Archives available at Journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349 – 9338
Volume 14 Issue 01, 2025

Enhancing Healthcare Security Block chain Technology for Secure Data Transmission

[1]Paritosh Biswas, [2]Dr Syed Umar, [3]Lakshmi Narasimhan Srinivasagopalan, [4]Ramu Mannava, [5]Jyothinadh nadella, [6]Dr Ramesh Safare

[1] M. Tech student, Department of Computer Engineering, Marwadi University, Rajkot, Gujarat. India.
[2] Professor, Department of Computer Engineering, Marwadi University, Rajkot, India
[3]Senior Technical Lead, Incdo, Plano Texas, U.S.A
[4]Master in Information Technology, Arkansas Tech University, U.S.A
[5]Software Engineer, Verinon Technology Solutions, U.S.A
[6]Associate Professor, Faculty of Management Studies, Marwadi University, Rajkot, India,
Email: paritosh.biswas@marwadieducation.edu.in,umar332@gmail.com, naryana123@gmail.com, ramu123@@yhoo.com,Jyothi123@gmail.com,ramesh.safare@marwadieducation.edu.in

Peer Review Information

Submission: 17 Feb 2025
Revision: 21 March 2025
Acceptance: 23 April 2025

Keywords
Block chain Technology, Healthcare Security, Secure Data Transmission, Data Privacy, Decentralized Systems, Cryptographic Protocols, Smart Contracts, Patient-Centric Data Control.

Abstract

A revolutionary way to improve data security, transparency, and trust in the sharing of medical information is through the use of block chain technology in the healthcare industry. In order to solve important issues including data breaches, illegal access, and interoperability, this study investigates the use of block chain technology for safe data transfer in healthcare systems. By leveraging block chain's decentralized architecture and cryptographic protocols, this approach ensures immutable record-keeping, real-time traceability, and patient-centric control over sensitive data. We propose a secure framework that integrates smart contracts for automated access management, minimizing the reliance on intermediaries and enhancing system efficiency. Scalability, privacy-preserving measures, and adherence to healthcare laws like HIPAA and GDPR are all examined in the study. A more safe and open digital healthcare environment is made possible by the results, which show notable gains in data integrity, system resilience, and user trust. Block chain's promise as a platform for safe healthcare data transmission is highlighted by this study, which also lays the groundwork for further advancements in the area.

Introduction

Significant improvements in patient care, operational effectiveness, and medical research have resulted from the healthcare sector's digital revolution [1]. But technology has also brought up significant difficulties in preserving the integrity, confidentiality, and security of private medical information. For the storage and exchange of patient data, healthcare organizations are increasingly depending on cloud-based platforms, Internet of Medical Things (IoMT) devices, and electronic health records (EHRs). These technologies improve accessibility and teamwork, but they also make people more susceptible to cyberattacks, illegal access, and data breaches. These occurrences can have disastrous repercussions, from monetary losses to jeopardized patient safety and trust.

Accessibility and privacy must be balanced, which adds to the difficulty of managing healthcare data [2]. Patients, providers, insurers, and researchers must access medical data for various purposes, but this access must be tightly controlled to prevent misuse. Existing

centralized systems, which rely on a single point of control, are susceptible to hacking, fraud, and operational failures. Tracking data consumption and ensuring compliance with regulatory frameworks like the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) are made more difficult by the fact that these systems frequently lack efficiency, transparency, and interoperability.

Block chain technology has surfaced as a game-changing answer to these problems. By tamper-proofing transaction recording over a network of nodes, block chain, a decentralized and distributed ledger system, guarantees data integrity, security, and transparency [3]. By eliminating single points of failure, block chain's decentralized architecture improves system resilience and lowers the possibility of data breaches. Furthermore, block chain protects data by using sophisticated cryptographic mechanisms that guarantee that only authorized parties can access and alter data.

One of the main innovations in block chain technology is the usage of smart contracts, which are self-executing contracts that enforce rights and regulations automatically without the need for middlemen. Smart contracts can be used to automate procedures like data sharing agreements, access control, and patient permission in the healthcare industry [4]. Because of this automation, there is less need for manual interventions, human error is reduced, and operational efficiency is increased. Patients are empowered to choose who can access their medical records and under what circumstances, giving them more control over their data.

