Building Dynamic permutation based Privacy Preservation Model with Block Chain Technology for IoT Healthcare Sector

A.Yogeshwar
Research Scholar,
Department of Computer Science,
Vels Institute of Science,Technology & Advanced Studies(VISTAS) School of Computing Sciences,
Pallavaram, Chennai, IndiaVels Institute of Science,Technology & Advanced Studies(VISTAS),
Pallavaram, Chennai, India
e-mail: yogeshma@gmail.com

S. Kamalakkannan
Associate Professor,
Department of Information Technology,
Vels Institute of Science,Technology & Advanced Studies(VISTAS) School of Computing Sciences,
Pallavaram, Chennai, IndiaVels Institute of Science,Technology & Advanced Studies(VISTAS
Pallavaram, Chennai, India
e-mail: kannan.scs@velsuniv.ac.in

2022 International Conference on Advanced Computing Technologies and Applications (ICACTA) | 978-1-6654-9515-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICACTA54488.2022.9753342

***Abstract*—Blockchain technology has the potential to address present interoperability issues in health information systems by establishing a technological standard that ensures safe electronic health data exchange amongst people, healthcare suppliers and medicinal up keep organizations including medical professionals. Patients' sensory data can be fed into Internet of Things (IoT) devices in real timewhich can be evaluated and managed in the healthcare industry. The privacy and security of health data pertaining topatients' is now also a major concern with IoT devices across a wide variety of product sectors.According to previous research, blockchain technology has been determined to be a substantial answer to the data security concerns that present in IoT. The Dynamic Permutation with Multi-Modal Safe Data (DPMMSD) based Hyper Elliptic Curve Cryptography (HECC) Framework (DPMMSD-HECC) is suggested in this research for safeadmission and regulator topatient's data in IoT. The suggested framework of healthcare data management in IoT devices is successfully utilized for fulfilling the optimum confidentiality and safety requirements. Blockchain approach has beenused in this study to develop a dependable and safe data sharing stage that connects several information sources and encrypts and records IoT data in a distributed ledger.A research on security revealed that a particular information secures the parameters related to DPMMSD-HECC model for data analysts and maintains the secrecy of important data from each data source. The recommended strategy is evaluated compared to two benchmark datasets from the UCI AI repository: Breast Cancer Wisconsin Data Set (BCWD) and Heart Disease Data Set (HDD). The. Simulation results showed that the proposed DPMMSD-HECC model has outperformed all of the other techniques in a number of ways.**

Keywords: Blockchain, IoT, Elliptical curve cryptosystem, Healthcare systems, DPMMSD-HECC, Privacy, Security

I. INTRODUCTION

Healthcare's main goal is to improve people's eminence of life by enhancing their well-being and also in delivering services [1]. Patient care is the recovery, avoidance, protection, and organizing emotional as well as bodilycomfort for healthcare experts[2]. In a hospital facility, patient data management entails establishing a functioning data structure which serves like a foundation to information accessibility as well ascentralized management [3]. A comprehensive tactic in processing of patient data is becoming gradually vital as businesses trust on to build value from intangible assets [4]. As an instance, it necessitatesdata from a variety of healthcare areas is collected, entered, encoded, output processed, retrieved, and stored.IoT category comprises sophisticated technologies like health/vital surveillance and wearable that is specifically developed for utilizing in healthcare industry at house, in neighborhood, in hospitals and clinics, as well as in tele-health including further additional amenities [5].The cornerstone for IoT machine-to-machine connectivity is Wi-Fi-enabled medical equipment [6]. IoT enables sensors to record important information and send across clinicians in real time for patient follow-up [7]. Smartphone applications and other connected devices may warn doctors and nurses to security dangers and crucial situations [8]. Many medical institutions have networks that are not reliable or strong enough to support IoT devices. Because of the large volume of data shared, clinicians may have difficulty accessing patient information when they need it, leading in bottlenecks [9].Patients can use blockchain technology to set access restrictions for their medical information, enabling specific researchers forretrieving sections of records during set time duration [10]. Blockchain technology can be used by patients to connect to other institutions and have its medical data

978-1-6654-9515-8/$31.00©2022IEEE

automatically captured. Smart contracts are utilized in protectingblockchain'sconfidentiality and safety [11].

