Baghdad Science Journal

Volume 22 | Issue 6 Article 28

6-24-2025

A smart blockchain-based privacy-preserving machine learning scheme in IoT healthcare

J. Deepika
Department of Information Technology, Sona College of Technology, Salem

Sahana Shetty
Department of CSE-AIML and Cyber Security, School of CSE, FET – Jain, Jayanagar, Bangalore, India

A. Selvarani
Department of ECE, Panimalar Engineering College, Chennai, Chennai, Tamil Nadu, India

Saroj Bala
Department of MCA, Ajay Kumar Garg Engineering College, Ghaziabad, India

Benita Gracia Thangam J
Department of AI & DS, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India

See next page for additional authors

How to Cite this Article

Deepika, J.; Shetty, Sahana; Selvarani, A.; Bala, Saroj; J, Benita Gracia Thangam; and G, Pradeep (2025) "A smart blockchain-based privacy-preserving machine learning scheme in IoT healthcare," *Baghdad Science Journal*: Vol. 22: Iss. 6, Article 28.
DOI: https://doi.org/10.21123/2411-7986.4978

A smart blockchain-based privacy-preserving machine learning scheme in IoT healthcare

Authors

J. Deepika, Sahana Shetty, A. Selvarani, Saroj Bala, Benita Gracia Thangam J, and Pradeep G

BAGHDAD SCIENCE JOURNAL 2025;22(6):2086–2098

Scan the QR to view the full-text article on the journal website

RESEARCH ARTICLE

A Smart Blockchain-Based Privacy-Preserving Machine Learning Scheme in IoT Healthcare

J. Deepika [1,*], Sahana Shetty [2], A. Selvarani [3], Saroj Bala [4], Benita Gracia Thangam J [5], Pradeep G [6]

[1] Department of Information Technology, Sona College of Technology, Salem
[2] Department of CSE-AIML and Cyber Security, School of CSE, FET – Jain, Jayanagar, Bangalore, India
[3] Department of ECE, Panimalar Engineering College, Chennai, Tamil Nadu, India
[4] Department of MCA, Ajay Kumar Garg Engineering College, Ghaziabad, India
[5] Department of AI & DS, Bannari Amman Institute of Technology, Sathyamangalam, Erode, Tamil Nadu, India
[6] Department of M.Tech. Computer Science and Engineering, Sri Krishna College of Engineering and Technology, Coimbatore, India

ABSTRACT

The idea of Blockchain has infused various fields of study, and its widespread adoption is projected to grow exponentially in the near future. By executing concise pre-defined code snippets known as smart contracts on the Blockchain, the need for intermediaries can be eliminated, and the number of contract executions can be significantly increased. The application of blockchain technology and smart contracts, in conjunction with machine learning methods, to IoMT-based e-healthcare is critically examined in this article. The goal of this project is to investigate how automation and decentralisation might improve healthcare. Integrating these components offers the chance to handle medical data securely, privately, and transparently while facilitating easy communication between patients, healthcare professionals, and insurers. A special architectural model designed for the Internet of Medical Things (IoMT) in e-healthcare is suggested to illustrate the aforementioned problem. In order to improve effectiveness, dependability, and scalability in medical settings, this paradigm makes use of decentralisation and smart contracts. The paper also addresses the approach's possible advantages, difficulties, and upcoming developments. Empirical data highlights the potential of the suggested architecture to transform the delivery of medical services by demonstrating its superiority over conventional approaches, especially in terms of packet delivery, latency, and energy efficiency.

Keywords: Block chain, Encryption, Internet of things, Medical data, Privacy

Introduction

The healthcare sector has embraced information technology through the use of Electronic Health Records (EHR), population health management systems, and remote patient monitoring. However, the surge of cybercrime has resulted in uncontrolled databases, jeopardizing medical accuracy and patient privacy. Patient data is crucial from the beginning of the disease until recovery, and it must be protected from unauthorized access. Integrating blockchain technology provides a solution that improves data security and privacy.[1] By implementing access limits using smart contracts, only authorized users may interact with EHRs, protecting both individual privacy and data integrity. Furthermore, blockchain enhances trust and transparency by allowing parties to share safe data.[2]

Blockchain is a decentralised digital ledger system that records transactions in an open, secure, peer-to-peer network.[3] With transactions grouped into blocks and added to the chain chronologically, each

Received 18 October 2023; revised 7 June 2024; accepted 9 June 2024.
Available online 24 June 2025

* Corresponding author.
E-mail addresses: deepikamohan16@gmail.com (J. Deepika), s.sahana@jainuniversity.ac.in (S. Shetty), selvaraninaac2022@gmail.com (A. Selvarani), saroj.chhokar@gmail.com (S. Bala), benitagraciathangam@bitsathy.ac.in (Benita Gracia Thangam J), pradeepg@skcet.ac.in (Pradeep G).

https://doi.org/10.21123/2411-7986.4978

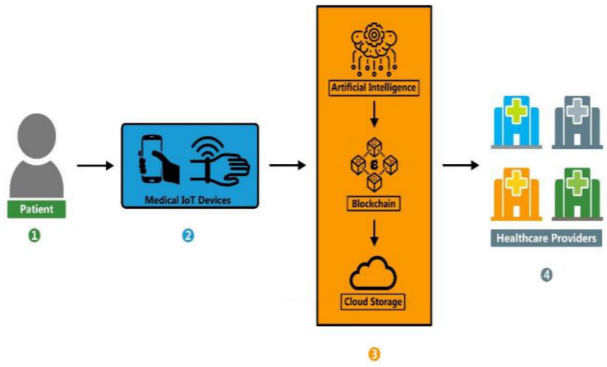

Fig. 1. Blockchain infrastructure.

participating node has a copy of the whole ledger, resulting in an immutable and impenetrable record. Blockchain technology's major properties are decentralisation, transparency, immutability, and cryptography-based security.[4] Blockchain has the potential to radically impact a range of sectors outside bitcoin by improving security, promoting trust, and speeding up procedures in banking, real estate, supply chain management, healthcare, and other areas.[4,5] Fig. 1 depicts the block chain infrastructure. The application of machine learning techniques in the proposed plan has a significant impact on the medical services industry. Here, machine learning is widely applied to a range of activities, including as personalised treatment recommendations, help with diagnosis, and predictive analytics. Algorithms may be used to analyse vast amounts of healthcare data, including genetic data, imaging data, and patient records, to identify patterns and relationships that may not be immediately apparent to human observers.[6,7] Predictive models can help with early sickness detection and risk assessment, leading to proactive and customised therapy. Furthermore, ML algorithms can accelerate administrative operations, improve decision-making in healthcare settings, and optimise resource allocation. Machine learning methods frequently improve patient outcomes and the overall efficacy of healthcare delivery by making medical services more efficient, data-driven, and personalised.[8,9]

This section investigates the notable differences observed in the setups and applications of various blockchain networks, focusing on how decentralized healthcare implementation mechanisms are shaped by a variety of factors such as modern architecture, device designs, protocols, processes, schemes, platforms, and algorithms.[10,11] As blockchain technology is introduced into healthcare, a number of issues arise that need a thorough evaluation of viable solutions in order to meet system standards. The article assesses the benefits and downsides of merging blockchain technology with healthcare. By delving into these areas, the section contributes to a comprehensive understanding of the challenges and opportunities.[12,13]