The use of block chain in healthcare is not without its difficulties, despite its potential. It's important to carefully consider issues like scalability, compatibility with current systems, and privacy restrictions [5]. Additionally, implementing block chain requires significant investment in infrastructure, stakeholder education, and collaborative governance models. This study explores how block chain technology can be used in the healthcare industry to transmit data securely. It examines block chain's fundamental ideas, how it might improve healthcare security, and how it complies with legal requirements [6]. Block chain technology has the ability to completely transform healthcare security by offering a strong foundation for data transmission. This would create a reliable ecosystem that protects sensitive data while encouraging creativity and teamwork.

Block chain Technology

An innovative digital ledger system called block chain technology makes it possible to record transactions across a dispersed network in a secure, transparent, and decentralized manner. A block chain's fundamental building blocks are successive data blocks that are cryptographically connected to create an unchangeable chain [7]. This framework guarantees data integrity and security by preventing data from being changed or removed once it has been recorded without the consent of network participants. In contrast to conventional centralized systems, block chain functions on a dispersed network in which data is synced and duplicated among several nodes [8]. This increases system resilience and lowers the possibility of single points of failure by doing away with the necessity for a central authority. Block chain employs cryptographic hashing to ensure that data stored within a block cannot be altered without changing subsequent blocks. This makes it virtually tamper-proof and highly reliable for maintaining accurate records.

All transactions on a block chain are recorded in a publicly accessible ledger (for public block chains) or shared among authorized participants (for private block chains) [9]. Stakeholder responsibility and confidence are increased by this transparency. Advanced cryptography protocols are used by block chain to protect data. Only legitimate entries are added to the ledger once transactions are validated using consensus techniques like Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT). Smart contracts are integrated self-executing code that is a unique characteristic of block chain technology [10]. Without the need for middlemen, they carry out tasks like processing payments or allowing access to data and automatically enforce certain regulations.

Real-time tracking and historical data analysis are made possible by block chain, which offers a comprehensive audit record of all transactions. Applications such as healthcare data management and supply chain management benefit greatly from this. Open to anyone, these block chains are decentralized and operate without a central authority. Examples include Bit coin and Ethereum. Restricted to authorized participants, private block chains are commonly used in enterprise settings for enhanced control and confidentiality. Governed by a group of organizations, these block chains combine the benefits of private and public block chains, offering both decentralization and controlled access. A combination of public and private block chains, hybrid block chains provide flexibility by allowing certain data to remain private while other parts are publicly accessible.

Allows patients, providers, and insurers to share electronic health records (EHRs) in a safe and effective manner. Uses smart contracts to give patients control over who can access their medical data. Enhances transparency and traceability to prevent fraudulent billing and claims. Ensures the authenticity of pharmaceuticals by tracing their origin and distribution. Guarantees the integrity and transparency of clinical trial data, ensuring ethical practices.

Secure Data Transmission

Ensuring the confidentiality, integrity, and validity of information while transmitting it over networks is known as secure data transmission. Secure data transmission is crucial in this age of digital transformation, as private information such as financial transactions, medical records, and personal identifiers are shared electronically. This is to avoid data breaches, cyberattacks, and unwanted access. Guarantees that only systems or people with permission can access the data that has been transferred. Data is frequently encoded using encryption techniques like RSA and Advanced Encryption Standard (AES), which prevent unauthorized parties from reading the data.

Ensures that no changes were made to the data while it was being transmitted. Hashing algorithms, such as SHA-256, generate a unique checksum for the data, allowing recipients to verify its authenticity. Confirms the identities of the sender and recipient to prevent impersonation or spoofing. Techniques such as digital certificates, public key infrastructure (PKI), and multi-factor authentication (MFA) are used to establish trust. Ensures that the sender cannot deny sending the data and the recipient cannot deny receiving it. Digital signatures offer proof of the data's integrity and place of origin.

Even in the event of system failures or possible cyber threats, guarantees that data is available to authorized users when needed [11]. Asymmetric or symmetric encryption methods are used to encrypt data before sending it, making sure that only the person who has the decryption key may access it. VPNs create encrypted tunnels for data transmission over public or unsecured networks, protecting it from interception. SSL/TLS protocols provide end-to-end encryption for secure communication over the internet, ensuring safe transmission of sensitive information like login credentials and payment details.

Block chain provides a decentralized and safe way to send data, with consensus processes and cryptographic algorithms guaranteeing data confidentiality and integrity. Sensitive data is replaced with non-sensitive tokens during transmission, reducing the risk of exposure even if intercepted. Firewalls filter traffic to block unauthorized access, while IDS monitor network activity to detect and prevent suspicious behavior. The interchange of sensitive patient data, including electronic health records (EHRs), diagnostic findings, and insurance information, is largely dependent on secure data transfer in healthcare systems. Safe transmission is essential for adherence to laws such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA).