A blockchain [12] is essentially a digital database related to transactions that are replicated as well as duplicated over blockchain's complete network of computer system. In smart and remote hospitals, patients' vital signs may be carefully followed. Infrastructure blockchain aids in sharinginformation in a safe manner. This is why JavaScript and HTML are so important to the Internet and user experience. The IoT is used to calculate blockchain network patient-centered services.Only authorized computer users have access to the IoT devices linked to the sensory health module. Patient portals, electronic medical records, and smartphone applications have all been utilized widely by health professionals [13]. Cloud storage allows health institutions to save all of their data while reducing computer maintenance costs [14].IoT data is stored as strings in blocks, in an off-chain database, patient data is kept in blocks called InterPlanetary File Systems (IPFS) [15]. The whole patient's medical information is stored on every participating node on blockchain network, causing data storage and bandwidth issues [16].IoT-enabled intelligent healthcare networks are subject to serious hazards and security concerns [17].

A healthcare application system has used blockchain key to safely issue warnings to certified healthcare practitioners [18]. The patient's verification is evaluated using blockchain-based digital authentication, which assesses the legitimacy of a digital identity or additional authenticators. It signifies that the technology used to authenticate a person attempting to access a digital service is under control. Utilizing patient data's blockchain encryption, the unique data source is turned into encoded language of an entity. This necessitates safeguarding confidentiality and security pertaining to electronic secured health information stored in healthcare annals, ensuring in way whereinunofficial individuals could not access or utilize data even though it is stored in a network or database.Blockchain is an encouraging technology which may be utilized to keep a translucent ledger as well as distribute informationamid members. It is frequently employed in cryptocurrency systems [19], [20]. Medical records can benefit from blockchain technology's stability and restoration promises because of its distributed nature and tamper-resistant. Cloud computing stores all of the data and reduces the need for physical device maintenance.In off-chain table, patient information is saved as strings in blocks, IoT data on the other hand is preserved in IPFS blocks. By implementing blockchain, eachcontributing node present in network has access to patient's whole medical archives that causes bandwidth and data storage issues.

The DPMMSD-HECC augmented data flow and safe access control on patient's information is proposed in this work. Sensory feedback from patients may be collected by IoT systems and processed atactual time for handling healthcare. The security and privacy of patient health information has been a major concern related to IoT devices in a variety of product categories.The use of blockchain in IoT to develop DPMMSD-HECC is recommended in this study. The proposed solution is simple to implement and meets the optimal safety and confidentiality criteria inhandling IoT data. A healthcare application network has used blockchain key to store health data related to patients and it may be securely used to provide important notifications for verified healthcare practitioners.

The following is how the paper is organized: The previous technique has a difficulty with healthcare data integration and security, as described in Section 2. Section 3 explains the proposed DPMMSD-HECC framework, including the encryption and decryption algorithms, Section 4 is where the results and discussions are discussed, and Section 5 is where the conclusion is reached.

II. LITERATURE REVIEW

By exchanging decentralized genetic data, Luis et al. [21] highlighted the prospective of blockchain technology in the public health's scrutiny. A fundamental explanation of why blockchain technologies are crucial in public health is provided, as well as dissimilarity amid private and public blockchain.

In conclusion, to solve interoperability difficulties in health sector, a plan for a network of blockchain grounded on the decentralized storage frameworks and Cosmos architecture like BigchainDB and IPFS and is presented. Tanzila Saba et al. [22] recommended a Safe and Energy-Efficient architecture for e-healthcare Founded on Internet of Medical Things (SEF-IoMT). Wireless body area networks play a crucial role in medical procedures. As they track patients' health and communicate information to remote medical facilities so that necessary steps may be taken.However, because of the restricted sensor capabilities, the data transfer system has to be both energy efficient and precise. Furthermore, sensitive patient data is more likely to be exposed to dangers, jeopardizing data security.This study proposes an e-health system that is both energy efficient and safe, utilizing IoMT to reduce energy consumption including offering more data to medical professionals on regular basis.For an IoMT framework in e-healthcare, Ashutosh Sharma et al. [23] supported blockchain-based smart contracts. Smart blockchain contracts, which are preset code short scripts, will eradicate intermediaries and enhance

978-1-6654-9515-8/$31.00©2022IEEE

contract execution. The paper examines the degree of IoMT decentralization and the use of intelligent contracts in e-healthcare, proposes current design, and assesses the benefits and drawbacks of combining all three, as well as future enhancements.In the healthcare area, blockchain technology is critical for providing security, trust, and authentication among all stakeholders (hospitals, doctors, patients and other medical entities).