One issue is that patients do not have control over access policies for their private information. Patients are typically denied control over data storage and access rights under current blockchain-based schemes.[14,15] As a result, a proposed framework introduces a blockchain-based access control architecture that is user-centric, entirely distributed, and functional. This design aims to empower patients by eliminating the need for a dependable third party and providing them entire control over their medical information through a user-managed IoT Healthcare Manager (IHM).[16,17]

The main contributions of this research are

1. Proposed Framework that enables users to set access policies for their sensitive data, ensuring it remains unpublished on the BC network without explicit user consent. In contrast to many BC-based initiatives, data is stored locally on a machine near the data owner, akin to edge computing, minimizing delays and communication overhead.
2. Proposed Framework utilizes two chains–the data chain for storing patient health data and the access control chain for patient-defined access policies within a private blockchain. Data confidentiality is maintained by storing the hash of patient data in the data chain. Simultaneously, patients manage access to their data by storing access policies in the access control chain, ensuring the preservation of data owner's access policies and controlled data access.
3. Proposed Framework adopts a novel clustering strategy to boost BC network throughput and scalability. Unlike the traditional Cluster Head (CH) model, Proposed Framework introduces a hierarchical structure. The first two bytes of data packets are allocated to the cluster number, allowing each cluster member to easily identify the associated cluster upon receiving a data packet. The rest of the paper is organized as follows. Section 2 explains the Overview of Machine Learning and Block Chain. Section 3 presents the Use of Machine Learning and Blockchain in Healthcare, while Section 4 describes the proposed architecture in detail. Section 5 evaluates the Results and Discussion, while Section 6 provides the conclusion.

Overview of machine learning and block chain

Many machine learning techniques function quite well when processing healthcare data inside the Internet of Medical Things (IoMT) architecture. In classification applications, supervised learning algorithms like Random Forests, Decision Trees, and Support Vector Machines are essential because they help with diagnosis, medical picture interpretation, and outcome prediction.[18,19] In unsupervised learning algorithms, patient segmentation, illness pattern detection, and population health analysis are aided by clustering methods like K-Means and dimensionality reduction strategies like Principal Component Analysis.[20] Convolutional neural networks, in particular, are excellent at deep learning algorithms for tasks like medical image analysis, anomaly detection, and meaningful feature extraction from large amounts of complicated healthcare data. According to the report, two important factors that are changing how medical services are delivered within the suggested framework are decentralization and automation.[21] Adoption of blockchain technology ensures a dispersed and secure infrastructure, hence achieving decentralization. By reducing reliance on a single authority, this decentralized approach offers improved security, data integrity, and patient-centric control over medical records.[22,23]

These self-executing contracts enhance efficiency through automated handling of tasks such as patient data access, billing, and insurance claims, minimizing errors and reducing the time and resources required for administrative functions.[24,25] The efficiency gains contribute to cost reduction, particularly in billing and insurance processing, fostering economic efficiency. Additionally, smart contracts operate on a transparent and tamper-resistant blockchain, providing increased visibility and trust among stakeholders while giving patients more control over their healthcare interactions.[26,27] The elimination of intermediaries not only accelerates workflows but also ensures a patient-centric approach, enhancing the overall effectiveness of IoMT-based e-healthcare systems.

Use of machine learning and blockchain in healthcare

In various industrial domains, ML and blockchain technology offers unique advantages and can serve as an effective tool for implementing healthcare systems. However, it is essential to recognize that blockchain might not be the ideal solution for every problem in industrial fields unless decentralization is a fundamental requirement.[28,29] Blockchain applications prove beneficial when decentralization is necessary, such as running an application on a peer-to-peer (P2P) network of computers instead of a single centralized system. While some healthcare applications may not require decentralization, the majority can benefit from a centralized and trusted approach.[30]

It is important to take into account the particular needs and characteristics of the application before deciding whether to combine ML with blockchain technology in healthcare applications. An extensive assessment procedure need to be employed to appraise the possible advantages and disadvantages of integrating blockchain technology within the medical domain. Within blockchain innovation initiatives, a generic methodology for assessing blockchain's feasibility for healthcare applications has been considered. Whether to employ blockchain technology to enhance the security, transparency, and efficacy of medical systems may be determined by decision-makers through a careful examination of the specifications and characteristics of every healthcare application. The healthcare sector may effectively leverage blockchain's potential benefits in terms of decentralisation, data integrity, and immutability when applied prudently and thoroughly.[31]

Blockchain technology and machine learning may be combined to enhance healthcare systems and guarantee data privacy, traceability, and integrity. The training set required for machine learning models may be preserved while transferring ownership and control of data in a secure manner thanks to blockchain technology. Without jeopardising patient privacy, decentralised machine learning models built on encrypted patient data might benefit medical research.[32] Examine the moral and legal ramifications of using blockchain and machine learning into healthcare administration systems. To address privacy concerns and patient data management on public blockchains, two essential privacy-focused components that must be incorporated are zero-knowledge proofs and data-minimization-focused smart contract designs. Strong consent procedures, decentralised identity systems, and regulatory compliance are essential for protecting patient privacy.[33]

ML combined with blockchains offers potential answers to these problems. Blockchains' tamper-proof and secrecy features guarantee safe and transparent records of public transactions, complete with timestamps that are accessible to the public and verifiable by all stakeholders. This feature ensures that every transaction in a blockchain network is properly reviewed and followed up on, making it extremely useful for health applications. Furthermore, blockchain's