Securely transmitting health records between providers to ensure continuity of care. Encrypting patient data during remote consultations to maintain confidentiality. Safeguarding data transmitted from IoMT devices to healthcare providers. Using block chain for tamper-proof and transparent data sharing [12]. Interception Risks: Data may be intercepted during transmission by cybercriminals employing man-in-the-middle (MITM) attacks. Securing encryption keys against loss or compromise remains a challenge. Ensuring secure transmission in large-scale systems with high data volumes can be resource-intensive. Meeting diverse regulatory requirements across jurisdictions adds complexity to implementing secure systems.

Enhancing Healthcare Security Block chain Technology for Secure Data Transmission

Sensitive medical data transfer is a major concern in today's networked healthcare setting. Patient care and operational efficiency have increased as a result of the quick digitalization of healthcare systems, which includes the broad use of electronic health records (EHRs) and the Internet of Medical Things (IoMT). But it has also made healthcare data vulnerable to serious security risks like cyberattacks, illegal access, and data breaches. A strong and creative solution for safe data sharing is required because to the growing complexity of data management, the requirement to protect privacy, and the necessity to comply with strict laws like HIPAA and GDPR.

One revolutionary method for overcoming these obstacles is block chain technology. Block chain provides unmatched benefits for protecting healthcare data by utilizing its decentralized, immutable, and cryptographically secure design. This study investigates how block chain technology can improve hospital security by facilitating safe data transfer. It outlines the principles, features, and applications of block chain in healthcare, with a focus on addressing

the critical issues of data privacy, integrity, and interoperability.

Block chain is a distributed, decentralized ledger system that transparently and irrevocably logs transactions across a network of nodes. It is ideal for safe data transfer in healthcare because of its fundamental characteristics, which include consensus processes, decentralization, and cryptographic security [13]. Block chain makes assurance that once recorded, medical data cannot be changed or tampered with. This ensures that diagnostic reports, treatment histories, and patient records are all accurate. Block chain lowers the risk of data breaches by dispersing data throughout a network, removing single points of failure. Smart contracts simplify procedures like access control and patient permission by enabling automated and rule-based data sharing.

Real-time tracking of data access and usage is made possible by block chain's transparent ledger, which encourages responsibility among stakeholders. Patients are given total control over their data thanks to block chain, which allows them to choose who can access it and why. Block chain technology transforms healthcare data transfer by offering a safe framework that takes into account the core principles of non-repudiation, confidentiality, integrity, and authentication. Only authorized parties can access data transmitted via block chain since it is encrypted using cutting-edge cryptographic algorithms. Block chain uses consensus techniques like Proof of Work (PoW) and Proof of Stake (PoS) to verify transactions and stop illegal changes.

Block chain facilitates safe and easy data transfer between various healthcare systems, encouraging cooperation and treatment continuity. Block chain solutions can be tailored to meet regulatory standards, ensuring secure data transmission while adhering to legal requirements [14]. Block chain ensures secure sharing and storage of patient records, preventing unauthorized access and maintaining data integrity. Securely transmits patient data during virtual consultations, safeguarding confidentiality. Tracks and verifies the authenticity of pharmaceuticals, reducing counterfeit drugs in circulation. Protects clinical trial data from fraud and manipulation by guaranteeing its integrity and transparency.

Safeguards data transmitted from interconnected medical devices, ensuring real-time monitoring without compromising patient privacy. While block chain offers immense potential, its adoption in healthcare is not without challenges. Scalability, integration with existing systems, and ensuring compliance with diverse regulations are significant hurdles. Additionally, the high energy consumption of certain block chain protocols and the need for stakeholder education and collaboration must be addressed. Future developments in block chain technology, such as lightweight consensus mechanisms, enhanced privacy-preserving techniques, and hybrid block chain models, hold promise for overcoming these challenges.

The healthcare sector may realize the full potential of block chain technology to transform data transmission and security by investing in it and encouraging interdisciplinary collaboration [15]. A safe, decentralized, and effective framework for tackling the significant problems associated with data transmission in the healthcare industry is provided by block chain technology. Through the utilization of its distinct features, healthcare institutions may improve data integrity, guarantee privacy, and give patients more authority over their medical data. Block chain technology has the potential to become a key component of a safe, open, and patient-focused healthcare ecosystem as it develops and becomes more widely used.