Mettler et al. [24] offered instances of how Blockchain may be utilized in healthcare business in a diversity of approaches. Blockchain enhances pharmaceutical safety in minimizing the expense of health-care continuation. The advantages of Blockchain for healthcare applications have been recognized, and it will have a major influence on the power balance in the healthcare business. A Blockchain prototype is presented that improves and ensures safety, confidentiality and approachability for monitoring and in malignant development, sharing EMR information (cancer) therapy of the patient [25].Chen et al. [26] presented a full medical information system built on blockchain technology to achieve the objective of safe medical data storage and exchange. A data collecting system based on the IoT is also being developed, which might collect data from a variety of non-invasive medical devices at the same time, allowing for real-time patient health records to be gathered at the time of operation.To increase the safety of private medical data sharing, this technique created an unidentifiable medical data sharing method using a proxy re-encryption algorithm and cloud servers.For data management and access control, the system is built on the permissioned blockchain architecture Hyperledger Fabric, through a medical chain code and dual-channel Fabric deployment design.This paper study paves the way for remote treatment as well asdata mining, diagnosis and further real-world applications built based on medical data recorded on a blockchain.

SPChain is a privacy-preserving eHealth system and a blockchain established medical information exchange suggested by Zou and co. [27]. They devised customized key blocks and micro blocks for patients in keeping their EMRs in order to achieve rapid retrieval. To incentivize medical establishments to link SPChain, a reputation method is being designed. SPChain uses proxy re-encryption technologies to make it easier for patients to share medical data while maintaining their privacy. To analyze SPChain, they use a real-world distribution of miners to examineperformance of systemand resistance to assaults outlined.SPChain could reach extraordinary throughput (220 TPS) having negligible storage overhead, according to findings. SPChain has a reduced temporal complexity in terms of data retrieval than existing schemes, and it can withstand suggested blockchain attacks including SPChain assaults.Rathee et al. [28] used the blockchain approach to create a security outline for healthcare multimedia information by producing hash of everyinformationas a result of any data change or update, such as a breach of pharmaceuticals, is replicated in whole blockchain network users.Due to Blockchain technology, findings have been compared to traditional approaches and confirmed with improved simulated findings, the success percentage of the product worm hole attack, drop ratio falsification attack and probabilistic authentication scenarios is all 86%.Sri et al. [29] studied and assessed the use of block chain technology to secure patient data on a shared network. In this scenario, a consensus technique is utilized for authenticating Proof of Word and Interoperability for data detection and admission.This approach computes structural and semantic compatibility authentication and creates a centralized point of trust for network consensus.In contrast to other network models, this consensus process demonstrates a superior trade-off. Chen et al. [30] devised a storage method established on cloud storage and blockchain for personal medical data management. Also mentioned is a service agenda for exchanging medical archives. Furthermore, through a comparison with existing systems, the properties of the medical blockchain are given and assessed.The suggested storage and sharing arrangement does not necessitate the involvement of a third party and no one entity has complete control over the processing.

III. PROPOSED METHODOLOGY

This study examined the use of IoT in healthcare sector in safeguarding patient informationbesides preventing data transmission failures. The IoT provides a framework in healthassociatedand medical testing, data collecting as well as analysis. The informationgatheredis safely stored in cloud-based systems.IoT in the medical industry now faces transmitting patient data, assimilation of data and Internet-connected medical device protection. As a result, the DPMMSD-HECC Framework is developed in this research for improved information flow and patient information access management safely.Patient health data may be safely notified to certified healthcare practitioners a network of healthcare apps that uses blockchain analysis of data and the associated blockchain key. Any failure or unauthorized access to blockchain warns the patient and IoT healthcare system in the course of data exchange.

