stage utilizes a hybrid model combining ensemble methods with deep learning techniques. The classification process is as follows:

- An ensemble of classifiers (e.g., Random Forests) is used to enhance generalization and reduce overfitting [1], [2], [3].
- Deep learning techniques, explicitly Convolutional Neural Networks (CNNs), are applied to learn complex patterns from the feature space [3], [17].

The classification decision is made through majority voting among the classifiers, which improves accuracy and robustness [4], [5].

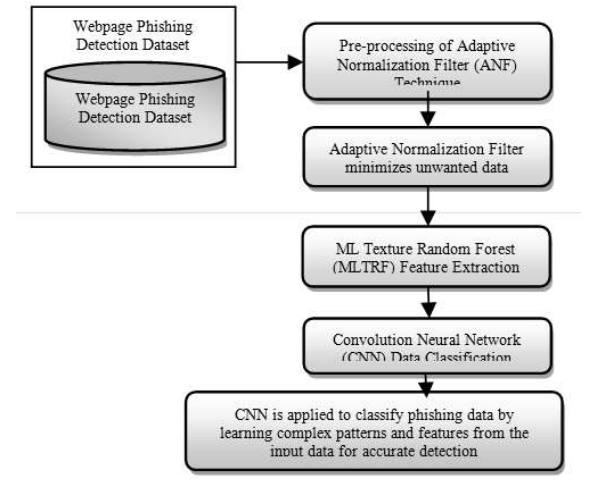

Figure 7. Proposed architecture diagram of Phishing Detection and classification

V. Results And Discussion

Accuracy: Prediction accuracy (%) serves as a crucial metric for evaluating the effectiveness of the proposed approach. It measures how many predictions made by the model are accurate related to the over-all number of prediction. The integration of various components enhances the overall predictive accuracy, thereby improving the reliability of phishing website detection.

The proposed hybrid model demonstrates superior accuracy in comparison to the existing Boosting Ensemble Learning and Neural Network techniques.

$$Prediction\ Accuracy = \frac{No\ of\ Correct\ \ Non\ Phishing\ website}{Total\ \ No\ of\ website} * 100 (1)$$

By using equation (1), prediction accuracy of phishing threats is measured. Table 1 and Fig.8 shows the comparative prediction accuracy of Proposed MLTRFCNN and conventional two methods.

Table 1 Prediction Accuracy of MLTRFCNN

Number of Input Data ( )	Prediction Accuracy (%)		
	Proposed MLTRFCNN	Boosting Ensemble Learning	Neural Network (NN)
1000	96	90	87
2000	94	92	83
3000	96	93	80
4000	93	91	83
5000	94	92	84
6000	95	93	82
7000	97	94	88
8000	95	92	89
9000	96	93	88
10000	97	94	90

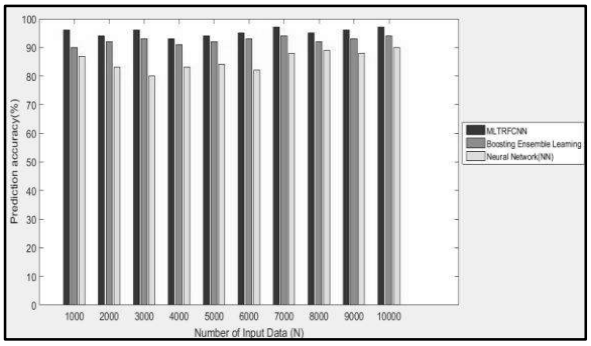

Fig 8: Comparison Graph for Prediction Accuracy

Comparison Error rate:

The proposed MLTRFCNN greatlydecreases the error rate with application of an Adaptive Normalization Filter Itimproves data pre-processing performancethroughremovingunrelated noise from input. The Texture-based Random Forest feature miningconcept further filters the information vi are veiling important attributes and lessening dimensionality, tolerating the model to concentrate on the mostvital patterns. With the support of optimized inputs, the CNN giveshigherefficiency and accuracy.

$$Error\ Rate = \frac{No\ of\ InCorrect\ \ Prediction}{Total\ \ No\ of\ website} * 100 \quad (2)$$

By using equation (2), error rate of phishing threats is determined. Table 2 and Fig.9 shows the comparative error rate of Proposed MLTRFCNN and conventional two methods.