Literature Survey Analysis

Block chain technology has been increasingly popular in the healthcare industry as a strong way to protect privacy and transmit data securely. This literature survey analyzes recent research and developments in the field, highlighting advancements, challenges, and future directions for integrating block chain technology into healthcare security frameworks. Research highlights how block chain might solve important security issues such data breaches, illegal access, and incompatibilities [16]. Shown how patient-centric access control and data immutability might be guaranteed by block chain-enabled solutions. Investigated hybrid block chain solutions that strike a balance between confidentiality and transparency by combining elements of public and private block chains.

Block chain's decentralized nature enhances data resilience, reducing risks associated with single points of failure. It provides real-time audit trails and supports secure data sharing among stakeholders, fostering trust and collaboration. Smart contracts automate access permissions, ensuring compliance with patient consent policies [17]. Implemented a smart contract framework for secure sharing of electronic health records (EHRs), improving operational efficiency and reducing human error. Discussed smart contracts' potential in streamlining telemedicine workflows by automating data-sharing agreements and billing processes. Smart

contracts enhance system efficiency by eliminating intermediaries and automating routine tasks. For broad adoption, however, issues with legal enforceability and programming accuracy must be resolved.

Data security and privacy are subject to strict regulations such as GDPR and HIPAA. Examined block chain's ability to meet these regulations through cryptographic data protection and decentralized storage. Proposed compliance-focused block chain architectures that integrate secure data encryption and access logs. Block chain aligns well with regulatory requirements, ensuring secure data transmission and traceability [18]. Integrating block chain with existing regulatory frameworks offers significant potential but requires robust governance models and stakeholder cooperation. The Internet of Medical Things (IoMT) generates vast amounts of sensitive data requiring secure transmission. Implemented block chain-based solutions to protect IoMT device communications, leveraging encryption and consensus mechanisms. Highlighted block chain's effectiveness in mitigating risks of data tampering and unauthorized access in IoMT ecosystems.

By offering a transparent and impenetrable platform for data exchange, block chain improves IoMT security. However, scalability and real-time processing capabilities must be improved for seamless integration with IoMT networks. High computational demands of block chain protocols like Proof of Work (PoW) limit its scalability. Integrating block chain with legacy healthcare systems remains a challenge [19]. Initial implementation costs and resource requirements can be prohibitive for small organizations. Overcoming these challenges requires innovation in lightweight consensus mechanisms, cross-platform interoperability standards, and cost-efficient deployment strategies. Collaboration among technology providers, healthcare organizations, and regulatory bodies is essential.

Integrating block chain and AI to enable safe decision-making and predictive analytics. Developments in homomorphic encryption and zero-knowledge proofs (ZKPs) to improve data secrecy. Granting patients self-sovereign IDs based on block chain technology so they may access data securely. Make research investments to increase block chain's energy efficiency and scalability. Create global guidelines for integrating block chain technology into the medical field. Encourage interdisciplinary cooperation to tackle regulatory and technical issues.

Through safe data transfer, block chain technology presents a viable way to improve healthcare security. Numerous issues raised by the digital transformation of healthcare might be resolved by block chain by guaranteeing data integrity, confidentiality, and transparency [20]. However, addressing scalability, interoperability, and compliance challenges is critical to unlocking its full potential. Continued research and innovation in block chain applications will drive the evolution of secure, efficient, and patient-centric healthcare ecosystems.

Existing Approaches

By distributing healthcare data among several nodes, block chain's decentralized architecture lowers the dangers connected with centralized solutions. Every transaction is recorded on a shared ledger, making data availability high while minimizing single points of failure. To prevent any one entity from having complete control over the data, inpatient records, medical histories, and diagnostic results are safely maintained across a network of nodes. Guarantees a safe, distributed system where data integrity is preserved independently of a central authority, hence lowering the danger of data breaches and corruption. Data immutability is enforced by block chain through distributed consensus and cryptographic hashing. Since information cannot be removed or changed once it is stored on the block chain, authenticity is guaranteed.