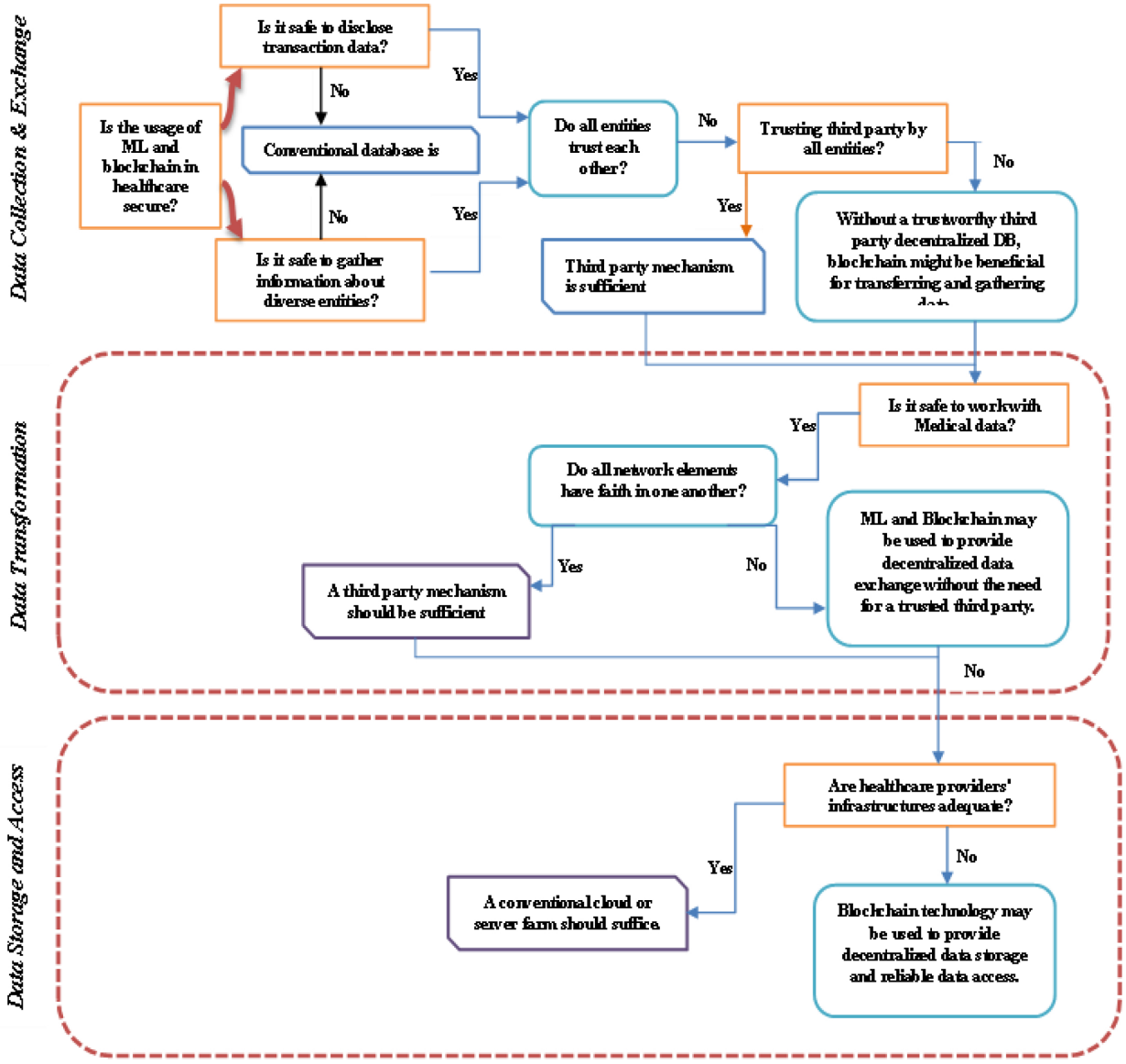

Fig. 2. ML and block chain usage in healthcare sector.

peer-to-peer connection makes it possible for parties and industrial processes to share data easily, which is vital for Electronic Health Record (EHR) systems where teamwork is required. The application of block chains in healthcare is seen in Fig. 2.

By automating procedures, smart contracts cut out middlemen and increase productivity. Sensitive health data is protected by blockchain's privacy protections, while its transparency makes audits easy and builds confidence throughout the healthcare system. All things considered, blockchain technology lays the groundwork for an IoMT-based e-healthcare infrastructure that is safer, more patient-centered, and compatible with other systems. Furthermore, the distributed nature of blockchains contributes to system efficiency and robustness. Implementing blockchain alternatives for cloud-based applications and equipment networks can meet diverse needs. However, challenges may arise due to organizational confusion regarding system ownership, such as in the case of cloud service providers, and meeting client privacy requirements.[34] In such cases, trust agencies must be accredited to ensure secure and reliable services. By leveraging blockchains, the healthcare industry can overcome various challenges related to security, transparency, and efficiency, unlocking a new era of secure data management and streamlined processes.

Proposed block chain and machine learning based medical IOT framework

The smart healthcare system's architecture, represented in Fig. 3, encompasses multiple security phases from patient registration to discharge. The

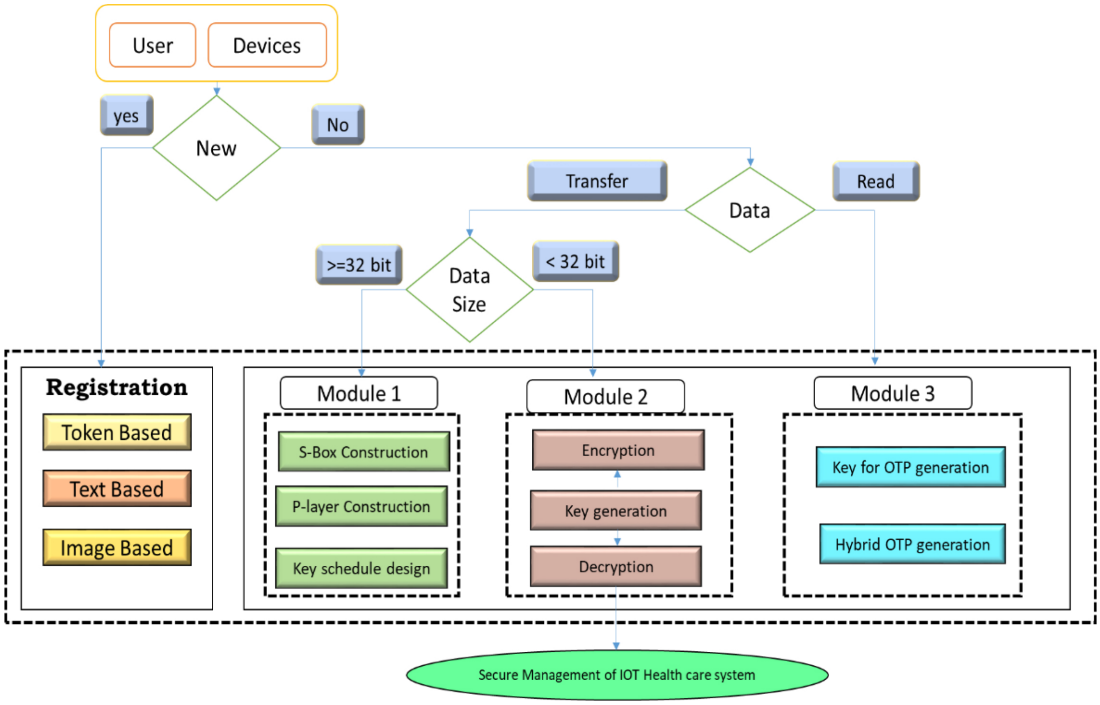

Fig. 3. Architecture diagram of block chain based smart healthcare.

registration process, a one-time procedure following medical and user device installation, offers three types of registration based on text, token, and image inputs.[35] During registration, essential parameters, including Patient ID, Password, and Device Product Code, are collected to uniquely identify and authenticate patients and devices within the system as shown in Fig. 3.

Registration process

Nationality ID (NID): In the Medical Internet of Things (IoT), each person is given a unique Nationality ID (NID), similar to the SSN in the United States or the Aadhaar in India. This ID improves healthcare administration and coordination by increasing the accuracy and efficiency with which patient records and health data are monitored.

Passcode (PC): A passcode is a secret string of characters that users enter to prove their identity. It is also commonly referred to as password. Patients can choose their own passwords within the portal's restrictions, guaranteeing safe access to sensitive information. Users now have greater control over the security and privacy of their accounts.

Device Product Code (DPC): The device product code (DPC) is a 96-bit global identifier designed exclusively for the unique identification of physical things. Its open format allows for simple RFID tag encoding. This identifier is used to monitor assets, documents, and commercial items. Businesses may use the device product code to manage inventory, trace the movement of items, and increase supply chain visibility. This improves logistical effectiveness, lowers losses, and guarantees that assets are well-managed throughout their lifetime.