978-1-6654-9515-8/$31.00©2022IEEE

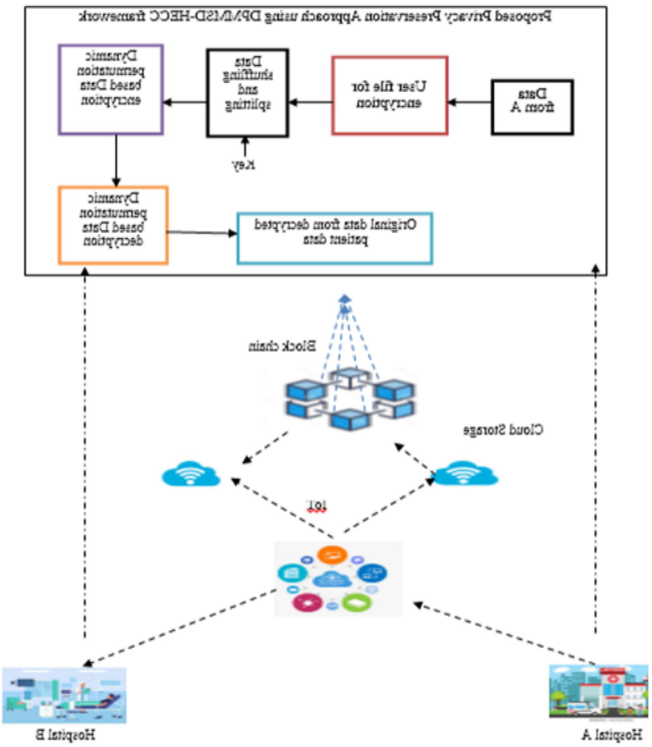

Figure 1: Architecture of the proposed work

The suggested DPMMSD-HECC is shown in Figure 1. Medical information systems are becoming increasingly popular among IoT systems. Through the Internet, Data from devices such as heart rate monitors, body sensors, and wearable devices may be collected, stored, and sent in real time using this technology. As technology advances, providers will be able to perform data analysis simultaneously and the outcomes could be shared with others who have admittance to data via the blockchain with IoT. Using a supplemental computer that is normally in permanent service, the patient will act as a data route for all data, resulting in vast sums of data.Information created data can be intervened by intelligent systems, which would process critical information and if required, add it to blockchain. As envisioned, itoutcomes in a vertically integrated device that is stable and constantly available.In IoT, the use of blockchain technology allows for a secure real-time patient monitoring system. Blockchain technology has been utilized to share genuine data. To develop an interesting technology for health surveillance, based on an intrinsic differentiation between border and core networks that allows for both centralized and decentralized data transmission techniques.This model exhibits increased scalability and proficiency for a blockchain scheme, particularly while considering dynamic data istaken into consideration.

The currentwork employs togethertwo encryption approaches, specifically asymmetric algorithms towards both ciphertext decryption (D) andplaintext (E) and asymmetric algorithms employ different keys for plaintext encryption and ciphertext decryption (D). Information can normally be encrypted using a network node's public key, and data can be decrypted using that node's private key. In our suggested paradigm, sender A first wishes to transfer a whole original file to Receiver A through the cloud.By employing dynamic permutation key, the entire original file may be arbitrarilyscuffled, and then this scrambled file can be separated into a number of subfiles called sectors. The original message may be broken into 64 bit chunks using this method. Each block has 64 bits of data, which is divided into two 32-bit halves.SLeft and SRight are the subblocks on the left and right, respectively. Sub-patterns B1, B2, B3, and B4 are created from these sub-blocks (8 bits). Odd digits of bits Bo and even digits of bits Be make up these sub patterns named asInter-bit Merge and Exchange Pattern (IbEM). Take, for example, the data owners of A and B, which are both considered open clouds.Each data owner is in charge of his or her own personal data. If data owner A wanted to transfer their own data to data owner B's persist, they would utilize public key for sending entire original data file. In entire situation, amount of words used in the original file can be utilized to turn the original file into a shuffled file with dynamic permutations. The shuffled file can then be divided into many sectors using a random key. For data transmission over resources, all sectors are picked at random using either of the Multi-Model IBEM and HECC approaches.

➢ **Data Encryption scheme**

A sender jumbled this Data File (D_F) into SHUFF (D_F) to generate a shuffled file using public key user A (PU_{KA}) for a user domain A as the whole input original file Original D_F. The suggested scheme's data encryption method may be divided into the following categories:

i. Splitting and shuffling data
ii. Multi-modal dynamic permutation is used to encrypt data.
iii. Decryption of data via multi-modal dynamic permutation

3.1 Data shuffling and splitting

Assume that the entire file is designated as D_F. SHUFF is the term given to these scrambled data files (D_F). Then, in this shuffled file, count the number of words that appear. Let's pick a number between 1 and 5 at random. Spitted data file (SD_F) is created by splitting a shuffled file using a previously produced random number and creating a new file.

A. Data encryption based on multi modal dynamic permutation

The owner of data A wishes to convey information to the owner of data B. In such case, the data owner A submits his whole original file together with his PU_{KA} public key. Both

978-1-6654-9515-8/$31.00©2022IEEE

data owners A and B share this key. The files are then encrypted with one of the schemes available. Following is a representation of the encryption algorithm:

Encryption algorithm:

Input: Original data file

Step:1 Input: Original data file D_F.

Step:2 SD_F Shuffling the data file

Where SD_F is randomly shuffled file ofD_F.

Step:3 Compute SP_F Splitting the data file

SP_F Splitting the SD_F.