Table 2 Error Rate of MLTRFCNN

Number of Input Data ( )	Error rate (%)		
	Proposed MLTRFCNN	Boosting Ensemble Learning	Neural Network (NN)
1000	5	10	13
2000	8	12	15
3000	11	17	16
4000	14	21	21
5000	22	25	30
6000	26	29	35
7000	27	32	37
8000	33	40	42
9000	35	44	54
10000	37	56	58

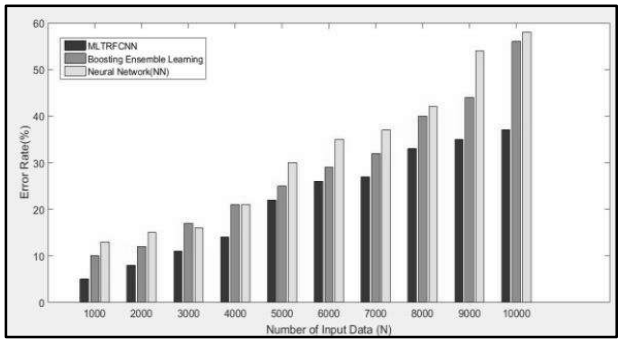

Fig 9: Comparison Graph for Error Rate

Prediction Time (ms):

The proposed MLTRFCNN decreases discovery time throughcombining the Adaptive Normalization Filter with Texture-based Random Forest concept. In feature extraction task, data complexity is decreased viaclustering relatedattributes. The Mapping Random Forest method further increases data competencethroughminimizing dimensionality and emphasizing the most significant features. The optimization applies the CNN concept in order to process inputs more efficiently which drastically lessens the time required for accurate phishing identification.

$$PT = Time\ at\ End\ of\ Prediction - Time\ at\ Start\ of\ Prediction \quad (3)$$

By using equation (3), prediction time of phishing threats is determined.

Table 3 Prediction time of MLTRFCNN

Number of Input Data ( )	Prediction Time (ms)		
	Proposed MLTRFCNN	Boosting Ensemble Learning	Neural Network (NN)
1000	96	90	87
2000	94	92	83
3000	96	93	80
4000	93	91	83
5000	94	92	84
6000	95	93	82
7000	97	94	88
8000	95	92	89
9000	96	93	88
10000	97	94	90

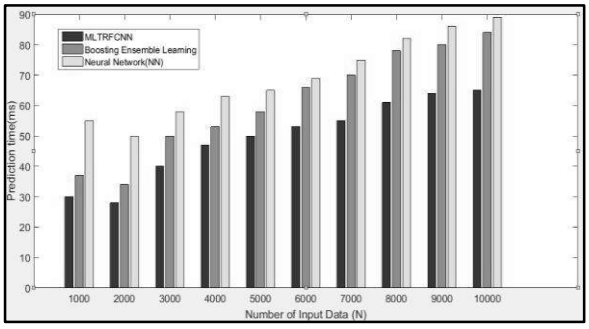

Fig 10: Comparison Graph of Prediction Time

Table 3 and Fig.10 shows the comparative prediction time of Proposed MLTRFCNN and conventional two methods.The proposed work achievesfast computation forthreat identificationtasks. On the contrary toconventional techniques, the CNN trained with improved dataset considerablyspeed ups the understanding process andthuslessenstotal taken for discovering the phishing attacks. As a result, implemented MLTRFCNN gets a minimal prediction time as compared toexisting [1] and [2].

VI. Conclusion

Machine learning algorithms give reliable performance for finding phishing attacks, resolves the evolving problems of these attacks. The existing study have revealed their efficiency; challenges handled during the phishing identification [2][5][6]. Future research should providestrong adversarial protectionsystemimproving interpretability, and implementing hybrid predictionmethods, because these factors are fundamental for accuratelyfinding phishing threats. [7][27][28].The proposed MLTRFCNN reveal senhanced performance in terms of accuracy by 97%, an execution time by 30 microseconds and reduced error rate by 5%. The testing results proved its appropriateness for real-time applications via rapid processing, higheraccuracy, and minimal errors. Future work could explore additional feature sets and further optimization to enhance and sustain these outcomes.

References

[1]. L. R. Kalabarige, "A Boosting-Based Hybrid Feature Selection and Multi-Layer Stacked Ensemble Learning Model to Detect Phishing Websites," 2023. – IEEE

[2]. S. Madisetty, "A Neural Network Based Ensemble Approach for Spam Detection in Twitter," 2018.