Text Based Registration: As part of the induction process, any patient who is not associated with the hospital industry needs to be registered. During registration, the patient's National ID (NID) and Patient Code (PC) are obtained. A hidden Patient Unique Number (PUN) is generated when these data points are subjected to a hash function. This PUN serves as the patient's protected and unique identity and is connected to their registration data. All patient data, including NID, PC, and PUN, is securely stored in the cloud application for convenient access and future use.

Step 1: Patient sends NID and PC IoT device for registration
Step 2: IoT device computes PID by combining NID and PC
Step 3: IoT device stores PID, PC, and NID in the Registration Table
Step 4: IoT device sends acknowledgement message to patient and complete the process

Token Based Registration: A medical device must pass through several stages of the registration procedure in order to be accurately identified and seamlessly integrated into the system. The following is a description of the process:

Device Product Code (DPC) and IP Address Collection: When a medical device is inserted into the system for registration, data on its unique IP address and equipment Product Code (DPC) is gathered. The DPC serves as a device-specific unique product identity, while the IP address indicates the device's position within the network.

Generating Device ID (DID): Each piece of medical equipment is assigned a unique equipment ID (DID) based on the IP address and DPC that have been collected. The device ID (DID) is the device's unique system identification.

Storing information in the registration table: The Device Product Code, IP address, and subsequent Device ID (DID) are recorded in the server's registration database, along with other pertinent information. This table lists the characteristics of registered devices, as well as the data linked with them.

Acknowledgement of Successful Registration: Once the medical device's information has been safely placed in the registration table, a confirmation message is shown. This acknowledgment confirms the conclusion of the registration procedure and the device's successful system integration. By using this registration process, each piece of medical equipment is assigned a unique identification and recorded in the system. In the hospital setting, this methodical approach ensures proper communication, comprehensive monitoring, and efficient device administration. The registration procedure is necessary to ensure the integrity and security of the medical device network because it permits authorized access and ongoing communication between devices and the central server. [36]

Step 1: Medical Device sends DPC and IP to server for registration
Step 2: Server computes DPC ack. DPC ack= {substring (DPC, 32, 60)}
Step 3: Server computes DID on DPC. DID= {Hash (DPC ack, IP)}
Step 4: Server stores DPC, IP, DPC ack and DID in the medical device registration table
Step 5: Server sendsregistration success message to medical device and terminates.
Step 6: End

Encryption

Plain text is changed by encryption into an unintelligible format that is only accessible by authorized users. It entails converting data into ciphertext by applying an algorithm and a special encryption key. In order to ensure security, the encryption key is essential to both encryption and decoding.

Key generation

Key distribution and security pose issues in symmetric key cryptography. To prevent communication compromise and interception, parties must securely transfer keys. By using random number permutations in key creation, security is improved by producing unexpected keys that are difficult to intercept during transmission. [37]

By generating keys using random number permutations, cryptographic systems become more resilient against assaults and illegal access. [38] Robust, erratic keys improve communication security by discouraging bad actors. Key generation plays a crucial role in secure symmetric key cryptography, guaranteeing privacy, reducing the danger of dissemination and maintaining secrecy. [39]

Security by isolation

Proven method, [40] isolation-based security, guarantees efficacy over time. Separating equipment physically, however, might result in redundant energy use and higher expenditures. For instance, there are extra costs involved with maintaining two machine versions with different CPUs and memory. Virtualization, on the other hand, offers an alternative solution by achieving logic isolation. This approach provides a degree of isolation without the need for multiple physical devices, thereby reducing costs and complexity. [41] The proposed architectural model optimizes the benefits of decentralization and smart contracts to ensure efficiency, reliability, and scalability in several ways. Firstly, decentralization enhances security and reliability by distributing health data across a network of nodes, minimizing the risk of a single point of failure and providing robustness against data breaches. Patient-centric control is facilitated through decentralized storage, ensuring greater privacy and trust. Smart contracts, operating within the decentralized blockchain, automate processes, such as data access permissions, billing, and insurance claims, leading to increased efficiency by reducing the need for intermediaries and manual interventions.

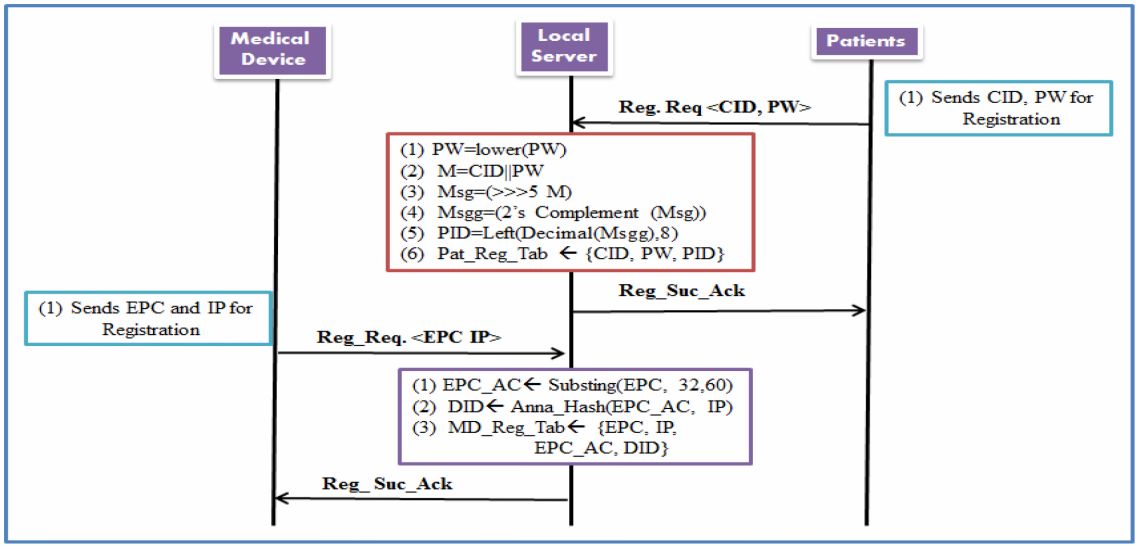

Fig. 4. Process flow diagram.

The transparent and tamper-resistant nature of smart contracts enhances reliability and trust among stakeholders.

However, complete isolation may not always be practical or feasible. This means that some entities must interact with each other, and total segregation becomes challenging. In the context of the Internet of Things (IoT), implementing security by isolation can be particularly complex.[42] Isolation can hinder seamless communication and data exchange between IoT devices, limiting the potential for interoperability and real-time data processing. The process flow diagram of proposed model is shown in Fig. 4. The proposed architectural approach in IoMT-based e-healthcare offers substantial advantages over traditional methods in terms of security, privacy, and communication efficiency. Leveraging blockchain technology ensures heightened security and data integrity, with decentralization minimizing the risk of unauthorized access. Patient-centric control facilitated by smart contracts enhances privacy by allowing individuals to dictate access to their health data. The streamlined communication achieved through decentralized networks, coupled with automated processes, significantly reduces delays and overhead, improving efficiency, particularly in time-sensitive healthcare scenarios. The tamper-resistant nature of blockchain transactions adds an extra layer of reliability, and the adaptable, scalable architecture ensures optimal performance even as the system evolves. In essence, this approach establishes a robust, secure, centric foundation for IoMT-based e-healthcare, surpassing the limitations of traditional methodologies and patient.