Step:4PICK E_{mode} = $DPMMSD_{mode1}$, $DPMMSD_{mode2}$, $DPMMSD_{mode3}$, $DPMMSD_{mode4}$,

DPMMSD HECC

If E_{mode} = 1

Out ← HASH ($DPMMSD_{mode1}$)

Else if E_{mode} = 2

Out ← HASH ($DPMMSD_{mode2}$)

Else if E_{mode} = 3

Out ← HASH ($DPMMSD_{mode3}$)

Else if E_{mode} = 4

Out ← HASH ($DPMMSD_{mode4}$)

Else

Out ← HASH ($DPMMSD_{HECC}$)

A. Data decryption based on multi modal dynamic permutation

If user B wishes to decode a file supplied by data owner A, he must first receive an encrypted file containing his PR_{KA}. The files are then decrypted using the encryption algorithms employed. The following is the decryption algorithm:

Decryption algorithm

Input : Out

Output: Original data file

Step:1 Get the encrypted file Out

Step:2SD_F← Out (E_{mode})

Where E_{mode} = { $DPMMSD_{mode1}$, $DPMMSD_{mode2}$, $DPMMSD_{mode3}$, $DPMMSD_{HECC}$ }

Step:3 SD_F← apply merge process SP_F

Step:4 RESHUFF← SD_F

3.4 Blockchain systems

The system describe a unique exchange structure for storing encrypted IoT data on blockchain. An exchange initiative is primarily divided into two areas: information and performance.The location, coded information, and kind of the information provider's IoT gadget are all included in the information field. The coded information, information auditor's whereabouts and IoT device kind are all contained in the service field. The 32 bytes hash assessment is derived from addresses in both fields. The encoded data is derived from the ECC computation. The private key is 128 bytes long if every instance of encoded data kept in a rectangle network is 128 bytes long, whereas an IoT device type component is 4 bytes long.Subsequent to each transaction, the hub links with a blockchain information provider to a peer-to-peer organization, where research centers may verify the legitimacy of exchange.

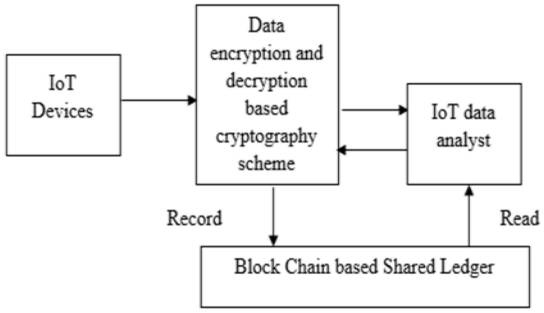

Figure 2: Proposed privacy-preserving secure data transport system based on block chains

According to Squares, blockchain is a public as well as widely accepted ledger that is initially meant to record trades in cryptographic money systems, as seen in figure. 2. It considers the trustworthiness of the information exchanged between suspected members' meetings. Hyper Ledger, Ethereum, and EOS are examples of blockchain tiers that have recently been developed and are now being deployed in a number of applications.The blockchain stages may be classified into three categories based on access rules for blockchain clients: private blockchains, open blockchains and consortium blockchains. A blockchain comprises of three essential properties which make it suited for exchanging trustworthy data:

- **Decentralized:**A blockchain, like a transferred disk, is established on distribution system and does not require a trustee or an outsider. In the register, there is some duplication of information in framework thatavoids information from being lost when there is just one goal of frustration.
- **Tamper-proof:**To regulate the choice and produce new squares, Blockchain employs consistent protocols like Proof of Work (PoW). In view of it, information control is typically incongruent in terms of computing cost. As a result, the data stored in the squares remains unaffected.
- **Traceability:**In the blockchain architecture, different participants may effectively regulate the

978-1-6654-9515-8/$31.00©2022IEEE

trade between two meetings. Each interaction may be tracked and used indefinitely by the information owner. For example - compliant to charges for all data collected by a stranger.

Even though blockchain has a wide variety of uses, it isn't appropriate for information exchange attacks and does not provide data security. All transactions are initially documented in plain text squares, resulting in personalinformation on exchanges that is accessible for users, including competitors. As a result, while using blockchain as a method of data transfer, safetyand well-being must be prudentlymeasured.

IV. Result and Discussion

The current study employed two reliable data indicators, HDD and BCWD, to analyze the technique for this examination. The BCWD parameters were derived from a scanned picture of a light needle inserted into a breast mass. It also specifies the features of the cell nuclei in the picture. Each case is a combination of mild and severe. The HDD consists of 13 numerical benefits, and each case is classified based on whether or not it has Coronary Artery Disease. To avoid any unwanted or diverse outcomes, the typical implications of mutual recognition of ten contracts are shown below.The dataset is separated into training and testing halves for exploration using a 10-fold cross validation technique.In the existing study, every IoT data provider gathered everyinformation from IoT devices in its area and subsequently used that data to fulfill the following services (e.g., data encryption).DPMMSD-HECC, a blockchain-based IoT system for safe admittance to and control of patient data assuggested in Java Development Kit 1.8.

