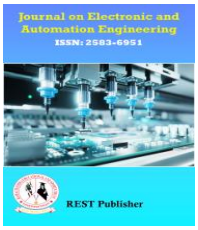
DOI: https://doi.org/10.46632/jeae/1/2/9

Journal on Electronic and Automation Engineering

Vol: 1(2), 2022

REST Publisher; ISSN: 2583-6951

Website: https://restpublisher.com/journals/jeae/



Building Privacy Preservation Methods for Internet of Things Healthcare Sector

[*]D. Prasanna, A. Umamaheswari, T. Prasanth, M. Brindha

Mahendra Engineering College, Namakkal, Tamil Nadu, India.

[*]Corresponding author Email: prasanna@mahendra.org

Abstract: *Sensory data of patients can be supplied toward Internet of Things (IoT) accessory in real-time, where it has been assessed and controlled in the health care management sector. The health data security and confidentiality from patients has increasingly critical concern for IoTs device in extensive and different product industries. Based on earlier study, Blockchain Technology (BCT) is being shown to be a significant solution to the concerns about data security that arise in IoT. However, this paper introduced Hyper Elliptic Curve Cryptography (HECC) influenced with Dynamic Permutation with Multi-Modal Safe Data (DPMMSD) is determined as (HECC-DPMMSD) method in the security accessibility as well as patient data regulation in the IoT. Therefore, the proposed architecture for Medical Data Management (MDM) in IoT devices is effectively used to meet the highest confidentiality and safety standards. The Blockchain (BC) technique was employed in this research for generating a trustworthy and secure data exchange stages linking various source data while encrypting as well as recording IoT data over distributed ledger. The study about security in smart healthcare has discovered that specific data security parameters associated to the HECC-DPMMSD method to analyze data as well as securing the confidentiality of essential data from all sources. The recommend technique is assessed against two dataset benchmark datasets are Heart Disease Data Set (HDD) and Breast Cancer Wisconsin Data Set (BCWD). Thus, the simulation findings demonstrated the suggested HECC-DPMMSD method is outperforms all kind of strategies over several encryption methods.*

Keywords: *IoT, Privacy, Security, Healthcare systems, Elliptical curve cryptography, HECC-DPMMSD*

1. INTRODUCTION

The major aim of Healthcare's is to enhance the life quality of each people by improving their health as well as their progress in service providence [1]. Patient care refers to the rehabilitation, protection, avoidance, and organization of mental and physical wellbeing for healthcare professionals [2]. In the healthcare sector, patient data management requires creating a functional data structure performs as the fundamental in data accessibility and centralized management [3]. For example, it requires that data from various healthcare fields be gathered, logged in, encoded, output examined, recovered, and preserved. The IoT category includes advanced technology such as health surveillance as well as sensors that have been developed specifically application within healthcare business at residence in the community for clinical and hospital settings, tele-health, as well as additional benefits [4]. The foundation of IoT communications from machine to machine using Wi-Fi enabled healthcare devices [5]. IoTs allows sensors in preserving critical data as well as then deliver it to clinicians for real-time follow-up with patients [6]. Applications for smartphones along with other linked devices might notify nurses and physicians to potential security risks and urgent circumstances [7]. Several medical organizations' infrastructures are not stable or sufficiently secure to accommodate IoT devices. Due to the enormous amount of data transmitted, clinicians might experience trouble obtaining patient records when needed, resulting in bottlenecks [8]. The Internet of Things is utilized for determining BC Network (BCN) in patient-centered services. Usually registered individuals with computers are allowed accessing in IoT devices associated with the sensory healthcare section. Patient's portal, computerized medical data and smartphone applications are commonly used by healthcare workers [9]. Cloud storage enables healthcare facilities to store all of their data whilst minimizing the cost of computer maintenance [10]. IoT data gets stored as texts in blocks, whereas patient information is kept within blocks known as Inter Planetary File Systems (IPFS) [11]. The entire medical data of patient's are saved on every node in the BCN, resulting in data bandwidth and storage addresses [12].