[3]. O. K. Sahingoz, "DEPHIDES: Deep Learning Based Phishing Detection System," 2024. – IEEE

[4]. N. Q. Do, "Deep Learning for Phishing Detection: Taxonomy, Current Challenges, and Future Directions,"2022. – IEEE

[5]. R. O. Andrade, "An Exploratory Study of CognitiveSciences Applied to Cybersecurity," 2022. – WOS

[6]. Vivas, D. E. D., Pena, W. Y. G., Botero, S. P. C., & Rojas, A. E. (2024). A Controlled Phishing Attack in a University Community: A Case Study. Journal of Internet Services and Information Security, 14(2), 98-110. https://doi.org/10.58346/JISIS.2024.I2.007

[7]. Oversampling Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," 2023. – IEEE

[8]. Mahmood, S. S. (2025). Intelligent cyber defense: Utilizing deep learning for robust detection and prevention of phishing websites. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 16(2), 591–610. https://doi.org/10.58346/JOWUA.2025.I2.036

[9]. G. Vrbančič, "Datasets for phishing websites detection," 2020. – SCI(elsevier)

[10]. Veerappan, S. (2023). The Role of Digital Ecosystems in Digital Transformation: A Study of How Firms Collaborate and Compete. Global Perspectives in Management, 1(1), 78-89.

[11]. A. O. Balogun, "Rotation Forest-Based Logistic Model Tree for Website Phishing Detection," 2021. – ACM

[12]. Hlushenkova, A., Kalinin, O., Navrozova, Y., Navolokina, A., Shcherbyna, V., & Doroshenko, T. (2024). Management of Strategies for Shaping the Innovative and Investment Potential of Enterprises as a Factor Ensuring Their Economic Security. Indian Journal of Information Sources and Services, 14(3), 16–22. https://doi.org/10.51983/ijiss-2024.14.3.03

[13]. M. A. Tamal, "Unveiling Suspicious Phishing Attacks: Enhancing Detection with an Optimal Feature Vectorization Algorithm and Supervised Machine Learning," 2024. – frontiers

[14]. Wan, Q., & Hu, X. (2024). Legal Framework for Security of Organ Transplant Information in the Digital Age with Biotechnology. Natural and Engineering Sciences, 9(2), 73-93. https://doi.org/10.28978/nesciences.1569190

[15]. R. A. Khurma, "Salp Swarm Optimization Search Based Feature Selection for Enhanced Phishing Websites Detection," 2021. – ACM

[16]. Deshmukh, S., & Menon, A. (2025). Machine Learning in Malware Analysis and Prevention. In Essentials in Cyber

Defence (pp. 74-89). Periodic Series in Multidisciplinary Studies.

[17]. I. J. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. Cambridge: MIT Press, 2016. – book [17] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," in *Advances in Neural Information Processing Systems*, vol. 25, 2012, pp. 1097–1105. – ACM

[18]. Lotfy, B., &Vatankhah, H. (2014). Study of insurance in cyberspace and its infrastructure in Iran and other countries. International Academic Journal of Science and Engineering, 1(1), 49–56.

[19]. R. Caruana, A. Niculescu-Mizil, "An Empirical Comparison of Supervised Learning Algorithms," in *Proceedings of the 23rd International Conference on Machine Learning*, 2006, pp. 161–168.- ACM

[20]. Aravind, B., Harikrishnan, S., Santhosh, G., Vijay, J. E., & Saran Suaji, T. (2023). An Efficient Privacy - Aware Authentication Framework for Mobile Cloud Computing. International Academic Journal of Innovative Research, 10(1), 1–7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[21]. Parvathapuram Pavan Kumar,T.Jaya and Dr.V.Rajendran ,"Detection Analysis Of URL Attack In SDR Systems For Network Data" International Journal of Future Generation Communication and Networking,Vol. 13, No. 4, pp. 1759-1772, November 2020.

[22]. Parvathapuram Pavan Kumar,T.Jaya and Dr.V.Rajendran," SI-BBA – A novel phishing website detection based on Swarm intelligence with deep learning, Volume 80, Part 3, Pages 3129-3139, 2023

[23]. F. A. Ghaleb, "Ensemble Synthesized Minority R. S. Rao, "Multilayer Stacked Ensemble Learning Model to Detect Phishing Websites," 2022.- IEEE

[24]. P. L. Indrasiri, "Robust Ensemble Machine Learning Model for Filtering Phishing URLs: Expandable Random Gradient Stacked Voting Classifier (ERG-SVC)," 2021.- IEEE

[25]. A. Kulkarni, "Phishing Webpage Detection: Unveiling the Threat Landscape and Investigating Detection Techniques," 2024. – IEEE

[26]. D. M. Mjahidi, "Enhancing Machine Learning Detection Techniques to Secure E-mail Communication against Malware-based Phishing Attacks," 2024. – academia

[27]. J. Abawajy, "A Multi-tier Phishing Detection and Filtering Approach," 2013. - SCI(elsevier)

[28]. Y. LeCun, Y. Bengio, and G. Hinton, "Deep Learning," *Nature*, vol. 521, no. 7553, pp. 436–444, 2015.

[29]. G. Hinton, L. Deng, D. Yu, et al., "Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 82–97, 2012. – IEEE