Results and discussion

The implemented system has undergone simulation using MATLAB Simulink on a computer equipped with an 8-GB RAM Intel(R) Core™ i5–7400 CPU operating at 3.00-GHz, running on the Windows 10 Operating System. To establish the connections between consecutive blocks in the chain, the delay and capacity of each link are generated with a normal distribution, following the range of [1, 100] seconds for delays and bits per second (bits/s) for capacity.[43] This simulation-based evaluation showcases the robustness and reliability of the proposed smart contract-based framework for trusted blocks in an e-healthcare context. It validates the system's ability to maintain trust and security even in the face of potential attacks or compromised blocks, making it a promising solution for enhancing trust and data integrity in e-healthcare systems.[44,45] Table 1 represents the parameters used for network simulation.

Each node (Block) in the system was originally assigned a trust value of 10 Joules, which indicated the degree of security it possessed. A threshold of 6 Joules was set in order to differentiate between malicious and non-malicious nodes. When nodes reached this energy threshold, they were considered trustworthy and not malevolent. Furthermore, a distinct threshold

Table 1. Parameters used for proposed system simulation.

S. No	Network Attributes	Values
1	Total nodes (blocks)	100, 200 and 500
2	Total links (chains) formulated	5000, 15,500 and 45,500
3	Network size	1000 m × 1000 m
4	Information traffic	512 bits

of 4 Joules was established for the miner, who is accountable for verifying transactions and generating fresh blocks. As part of the gray assault simulation, different numbers of malicious miners (10, 50, and 100) were included to mimic adversarial conditions.[46] The goal of these upgrades was to evaluate the security and resilience of the system. Transactions were verified and added to the Blockchain by the miners. Table 1 provides a comprehensive summary of the architecture of the experiment, including all of the used parts and combinations.

Each block's data was put through a rigorous authentication procedure in this investigation, which included miner data validation and hash verification. The integrity and dependability of the Blockchain were maintained by reversing the validity of the previous block in the event that any block's authentication failed. Any effort at tampering rendered the whole chain preceding the modified block invalid as well. Extensive experimental findings were presented, along with a thorough analysis contrasting the effectiveness of the suggested algorithm with the traditional approach. The study shed light on the relative benefits and drawbacks of each strategy through data analysis and result interpretation, providing a thorough grasp of the suggested algorithm's efficacy in improving Blockchain system performance.[47–49]

Throughput analysis

Fig. 4 illustrates the comparison's findings visually and focuses on the average packet delivery ratio. The results clearly demonstrate how much better the recommended technique works than the conventional method. This benefit is due to a critical component of the proposed technique, which handles circumstances when data may have been hacked.[50] By preventing the next node in the chain from confirming polluted data, the system efficiently identifies and reverses data generated by rogue nodes. This resistance to data tampering improves the overall packet delivery ratio, increasing the reliability and efficiency of data transport in the Blockchain network. The proposed solution is resilient because it may be resistant to detrimental data modification, hence improving security and confidence.[51]

Average latency

In addition to assessing the average packet delivery ratio, the suggested approach was simulated for average latency—the amount of time it took to transmit data—in the presence of hostile and compromised nodes (blocks). In this comprehensive evaluation, the performance of the proposed algorithm was compared with the existing traditional approach.[48] Fig. 5 displays an example of the average delay achieved by both methods. The results indicated that the average latency of the recommended approach was greater than that of the conventional method. This increase could be related to a crucial element of the suggested algorithm: when the method finds data from a compromised block that contains hazardous operations, it requests retransmission of the data for the next block. Even while this method increases data security and dependability, the extra steps needed for data validation and retransmission might lead to a little increase in average delay. The network latency for the proposed model is displayed in Fig. 6 and Fig. 7.[52]

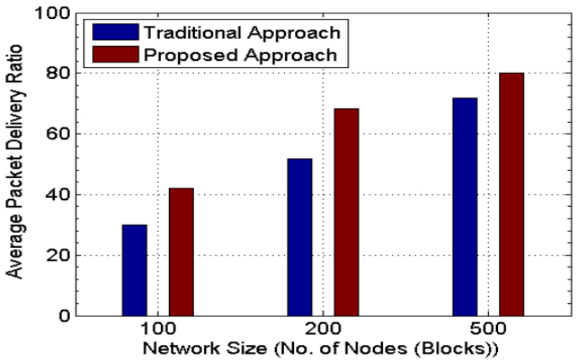

Fig. 5. Throughput vs no. of nodes.

The one of the most important performance metrics for evaluating the efficacy of the proposed algorithm is average energy efficiency, which is expressed in bits/s/joule.[44] As seen in Fig. 6, the average energy efficiency was taken into account and contrasted with the current procedure in order to assess the improvement attained. Within the Blockchain network, the suggested algorithm deliberately chooses particular miners to perform data transmission and authentication responsibilities. By carefully choosing the miners with the lowest threshold value of 4 Joules, or the most efficient miners, crucial processes are ensured. As a result, as compared to the current approach, the suggested algorithm achieves a greater average energy efficiency as shown in Fig. 7. This result is explained by the algorithm's consistent use of the energy-efficient miners throughout the process.[53] The proposed method optimizes energy usage, raising the Blockchain network's overall efficiency by taking advantage of miners with lower energy thresholds. Setting energy-efficient miners as a priority allows the system to complete jobs with the least amount of energy consumed, which improves energy efficiency. In e-healthcare systems, lower energy use boosts sustainability, encourages cost savings, and is better for the environment. The energy efficiency of the sug-

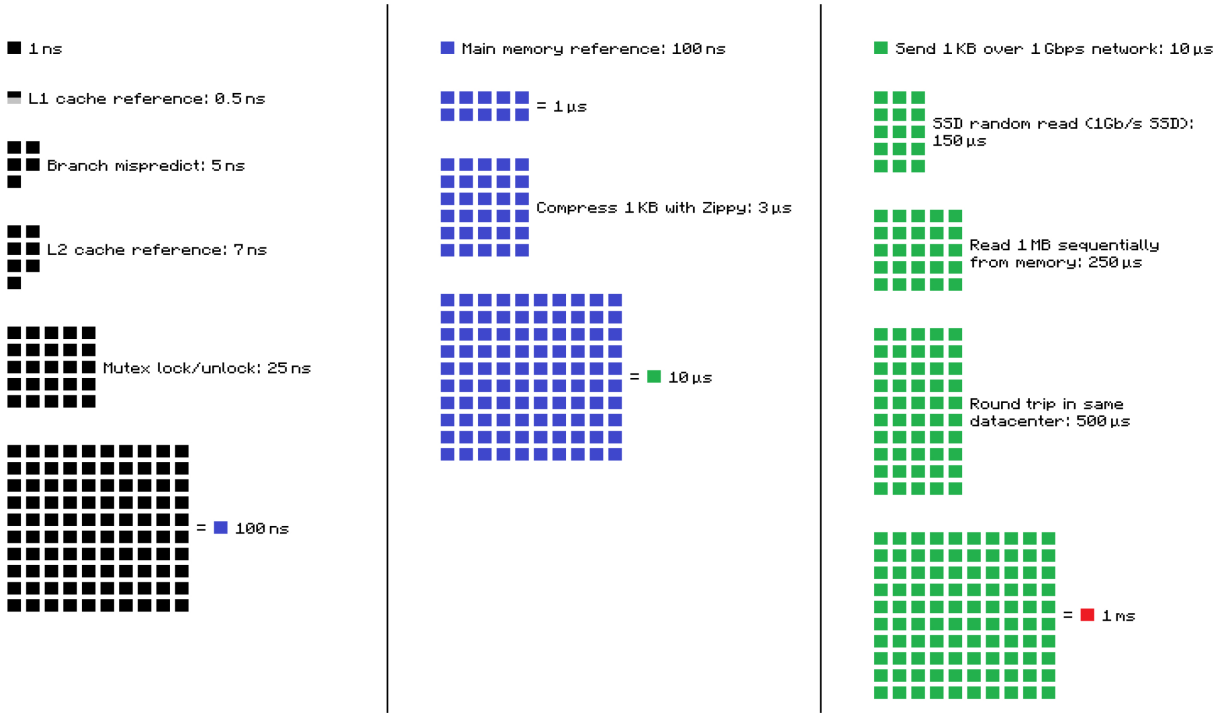

Fig. 6. Latency estimation average energy efficiency.