IoT-enabled smart healthcare networks face major risks and security problems [13]. Cryptographic techniques are critical for securing the Internet of Things ecosystem. Techniques are deployed to ensure that the CIA receives the information transferred across networks. Cryptographic algorithms are employed in Internet security for protecting data and inhibit unauthorized access, secure data integrity by identifying changes during transmission, and deliver authentication ensuring only authorized users to access data. Cryptography is a technical method of preserving data safe when it is transmitted across a network through the use of data encryption methods. A variety of encryption technologies are utilized for secure networks.

The three major types are

1. Asymmetrical algorithms
2. Symmetrical algorithms
3. Cryptography protocols

The number of keys used distinguishes asymmetric algorithms that utilized both private as well as public keys from symmetric algorithms that utilize distinct keys to encrypt and decrypt data. Private keys have employed to decryption, while public keys have utilized to encrypt. Since these methods are critical for data security, they require a significant amount of memory, time for Central Processing Unit, as well as battery power. Keys have utilized determines the security of symmetric key encryption. In instance, RC2 utilizes a 64-bit key, while DES employs a 64-bit key, Triple DES (3DES) employs two set of 64-bit keys. Moreover, the AES and RC6 are capable of using keys that have a bit counts among 192, 128, and 256 bits, while blowfish may employ keys of all sized among 32448 bits [14]. Cryptography provides a foundational layer for data security and services. Thus, the fundamental architecture of the cryptography algorithm, as well as its accompanying technology functionalities is critical concerns. This work proposes HECC-DPMMSD enhanced data flow along with secure access management over patient data. Sensor feedback from patients can be obtained from IoT devices and analyzed in real time to handle healthcare. Security and privacy of medical data from patients have prominent apprehension for IoT devices to various categories of products. The application of BC in IoT development for HECC-DPMMSD is recommend in this research. The proposed system is easy to deploy and fulfills the highest security and privacy standards for processing IoT data. Healthcare application network is using a BC key for maintaining patient health data, which can then be confidentially utilized for communicating vital messages to verified healthcare professionals.

2. LITERATURE REVIEW

Finally, to address interoperability issues in the health industry, the BCN based on decentralized data storage frameworks as well as Cosmos architecture, such as BigchainDB as well as IPFS, is proposed. Tanzila Saba et al., have proposed security as well as energy efficient infrastructure to e-healthcare. Based on the Medical Internet of Things (MIoTs), wireless networks in the body offer an important part in medical treatments [15]. They monitor patients' well-being and relay data to remote healthcare centers so that appropriate steps can be done. However, due to the limited sensor abilities, the data transportation system must be both energy efficiency and accurate. In addition, confidential information about patients is more vulnerable to threats, endangering security of data. This paper suggests e-health approach is both economical and secured using MIoT to decrease energy consumptions while providing high information for medical experts on a consistent basis. Ashutosh Sharma et al. have proposed smart contracts with BC as MIoT architecture for e-healthcare. Smart BC contracts are pre-coded diminutive scripts will eliminate intermediaries as well as enhancing contract performance [16]. The study investigates the degree of MIoT decentralization as well as using intelligent contracts over e-healthcare provides an existing design, as well as evaluates the merits and downsides of integrating it as well as future improvements. BCT is crucial in healthcare because it provides trust, security, and authenticity for all parties. Nao et al. have evaluated three IoT security algorithms and compared them based on security considerations. According to the study's findings, ECC is the most efficient of the approaches. The scientists remained available the prospect of preventing access towards IoT devices through the use of asymmetrical strategies to aid in the difficult development of cryptography [17]. Meshram et al. have proposed a robust authentication scheme to IoT-based smart cities which enables secure resource managements as well as communications. The suggested protocol employs large chaotic maps for enhanced security as well as mitigates various forms of assaults. Its reliability as well as effectiveness in password authentication of smart card has been established through verification of BAN logic [18]. Rahul Saha et al. have presented a bilinear map process method in IoT security. Aggregating sign has utilized to increase network performance, while time stamps get utilized during the process of key generation [19]. The proposed solution has been designed for use in the IoT architecture with fog region. The technique results have been comparing with current processes and the contrast shows that the suggested