4.1 Accuracy

The two most often used criteria in ML classification evaluation are universally accepted.Table 1 and Figure 3 exhibit the accuracy analysis of DPMMSD-HECC model with comparable techniques on applied two BCWD and HDD datasets. On the BCWD and HDD datasets, the suggested DPMMSD-HECC model achieved maximum accuracy values of 93.54 percent and 96.78 percent correspondingly, according to the table values.On the BCWD and HDD datasets, the current Ant Colony Optimization (ACO) method has somewhat lower accuracy values of 92.42 percent and 94.12 percent, respectively. Simultaneously, the Support Vector Machine (SVM) model showed inadequate performance on HDD and BCWD datasets, with minimal precision values pertaining to 91.56 percent and 93.21 percent correspondingly. Table 2 and Figure 4 provide a thorough recall study of the DPMMSD-HECC model over the similar methodologies on two BCWD and HDD datasets.DPMMSD-HECC model suggested has higher recall values of 93.54 percent and 96.78 percent on BCWD and HDD datasets respectively as shown in table values. The accessible ACO technique has even lower recall values on the BCWD and HDD datasets, with 92.42 percent and 94.12 percent respectively. On HDD and BCWD datasets, SVM model produced the worst results with least recall values of 91.56 percent and 93.21 percentcorrespondingly.

Table 1: Proposed and existing precision measures

S.No	Input dataset	DPMMSD-HECC model	ACO	SVM
1.	BCWD	93.54%	92.42%	91.56%
2.	HDD	96.78%	94.12%	93.21%

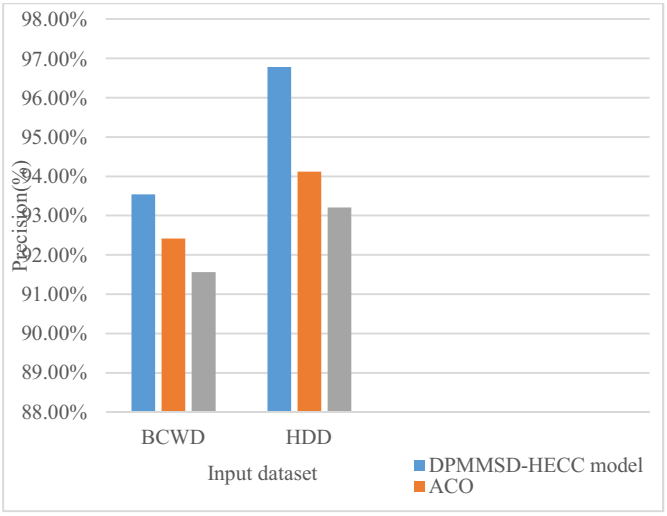

Figure 3: Proposed and existing recall are shown graphically

Table 2: Proposed and existing recall measures

S.No	**Input dataset**	**DPMMSD-HECC model**	**ACO**	**SVM**
1.	BCWD	93.54%	92.42%	91.56%
2.	HDD	96.78%	94.12%	93.21%