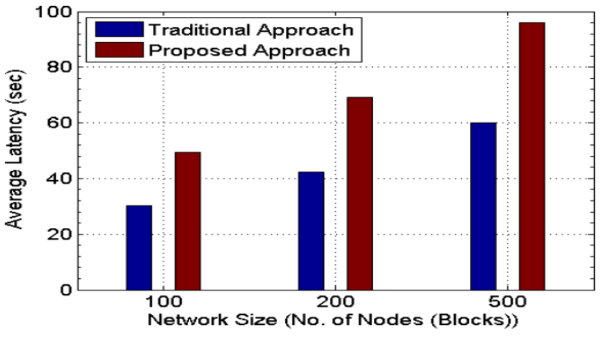

Fig. 7. Average latency vs no. of nodes.

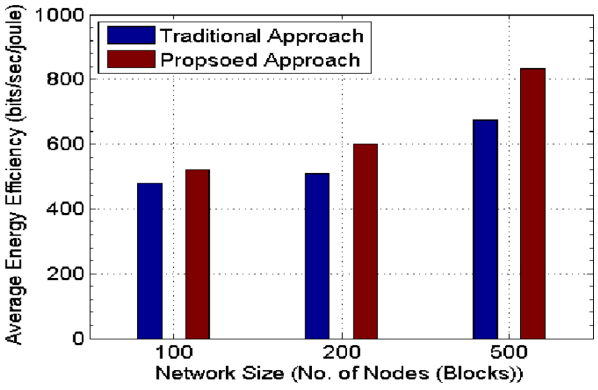

Fig. 8. Average energy efficiency vs no. of nodes.

gested model in relation to the number of nodes is shown in Fig. 8.

In terms of average packet delivery ratio, average latency, and average energy efficiency, the suggested design for IoMT-based e-healthcare systems shows promise for superiority over conventional approaches. Interoperability standards, energy-saving techniques, and improved communication protocols in networked devices enable this supremacy.

Limitations

The proposed method highlights the use of IoMT in e-healthcare, yet there are a few things to be aware of. The dynamic nature of IoMT devices might make it difficult to implement the recommended approach, which could cause problems with communication protocol standardization and compatibility. Health data security issues continue to arise in spite of encryption and privacy technology, necessitating continuous protection against cyberattacks. Financial limitations and variations in technological infrastructure between healthcare institutions may restrict scalability. Patient and healthcare provider approval is essential for successful adoption.

Conclusion

In conclusion, this research has significant theoretical and practical implications for the integration

of IoMT in e-healthcare. Theoretical contributions include developing a comprehensive architectural model that enhances the security, interoperability, and scalability of the healthcare ecosystem. Using industry-standard communication protocols, maintaining user privacy, and keeping up with the fast growing number of Internet of medical devices are all made possible by this model, which offers a conceptual framework. In practical terms, the proposed design facilitates effective communication among stakeholders, enhances patient involvement, and permits data-driven decision-making, all of which support the delivery of more efficient and patient-centered healthcare. In terms of scholarly contributions, this study expands our understanding of the promise and challenges connected with it while addressing significant issues like data security, interoperability, and scalability.

Authors' declaration

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are ours. Furthermore, any Figures and images, that are not ours, have been included with the necessary permission for re-publication, which is attached to the manuscript.
- No animal studies are present in the manuscript.
- No human studies are present in the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee at Sona College of Technology, Salem.

Authors' contributions statement

J. D Conceptualization, Methodology, Software, Data curation, Writing- Original draft preparation, S.S.y Validation, Writing- Reviewing and Editing, M. S Validation, Writing- Reviewing and Editing, S. B Supervision, Validation, B. G. T Validation, Writing-Reviewing and Editing, P. GSupervision, Validation.

References

1. Farhan L, Kharel R, Kaiwartya O, Hammoudeh M, Adebisi B. Towards green computing for Internet of things: Energy oriented path and message scheduling approach. Sustain Cities Soc. 2018 Apr 1;38:195–204. https://doi.org/10.1016/j.scs.2017.12.018.
2. El Majdoubi D, El Bakkali H, Sadki S. SmartMedChain: A blockchain-based privacy-preserving smart healthcare framework. J Healthc Eng. 2021 Nov 5;2021(1):4145512. https://doi.org/10.1155/2021/4145512.
3. Huang H, Zhu P, Xiao F, Sun X, Huang Q. A blockchain-based scheme for privacy-preserving and secure sharing of medical data. Comput Secur J. 2020 Dec 1;99:102010. https://doi.org/10.1016/j.cose.2020.102010.
4. Xu J, Xue K, Li S, Tian H, Hong J, Hong P, *et al.* Healthchain: A blockchain-based privacy preserving scheme for large-scale health data. IEEE Internet Things J. 2019 Jun 18;6(5):8770–8781. https://doi.org/10.1109/JIOT.2019.2923525.
5. Hossein KM, Esmaeili ME, Dargahi T. Blockchain-based privacy-preserving healthcare architecture. In 2019 IEEE CCECE, 2019 May 5;1–4, https://doi.org/10.1109/CCECE.2019.8861857.
6. Ali A, Al-Rimy BA, Alsubaei FS, Almazroi AA, Almazroi AA. HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. Sensors. 2023 Jul 28;23(15):67626791-. https://doi.org/10.3390/s23156762.
7. Luong DA, Park JH. Privacy-preserving blockchain-based healthcare system for IoT devices using zk-SNARK. IEEE Access. 2022 May 23;10:55739–55752. https://doi.org/10.1109/ACCESS.2022.3177211.
8. Bi H, Liu J, Kato N. Deep learning-based privacy preservation and data analytics for IoT enabled healthcare. IEEE Trans Industr Inform. 2021 Oct 8;18(7):4798–807. https://doi.org/10.1109/TII.2021.3117285.
9. He Q, Xu Y, Liu Z, He J, Sun Y, Zhang R. A privacy-preserving Internet of Things device management scheme based on blockchain. Int J Distrib Sens Netw. 2018 Nov;14(11):1550147718808750. https://doi.org/10.1177/1550147718808750.
10. Devi KR, Suganyadevi S, Balasamy K. Healthcare data analysis using deep learning paradigm. Deep Learning for Cognitive Computing Systems. 2023;129–148. https://doi.org/10.1515/9783110750584-008.
11. Balasamy K, Seethalakshmi V. HCO-RLF: Hybrid classification optimization using recurrent learning and fuzzy for COVID-19 detection on CT images. Biomed. Signal Process. Control. 2025;100(Part A):106951. ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2024.106951.
12. Balasamy K, Seethalakshmi V, Suganyadevi S. Medical image analysis through deep learning techniques: A comprehensive survey. Wireless Pers Commun. 2024;137:1685–1714. https://doi.org/10.1007/s11277-024-11428-1.
13. Rejeb A, Rejeb K, Zailani S, Treiblmaier H, Hand KJ. Integrating the internet of things in the halal food supply chain: A systematic literature review and research agenda. IEEE IOT. 2021 Mar 1;13:100361. https://doi.org/10.1016/j.iot.2021.100361.
14. Mandala V, Senthilnathan T, Suganyadevi S, Gobhinath S, Selvaraj D, Dhanapal R. An optimized back propagation neural network for automated evaluation of health condition using sensor data. Measurement: Sensors. 2023 Oct 1;29:100846. https://doi.org/10.1016/j.measen.2023.100846.
15. Weber RH. Internet of things–new security and privacy challenges. Comput Law Secur Rev. 2010 Jan 1;26(1):23–30. https://doi.org/10.1016/j.clsr.2009.11.008.
16. Ziegeldorf JH, Morchon OG, Wehrle K. Privacy in the internet of things: Threats and challenges. Secur Commun. Netw. 2014 Dec;7(12):2728–2742. https://doi.org/10.1002/sec.795.
17. Jing Q, Vasilakos AV, Wan J, Lu J, Qiu D. Security of the Internet of Things: perspectives and challenges. Wirel Netw.. 2014 Nov;20:2481–501. https://doi.org/10.1007/s11276-014-0761-7.