method is effective in IoT applications. Moreover, Tarandeep Singh et al., have proposed a new encryption as well as steganography approach which employs less complex in Elliptic Galois Cryptography (EGC) for IoT security [20]. The matrix XOR steganography is used in conjunction with EGC. Numerous trials demonstrate that EGCrypto beats competing models across a variety of metrics. F uture work on this will focus on improving EGCs effectiveness as well as safety towards advanced IoT attacks. Reji Thomas et al. have suggested authentication protocol in IoT security which relies on LiSP encryption. It employed two lightweight cryptography modules with efficient features [21]. The testing revealed that LiSP-XK is 35% more efficient than other encryption techniques. The authors' remaining research focuses on a distributed key generation process.

3. RESEARCH METHODOLOGY

The present research investigated the IoT use in healthcare sector to the security of patient records as well as fault prevention of data transmission. The IoT presents a platform for physical and medical testing, collection of data, and analysis. The data collected is securely stored over cloud-based systems. IoT in the healthcare industries currently includes patient data transmission, data integration, and Internet-connected devices for healthcare security. As an outcome, the HECC-DPMMSD Framework is being created in the present research to optimize flow of data and patient data access management while maintaining safety. The proposed HECC-DPMMSD framework is illustrated in Figure 1. The MDM are gaining popularity between IoT system that allows for real-time collection, storage, and transmission of data from devices like monitoring heart rate, wearable gadgets and body sensor through an Internet. When technology progresses have providers may eventually be allowed in undertaking the data analysis concurrently along with sharing the results to those who possess access to data using the BC and IoT. Employing a supplement processor generally in permanent services, the individual will function as a data pathway in all data, which leads to massive amounts of data. Intelligent systems may interact with created data, processing essential data and, when necessary, adding it to BC. As intended, it results in a fully vertically integrated gadget that can be secure and always accessible. In IoT, BCT enables an encrypted real-time solution for patient monitoring. BCT is currently used to exchange legitimate data. To create an intriguing technology enabling health surveillance using an inherent distinction among border as well as core networks, allowing for both centralized and decentralized communication of information methods. This framework demonstrates greater scalability with proficiency for a BC system, especially when dynamic data is considered.