978-1-6654-9515-8/$31.00©2022IEEE

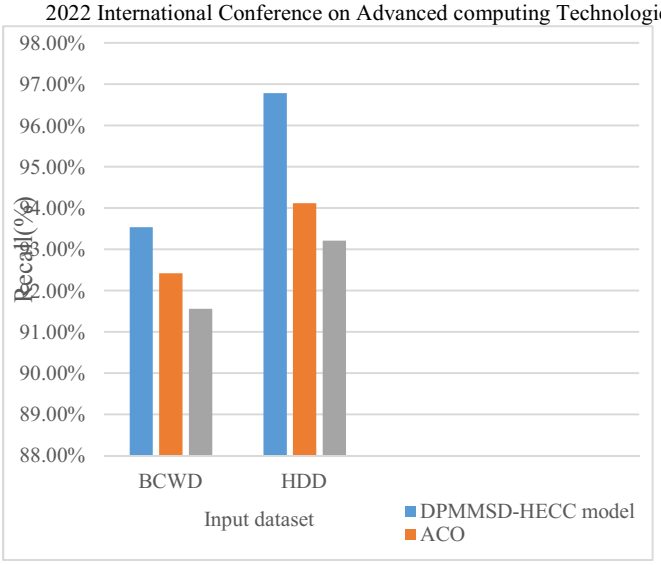

Figure 4: The proposed and existing recall are depicted graphically

V. CONCLUSION

Medical evidence like prescriptions as well as past medical histories is critical in assessing a patient's diagnosis and subsequent treatment since health care is such an important aspect of our lives. The health database, on the other hand, may be permanently changed or removed. The information stifling is an issue. Information is prohibited as a person may not have been provided an access to data that must not have been seen without patients' or hospitals' permission.The current paper looked at every work that might be done using blockchain technology and IoT devices to improve medical treatment and data management. In conclusion, blockchain improves data privacy and security by encrypting data and allowing only the private key ofpatient to be utilized for decryption. IoT data is recorded and maintained in a distributed ledger utilizing blockchain technology, which has been recommended, which enables a safe and trustworthy data exchange platform across numerous data sources.The proposed model's performance is validated utilizing two benchmark datasets from UCI repository, the HDD datasets and BCWD. Experimental outcomes showed that DPMMSD-HECC model outperformed the other techniques in terms of precision and recall on all datasets.The suggested model may be expanded into a framework which might be utilized to develop a range of machine learning training methods which preserve confidentiality in numerous mechanisms of encrypted information in future.

REFERENCES

[1] Girardi F, De Gennaro G, Colizzi L, Convertini N, "Improving the Healthcare Effectiveness: The Possible Role of HER", IoMT, and Blockchain. Electronics,2020, Vol- 9,issues-6,pp-884.

[2] Manogaran G, Rawal BS, Saravanan V, Kumar PM, Martínez OS, Crespo RG, Montenegro-Marin CE, Krishnamoorthy S, "Blockchain based integrated security measure for reliable service delegation in 6G communication environment", Comput Commun,2020, Vol- 161, pp-248−256.

[3] Singh P, Singh N, "BlockchainWith IoT andAI:A Review of Agriculture and Healthcare", Int J Appl Evol Comput (IJAEC),2020, Vol- 11, issues-4,pp-13−27.

[4] Manogaran G, Chilamkurti N, Hsu CH, "Emerging trends, issues, and challenges in Internet of Medical Things and wireless networks", Pers Ubiquit Comput,2018, Vol- 22, issues-5-6, pp-879−882.

[5] Jamil F, Ahmad S, Iqbal N, Kim DH, "Towards a Remote Monitoring of Patient Vital Signs Based on IoT-Based Blockchain Integrity Management Platforms in Smart Hospitals", Sensors,2020,Vol-20, issues-8, pp- 2195

[6] Hakak S, Khan WZ, Gilkar GA, Assiri B, Alazab M, Bhattacharya S, Reddy GT, "Recent advances in Blockchain Technology: A survey on Applications and Challenges",2020, arXiv preprint arXiv: 2009.05718.

[7] Xiong Z, Zhang Y, Luong NC, Niyato D, Wang P, Guizani N, "The best of both worlds: A general architecture for data management in blockchain-enabled Internet-of-Things", IEEE Netw,2020, vol- 34, issues-1, pp-166−173.

[8] Muthu B, Sivaparthipan CB,Manogaran G, Sundarasekar R,Kadry S, Shanthini A, Dasel A, "IOT based wearable sensor for diseases prediction and symptom analysis in healthcare sector", Peer-to-peer Netw Appl ,2020, pp-1−12.

[9] Satamraju KP, "Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare", Sensors,2020, Vol- 20, issues-5, pp- 1389.

[10] Al-Turjman F, Zahmatkesh H, Mostarda L, "Quantifying uncertainty in internet of medical things and big-data services using intelligence and deep learning", IEEE Access,2019, Vol-7, pp-115749−115759.

[11] Singh S, Sharma PK, Yoon B, Shojafar M, Cho GH, Ra IH, "Convergence of blockchain and artificial intelligence in IoT network for the sustainable smart city", Sustain Cities Soc,2020, vol-63, pp-102364

[12] Jing Z, Gu C, Li Y, Zhang M, Xu G, Jolfaei A, Shi P, Tan C, Zheng X, "Security analysis of indistinguishable obfuscation for internet of medical things applications", Comput Commun,2020,Vol- 161, pp-202−211

[13] Abou-Nassar EM, Iliyasu AM, El-Kafrawy PM, Song OY, Bashir AK, Abd El-Latif AA, "DITrust Chain: Towards Blockchain-Based Trust Models for Sustainable Healthcare IoT Systems", IEEE Access ,2020, vol-8, pp-111223−111238.

[14] Shi S, He D, Li L, Kumar N, Khan MK, Choo KKR, "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey", Comput Secur,2020, 101966

[15] YánezW,Mahmud R, Bahsoon R, Zhang Y, Buyya R, "Data Allocation Mechanism for Internet-of-Things Systems With Blockchain", IEEE Internet Things J,2020, vol- 7, issues-4, pp-3509−3522.