18. Shamia D, Balasamy K, Suganyadevi S. A secure framework for medical image by integrating watermarking and encryption through fuzzy based ROI selection. J Intell Fuzzy Syst. 2023 Jan 1;44(5):7449–7457.
19. Alaba FA, Othman M, Hashem IA, Alotaibi F. Internet of things security: A survey. J Netw Comput Appl. 2017 Jun 15;88.
20. Rejeb A, Keogh JG, Treiblmaier H. Leveraging the internet of things and blockchain technology in supply chain management. Future Internet. 2019 Jul 20;11(7):161. https://doi.org/10.3390/fi11070161.
21. Rejeb A, Keogh JG, Simske SJ, Stafford T, Treiblmaier H. Potentials of blockchain technologies for supply chain collaboration: a conceptual framework. Int J Logist Manag. 2021 Jul 22;32(3):973–994. https://doi.org/10.1108/IJLM-02-2020-0098.
22. Bera B, Chattaraj D, Das AK. Designing secure blockchain-based access control scheme in IoT-enabled Internet of Drones deployment. Comput Commun. 2020 Mar 1;153:229–249. https://doi.org/10.1016/j.comcom.2020.02.011.
23. Jesus EF, Chicarino VR, De Albuquerque CV, Rocha AA. A survey of how to use blockchain to secure internet of things and the stalker attack. Secur Commun Netw. 2018;7:1–27. https://doi.org/10.1155/2018/9675050.
24. El-Masri M, Hussain EM. Blockchain as a mean to secure internet of things ecosystems–a systematic literature review. J Enterp Inf Manag. 2021 Nov 9;34(5):1371–1405. https://doi.org/10.1108/JEIM-12-2020-0533.
25. Wang X, Zha X, Ni W, Liu RP, Guo YJ, Niu X, *et al.* Survey on blockchain for internet of things. Comput. Commun. 2019 Feb 1;136: 10–29. https://doi.org/10.1016/j.comcom.2019.01.006.
26. Ferrag MA, Derdour M, Mukherjee M, Derhab A, Maglaras L, Janicke H. Blockchain technologies for the internet of things: Research issues and challenges. IEEE Internet Things J. 2018 Nov 22;6(2):2188–204. https://doi.org/10.1109/JIOT.2018.2882794.
27. Viriyasitavat W, Anuphaptrirong T, Hoonsopon D. When blockchain meets internet of things: Characteristics, challenges, and business opportunities. J Ind Inf Integr. 2019 Sep 1;15: 21–8. https://doi.org/10.1016/j.jii.2019.05.002.
28. Cheng YL, Lim MH, Hui KH. Impact of internet of things paradigm towards energy consumption prediction: A systematic literature review. Sustain Cities Soc. 2022 Mar 1;78:103624. https://doi.org/10.1016/j.scs.2021.103624.
29. Khowaja SA, Prabono AG, Setiawan F, Yahya BN, Lee SL. Contextual activity-based healthcare internet of things, services, and people (HIoTSP): An architectural framework for healthcare monitoring using wearable sensors. J Comput Netw. 2018 Nov 9;145:190–206. https://doi.org/10.1016/j.comnet.2018.09.003.
30. Rejeb A, Simske S, Rejeb K, Treiblmaier H, Zailani S. Internet of things research in supply chain management and logistics: A bibliometric analysis. IEEE Internet Things J. 2020 Dec 1;12:100318. https://doi.org/10.1016/j.iot.2020.100318.
31. Ben-Daya M, Hassini E, Bahroun Z. Internet of things and supply chain management: a literature review. Int J Prod Res. 2019 Aug 29;57(15–16): 4719–42. https://doi.org/10.1080/00207543.2017.1402140.
32. Xhafa F, Kilic B, Krause P. Evaluation of IoT stream processing at edge computing layer for semantic data enrichment. Future Gener Comput Syst. 2020 Apr 1;105:730–736. https://doi.org/10.1016/j.future.2019.12.031.
33. Poniszewska-Maranda A, Kaczmarek D, Kryvinska N, Xhafa F. Studying usability of AI in the IoT systems/paradigm through embedding NN techniques into mobile smart service system. Computing. 2019 Nov;101(11):1661–85. https://doi.org/10.1007/s00607-018-0680-z.
34. Sula A, Spaho E, Matsuo K, Barolli L, Xhafa F, Miho R. A new system for supporting children with autism spectrum disorder based on IoT and P2P technology. Int J Space Based Situated Comput.. 2014 Jan 1;4(1):55–64. https://doi.org/10.1109/BWCCA.2013.51.
35. French AM, Shim JP. The digital revolution: Internet of things, 5G, and beyond. Commun Assoc Inf Syst.. 2016;38(1):40. https://doi.org/10.17705/1CAIS.03840.
36. Mazhelis O, Luoma E, Warma H. Defining an internet-of-things ecosystem. In Conference on internet of things and smart spaces. 2012 Aug 27;1–14. Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-32686-8_1.
37. Rejeb A, Rejeb K, Treiblmaier H, Appolloni A, Alghamdi S, Alhasawi Y, *et al.* The internet of things (IoT) in healthcare: Taking stock and moving forward. IEEE IOT. 2023;100721.https://doi.org/10.1016/j.iot.2023.100721.
38. Rashid OF, Subhi MA, Hussein MK, Mahdi MN. "Enhancing internet data security: A fusion of cryptography, steganography, and machine learning techniques. Baghdad Sci J. 2024 Dec. 11;22(4). https://doi.org/10.21123/bsj.2024.10371.
39. Putra HN, Defit S, Nurcahyo GW. "Development of hybrid machine learning in patient diagnosis classification using the XRP Model (extraction, reduction & prediction). Baghdad Sci J. 22(2). https://doi.org/10.21123/bsj.2024.9695.
40. Ali HA, Hariri W, Zghal NS, Aissa DB. Comparing PCA-based machine learning algorithms for COVID-19 classification using chest X-ray images. Baghdad Sci. J. https://doi.org/10.21123/bsj.2024.9422.
41. Devi KR, Balasamy K, Prathyusha M, Jeevitha R, Balasubramanie P, Eswaran M. Optimization techniques for preserving privacy in data mining. ICECCT. 2023 Feb 22;1–6. IEEE. https://doi.org/10.1109/ICECCT56650.2023.10179655.
42. Fernández-Caramés TM, Fraga-Lamas P. A Review on the use of blockchain for the internet of things. IEEE Access. 2018 May 31;6:32979–3001. https://doi.org/10.1109/ACCESS.2018.2842685.
43. Rejeb A, Rejeb K, Appolloni A, Kayikci Y, Iranmanesh M. The landscape of public procurement research: A bibliometric analysis and topic modelling based on Scopus. J Public Procure. 2023 Mar 16 (ahead-of-print). https://doi.org/10.1108/JOPP-06-2022-0031.
44. Guo Y, Barnes SJ, Jia Q. Mining meaning from online ratings and reviews: Tourist satisfaction analysis using latent dirichlet allocation. Tour Manag. 2017 Apr 1;59:467–83. https://doi.org/10.1016/j.tourman.2016.09.009.
45. Enhancing Internet Data Security: A Fusion of Cryptography, Steganography, and Machine Learning Techniques. Baghdad Sci J. [cited 2024 Dec. 11];22(4) https://doi.org/10.1145/2133806.2133826.
46. Li RT, Khor KA, Yu LG. Identifying indicators of progress in thermal spray research using bibliometrics analysis. J Therm Spray Technol. 2016 Dec;25:1526–33. https://doi.org/10.1007/s11666-016-0445-1.
47. Raju K, Ramshankar N, Shathik JA, Lavanya R. Blockchain assisted cloud security and privacy preservation using hybridized encryption and deep learning mechanism in IoT-healthcare application. J Grid Comput. 2023 Sep;21(3):45. https://doi.org/10.1007/s10723-023-09678-7.
48. Amri MM, Abed SA. The data-driven future of healthcare: A review. Mesop Environ J. 2023 Jun;8:68–74. https://doi.org/10.58496/MJBD/2023/010.