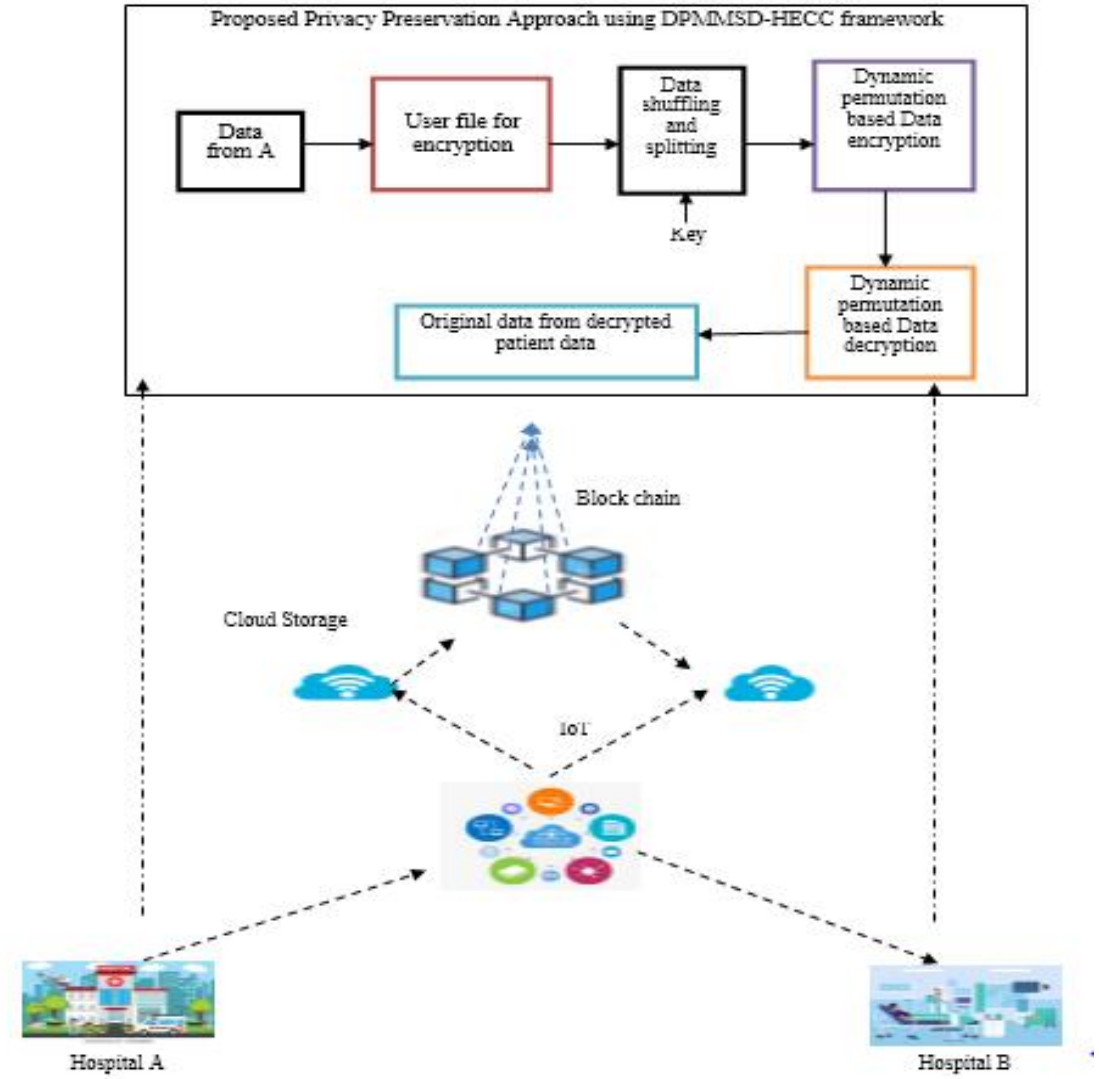


FIGURE 1. Proposed architecture for privacy preservation in smart healthcare

The present research combines two encryption methods, especially asymmetric algorithms in both plaintext (E) as well as ciphertext decryption (D) with asymmetric algorithms using distinct keys in E encryption as well as D. In general, data gets encrypted with a BC block node's public key as well as decrypted with BC block node's private key. In this proposed framework, sender A initially intends to deliver the entire original file to Receiver A using the cloud. Applying a dynamic permutation key, every element of the initial record is capable of being arbitrarily scrambled, and that scrambled record may then be separated into a several subfiles known as sectors. This approach allows the initial text to be split down into 64-bit chunks. Every block encompasses 64 data bits that divided towards two 32-bit half. SLeft and SRight is the left and right subblocks correspondingly. Sub-patterns like B1, B2, B3, and B4 are formed using these sub-blocks. These sub patterns is known as the Inter-bit Exchange and Merge (IbEM) pattern are made by combining odd bits digits (B_o) and even bits digits (B_e). Consider the data owners for A and B, both of these has public clouds. Owner's of each data is responsible for their individual personal data. When the owner A wished for data transfer to owner B's endure, they might employ the public key for sending the complete records as original data. In this case, the number of words in the original data might be employed for creating a randomized file having dynamic permutations. The randomized file is subsequently separated into numerous sectors by random keys. Resources with data transmission in sectors are selected at random applying either by Multi-Model IBEM or HECC techniques. This method involves four main process are

1. Data Ecryption Process (DEP)
2. Data Randomization and Splitting (DRS)
3. Multi-Modal Dynamic Permutation (MMDP) for data encryption
4. Multi-Modal Dynamic Permutation (MMDP) for data decryption

DEP

Sender 'A' has cluttered Data File (D_F) into SHUFF (D_R) for generating randomized file by assigning public key for user A (PU_{KA}) to the user domain A with the original file as entire input for D_F. Thus, the proposed method of data encryption is segregated into the subsequent categories are

- Splitting and randomizing data
- MMDP is utilized for encrypt data
- Decryption of data using MMDP

DRS

Assume that complete file has considered as D_F. SHUFF represent the term provided for randomized the D_F. Once the file get randomized, the number of words appeared is accumulated. Number between 1 and 5 are made picked randomly and splitting the data file as SD_F has been created using splitting the randomized file by earlier generated random number as well as creating a recent file.