[16] Le Nguyen B, Lydia EL, ElhosenyM, Pustokhina I, Pustokhin DA, Selim MM et al, "Privacy Preserving Blockchain Technique to Achieve Secure and Reliable Sharing of IoT Data", CMC Comput Mater Continua,2020, Vol- 65, issues-1, pp-87−107.

[17] Bisis S, Sharif K, Li F, Mohanty S, "Blockchain for ehealth- care systems: Easier said than done", Computer,2020, Vol- 53, issues-7, pp-57−67

[18] Thota C, Sundarasekar R, Manogaran G, Varatharajan R, Priyan MK, "Centralized fog computing security platform for IoT and cloud in healthcare system", In Fog computing: Breakthroughs in research and practice, IGI global,2018, pp 365−378.

[19] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", Tech. rep., Manubot ,2019.

[20] F. Casino, T. K. Dasaklis, C. Patsakis, "A systematic literature review of blockchain-based applications: current status, classification and open issues", Telematics and informatics, 2019, vol-36.

[21] Luis, B. C. J., Frank, M. A., & Ole, L. (2018), "Public health surveillance using decentralized Technologies", Blockchain in Health Care Today, vol-1, 1e14, 2018, https://doi.org/10.30953/bhty.v1.17.

978-1-6654-9515-8/$31.00©2022IEEE

[22] Saba T, Haseeb K, Ahmed I, Rehman A, “Secure and energy efficient framework using Internet of Medical Things for e healthcare”, J Infect Public Health, 2020, vol- 13, issues-10, pp-1567−1575.

[23] Sharma A, Tomar R, Chilamkurti N, Kim BG, “Blockchain Based Smart Contracts for internet of Medical Things in e-Healthcare”, Electronics,2020, vol- 9, issues-10, pp-1609.

[24] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016.

[25] R. Lokeshkumar, E. Maruthavani, and A. Bharathi , A new perspective for decision makers to improve efficiency in social business intelligence systems for sustainable development, International Journal of Environment and Sustainable Development 2018 17:4, 404-416.

[26] S. Balakrishnan, V. K. and M. S. S. Hameed, "An Embarking User Friendly Palmprint Biometric Recognition System with Topnotch Security," 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), 2021, pp. 1028-1032, doi: 10.1109/ICICCS51141.2021.9432230.

[27] V. Arulkumar A Survey on Multimedia Analytics in Security Systems of Cyber Physical Systems and IoT, 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) pp 1556-1561, Nov 2021. 10.1109/ICOSEC51865.2021.9591754

[28] Ravi Kumar Poluru & Lokesh Kumar R (2021) An Improved Fruit Fly Optimization (IFFOA) based Cluster Head Selection Algorithm for Internet of Things, International Journal of Computers and Applications, 43:7, 623-631, DOI: 10.1080/1206212X.2019.1600831

[29] Selvan.C, S.R.Balasundaram, (2020), Data Analysis in Context Based Statistical Modeling in Predictive Analytics, IGI Global, Handbook of Research on Engineering, Business, and Healthcare Applications of Data Science and Analytics, pages 98-114.

[30] V. Arulkumar An Intelligent Face Detection by Corner Detection using Special Morphological Masking System and Fast Algorithm, 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC) pp 1556-1561, Nov 2021.

[31] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher and F. Wang, "Secure and trustable electronic medical records sharing using Blockchain," in AMIA Annual Symposium Proceedings., 2017.

[32] Zeng Chen,Weidong Xu,Hua Yu"A blockchain-based preserving and sharing system for medical data privacy", Future Generation Computer Systems, 2021.

[33] Renpeng Zou,Xixiang Lv,Jingsong Zhao,"SPChain: Blockchain-based medical data sharing and privacy-preserving eHealth system", Information Processing & Management, 2021.

[34] Geetanjali Rathee, Ashutosh Sharma, Hemraj Saini, Rajiv Kumar & Razi Iqbal , "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology", Multimedia Tools and Applications, 2020.

[35] P. S. G. Aruna Sri,D. Lalitha Bhaskari,"Blockchain technology for secure medical data sharing using consensus mechanism", Materials Today: Proceedings, 2020

[36] Yi Chen, Shuai Ding, Zheng Xu, Handong Zheng & Shanlin Yang , "Blockchain-Based Medical Records Secure Storage and Medical Service Framework", Journal of Medical Systems , VOl.43, 2019.

978-1-6654-9515-8/$31.00©2022IEEE