49. Lakhan A, Lateef AA, Abd Ghani MK, Abdulkareem KH, Mohammed MA, Nedoma J, Martinek R, Garcia-Zapirain B. Secure-fault-tolerant efficient industrial internet of healthcare things framework based on digital twin federated fog-cloud networks. J King Saud Univ. Comput Inf Sci. 2023 Oct 1;35(9):101747. https://doi.org/10.1016/j.jksuci.2023.101747.
50. Lakhan A, Mohammed MA, Abdulkareem KH, Khanapi Abd Ghani M, Marhoon HA, Nedoma J, *et al.*, Secure blockchain assisted Internet of Medical Things architecture for data fusion enabled cancer workflow. IEEE IOT. 2023 Dec 1;24:100928. https://doi.org/10.1016/j.iot.2023.100928.
51. Mohammed MA, Lakhan A, Abdulkareem KH, Zebari DA, Nedoma J, Martinek R, *et al.* Energy-efficient distributed federated learning offloading and scheduling healthcare system in blockchain based networks. IEEE. IOT. 2023 Jul;1:22:100815. https://doi.org/10.1016/j.iot.2023.100815.
52. Lakhan A, Mohammed MA, Nedoma J, Martinek R, Tiwari P, Kumar N. DRLBTS: deep reinforcement learning-aware blockchain-based healthcare system. Sci Rep. 2023 Mar;13:13(1):4124. https://doi.org/10.1038/s41598-023-29170-2.

نظام تعلم آلي ذكي قائم على تقنية Blockchain للحفاظ على الخصوصية في مجال الرعاية الصحية لإنترنت الأشياء

جيه. ديبيكا [1]، ساهانا شيتي [2]، د. إم. سيفاكومار [3] ، د. ساروج بالا [4]، بينيتا جراسيا ثانغام جي [5]، براديب جي [6]

[1] قسم تكنولوجيا المعلومات، كلية سونا للتكنولوجيا، سايلم، الهند.
[2] قسم *CSE-AIML* والأمن السيبراني، كلية *CSE*، *FET* - جاين، جاياناجار، بنغالور، الهند.
[3] قسم علوم الكمبيوتر والهندسة، كلية سيماتس للهندسة، معهد سافيثا للعلوم الطبية والتقنية، تشيناي، تاميل نادو، الهند.
[4] قسم *MCA* ، كلية أجاي كومار جارج للهندسة، غازي آباد، الهند.
[5] قسم الذكاء الاصطناعي و*DS*، معهد باناري عمان للتكنولوجيا، ساتيامانغالام، إيرود، تاميل نادو، الهند.
[6] قسم التكنولوجيا ، علوم وهندسة الحاسوب، كلية سري كريشنا للهندسة والتكنولوجيا، كويمباتور، الهند.

الخلاصة

لقد غزت فكرة البلوك تشينBlockchain مجالات دراسية مختلفة، ومن المتوقع أن ينمو اعتمادها على نطاق واسع بشكل كبير في المستقبل القريب. من خلال تنفيذ مقتطفات تعليمات برمجية موجزة محددة مسبقًا والمعروفة باسم العقود الذكية على بلوكتشين، يمكن التخلص من الحاجة إلى الوسطاء، ويمكن زيادة عدد عمليات تنفيذ العقود بشكل كبير. يتم فحص تطبيق تقنية blockchain والعقود الذكية، جنبًا إلى جنب مع أساليب التعلم الآلي، على الرعاية الصحية الإلكترونية القائمة على IoMT بشكل نقدي في هذه المقالة. الهدف من هذا المشروع هو استكشاف كيف يمكن للأتمتة واللامركزية تحسين الرعاية الصحية. يوفر دمج هذه المكونات الفرصة للتعامل مع البيانات الطبية بشكل آمن وخصوصي وشفاف مع تسهيل التواصل السهل بين المرضى ومتخصصي الرعاية الصحية وشركات التأمين. يُقترح نموذج معماري خاص مصمم لإنترنت الأشياء الطبية (IoMT)في الرعاية الصحية الإلكترونية لتوضيح المشكلة المذكورة أعلاه. ومن أجل تحسين الفعالية والاعتمادية وقابلية التوسع في البيئات الطبية، يستفيد هذا النموذج من اللامركزية والعقود الذكية. تتناول الورقة أيضًا المزايا المحتملة لهذا النهج، والصعوبات، والتطورات القادمة. تسلط البيانات التجريبية الضوء على إمكانات البنية المقترحة لتحويل تقديم الخدمات الطبية من خلال إظهار تفوقها على الأساليب التقليدية، وخاصة من حيث تسليم الحزم، وزمن الوصول، وكفاءة الطاقة .

الكلمات المفتاحية: البلوك تشين، التشفير، إنترنت الأشياء، البيانات الطبية، الخصوصية