MMDP for data encryption

Data transformation is initiated from data owner A to data owner B whereas the data owner A has submitted the complete original data file along with its public key PU_K. The public key is shared to both owner A and owner B as well as the files is made encrypted once the process is initiated.

MMDP for data decryption

When the owner B need to decode a file provided from data owner A, the file is received with the encrypted data along with private key represented as PR_K. The process MMDP assist in decrypting the data file from the encrypted data provided from the earlier process named MMDP for data encryption.

4. RESULT AND DISCUSSION

The experimental work used two credible dataset parameters of HDD as well as BCWD, for assessing the technique in this investigation. Parameters of BCWD have been established using a scanned image of a LED probe placed into a breast dense. Additionally, it identifies the cell nuclei appearance in the image. Each instance involves a mixture of mild as well as severe. Similarly, HDD comprises 13 numerical advantages in classifying each case according to the degree to which they have Coronary Artery Disease. In order to prevent any unexpected or different effects, the common consequences of recognizing each other of ten contracts are measured and evaluated with proposed method. The dataset have divided into both testing as well as training halves in investigation employing a 10-fold cross validation method. In the current study, each IoT data source acquired every record from IoT devices in the region it served and then employed that data to deliver the subsequent services like data encryption and data decryption within the BCT. HECC-DPMMSD is BC-based IoT system for securing access to and controlling the patient's data using python libraries with google colab environment.

The two prevalent criteria for ML classification evaluations are broadly agreed. Table 1 and Figure 2 show the precision analysis of HECC-DPMMSD method using comparative methodologies on the two dataset namely HDD as well as BCWD. Based on the table results, the proposed HECC-DPMMSD method acquired the highest precision values as 93.04% in the BCWD dataset and 95.78% in the HDD dataset. In the case of Ant Colony Optimization (ACO) method, BCWD and HDD datasets is calculated and evaluated with proposed method and it achieves slightly lower precision values as 92.42 % and 94.12%. Simultaneously, the SVM method has performed inadequately performance in HDD as well as BCWD datasets with precision 91.56% and 93.21% respectively.

TABLE 1. Comparison of proposed and existing precision value

Dataset Used	SVM	ACO	DPMMSD-HECC
BCWD	91.56%	92.42%	93.04%
HDD	93.21%	94.12%	95.78%

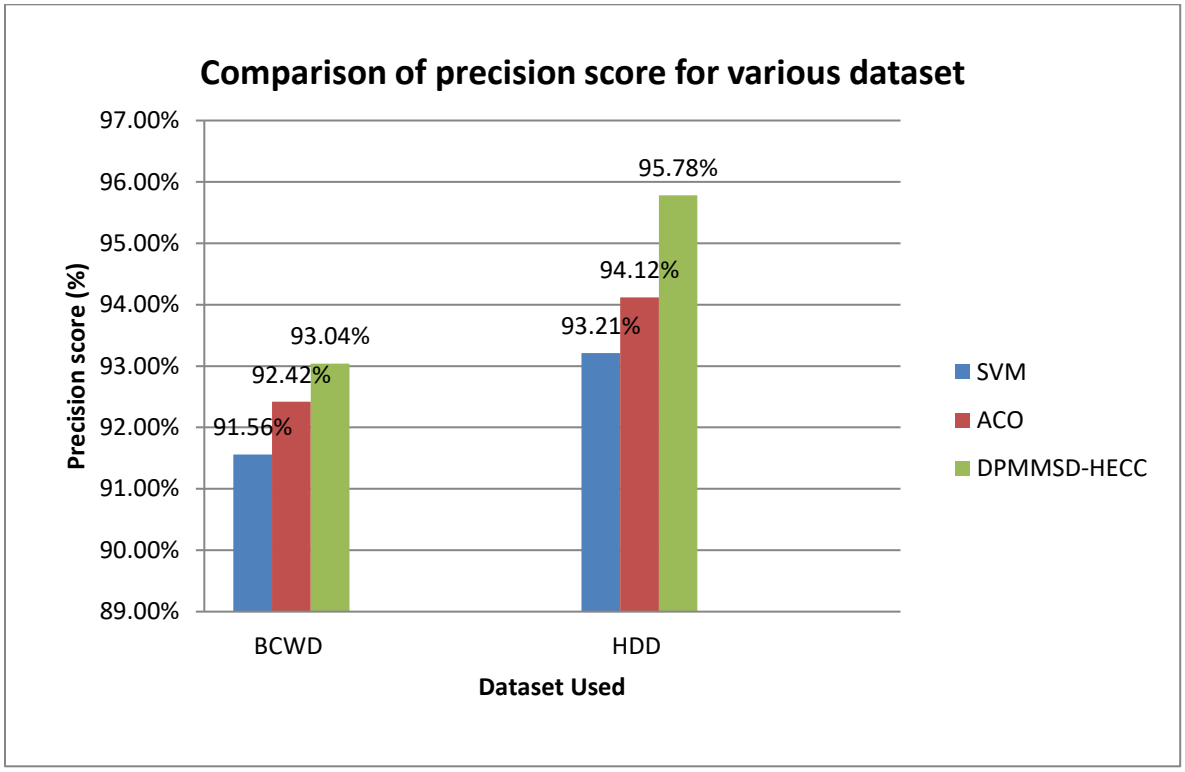


FIGURE 2. Comparison of proposed and existing precision

Table 2 and Figure 3 provides recall or true positive rate for the current study with proposed HECC-DPMMSD method is involved for these two dataset namely HDD as well as BCWD. HECC-DPMMSD method suggested higher recall values as 93.44% and 96.62% in BCWD and HDD datasets respectively. The accessible ACO technique generate slightly lesser than proposed method recall values on the dataset HDD as well as BCWD with 92.18% and 94.67% respectively. Simultaneously, the SVM method has performed inadequately performance HDD and BCWD datasets involves least recall values 90.42% and 92.58% correspondingly.

TABLE 2. comparison of proposed and existing recall value

Dataset Used	SVM	ACO	DPMMSD-HECC
BCWD	90.42%	92.18%	93.44%
HDD	92.85%	94.67%	96.62%

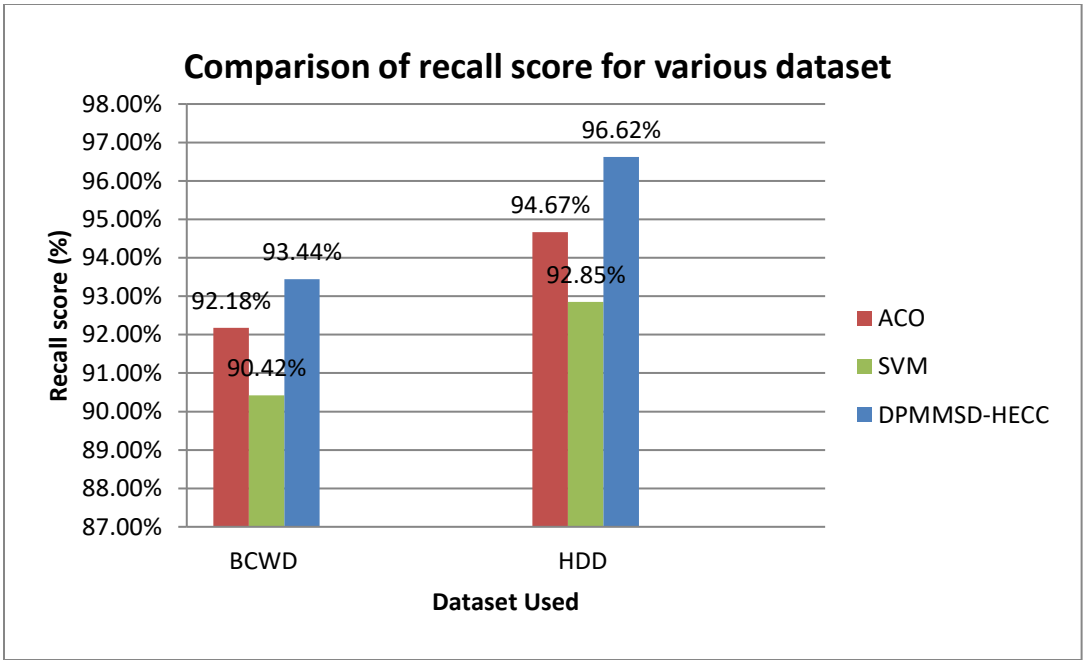


FIGURE 3. Comparison of proposed and existing recall

5. CONCLUSION

Since healthcare is such a vital component of our everyday lives, clinical evidence including prescriptions and previous clinical records are crucial in determining an individual's diagnosis and subsequent therapy. The health database can be completely modified or deleted. The data that is stifling is a problem. Data is forbidden because an individual could not permit to provide access to data that ought not to have been seen absent the patients' or hospitals' authorization. The present paper examined all possible applications of BCT with IoT devices to better medical care and data management. In conclusion, BC increases the data security and data privacy by encrypting data and enabling solely the patient's with private key has employed for decryption. The proposed method efficiency has evaluated with two datasets from the UCI repository are HDD as well as BCWD. The experimental results demonstrated that the DPMMSD-HECC method assaulted the other approaches with regard to of precision and recall across all datasets. The proposed method might be developed into an architecture that could be utilized in the future for building a range of ML training methods that maintain confidentiality in a variety of encrypted data processes.

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]. 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

[5]. 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.

[6]. 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.

[7]. 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.
[8]. Satamraju KP, "Proof of Concept of Scalable Integration of Internet of Things and Blockchain in Healthcare", Sensors,2020, Vol- 20, issues-5, pp- 1389.
[9]. 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.
[10]. 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
[11]. 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.
[12]. 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.
[13]. 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
[14]. Thakor, Vishal A., Mohammad Abdur Razzaque, and Muhammad RA Khandaker. "Lightweight cryptography algorithms for resource-constrained IoT devices: A review, comparison and research opportunities." IEEE Access 9 (2021): 28177-28193.
[15]. 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.
[16]. 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.
[17]. Duan, Xintao, Daidou Guo, Nao Liu, Baoxia Li, Mengxiao Gou, and Chuan Qin. "A new highcapacity image steganography method combined with image elliptic curve cryptography and deep neural network." IEEE Access 8 (2020): 25777-25788.
[18]. C. Meshram, R. W. Ibrahim, L. Deng, S. W. Shende, S. G. Meshram, and S. K. Barve, "A robust smart card and remote user password-based authentication protocol using extended chaotic maps under smart cities environment," Soft Comput, vol. 25, no. 15, pp. 10037–10051, Aug. 2021, doi: 10.1007/s00500-021-05929-5.
[19]. Kim, Tai-Hoon, Gulshan Kumar, Rahul Saha, Mamoun Alazab, William J. Buchanan, Mritunjay Kumar Rai, G. Geetha, and Reji Thomas. "CASCF: Certificateless aggregated signcryption framework for internet-of-things infrastructure." IEEE Access 8 (2020): 94748-94756.
[20]. Kaur, Manjit, Ahmad Ali Alzubi, Tarandeep Singh Walia, Vaishali Yadav, Naresh Kumar, Dilbag Singh, and Heung-No Lee. "EGCrypto: A Low-Complexity Elliptic Galois Cryptography Model for Secure Data Transmission in IoT." IEEE Access (2023).
[21]. Kim, Tai-Hoon, Gulshan Kumar, Rahul Saha, William J. Buchanan, Tannishtha Devgun, and Reji Thomas. "LiSP-XK: extended light-weight signcryption for IoT in resource-constrained environments." IEEE Access 9 (2021): 100972-100980.