The block chain creates an unchangeable trail by cryptographically connecting and permanently storing lab data, prescription logs, and patient records. Increases trust by removing the potential for illegal changes and maintaining an honest, open audit trail. Granular control is provided by role-based access systems and smart contracts, which regulate who has access to particular medical records. With pre-established permissions, block chain-based solutions guarantee that only authorized individuals or systems can access sensitive data. Only with authorization can a healthcare provider access a patient's records, guaranteeing that information is shared only with those who need to know. Ensures confidentiality by restricting access to data and establishing a safe environment for managing patient data.

Block chain makes it possible for health data to be securely shared between various systems and organizations, guaranteeing that records can move freely while still being secure. A hospital and a specialist clinic can exchange encrypted patient data via block chain, ensuring secure data sharing without compromising patient privacy. Enhances collaboration between healthcare providers while reducing data silos and ensuring the security of sensitive information. Block chain

integrates advanced encryption techniques, including hashing, public-private key cryptography, and zero-knowledge proofs, ensuring that data is protected both at rest and in transit. Additionally, anonymization techniques remove or obscure personal identifiers from the data before recording it on the block chain.

Patient data, such as genetic information, is hashed and anonymized before being recorded, ensuring that only meaningful insights can be extracted without compromising patient identities. Balances data security with privacy preservation, minimizing risks associated with unauthorized data access. Block chain enables the creation of secure, self-sovereign digital identities for patients and healthcare providers. These identities can be managed by individuals, ensuring they have complete control over their health records and personal data. A patient creates a decentralized identifier (DID) linked to their health records, which can be verified by healthcare providers and organizations. Reduces identity theft risks, streamlining authentication and making data access more secure.

Block chain allows for tokenizing healthcare data, which can incentivize secure sharing through reward systems. Individuals, providers, and researchers may receive tokens for sharing de-identified data securely. A patient can earn tokens by providing access to their anonymized health data for research purposes, which can then be exchanged for discounts on healthcare services or other benefits. Encourages secure data exchange while compensating individuals for their participation, promoting ethical data usage. Block chain-based smart contracts can automate adherence to legal requirements like GDPR and HIPAA. Data protection policies are encoded into the block chain, ensuring adherence and providing a clear audit trail. A smart contract that enforces privacy policies for patient data use, ensuring organizations comply with privacy laws at every step.

Reduces legal risks and facilitates automated compliance monitoring, minimizing manual oversight. Block chain secures data from IoT devices used in healthcare settings, such as wearables or connected medical devices. Real-time monitoring data is securely transmitted through the block chain network. Wearable technology encrypts and records blood pressure and heart rate data on a block chain, guaranteeing safe, traceable delivery to medical professionals. ensures patient data from IoT devices is safe and tamper-proof by offering real-time data security and monitoring. By safely storing trial data, patient consent, and research findings, block chain enhances security and transparency in clinical trials and medical research. Clinical trial results and participant consent are stored in an immutable block chain ledger, providing transparency and preventing falsification. Increases trust and reduces the risk of fraudulent activities in research through an unalterable, transparent, and traceable data trail.

Proposed Method

The proposed method integrates advanced block chain technology into healthcare systems to ensure secure and efficient data transmission. This approach combines decentralized ledgers, encryption, and smart contracts to enhance data security, integrity, and access control, while addressing regulatory compliance and interoperability challenges. Distribute healthcare data across multiple nodes, ensuring no single point of failure. Install a distributed ledger system that securely and irrevocably replicates patient records and medical data across several nodes. Decreases downtime during system breakdowns and lowers the danger of data breaches. Keep a record of medical data that cannot be altered. To guarantee that material cannot be changed or removed once it has been recorded, use consensus techniques and cryptographic hashing.

Provides a transparent, auditable trail of patient data, ensuring accuracy and security. Implement fine-grained access control mechanisms for healthcare data. Smart contracts enforce access policies, allowing only authorized users (e.g., patients, providers, researchers) to access specific healthcare records. Ensures that sensitive data is shared only with relevant parties, enhancing privacy and confidentiality. Protect sensitive healthcare data during transmission and storage. Encrypt data using advanced cryptographic techniques (e.g., end-to-end encryption, zero-knowledge proofs) and implement anonymization protocols to reduce exposure risks. Prevents data breaches and unwanted access to patient information. Verify if block chain-based healthcare systems comply with local data protection legislation, HIPAA, GDPR, and other regulatory requirements.

Smart contracts embedded with compliance rules automatically enforce data protection policies, maintaining an auditable record of regulatory adherence. Facilitates automated compliance monitoring and reduces legal risks. Enable secure and efficient data sharing across multiple healthcare organizations and systems. Implement block chain-based health information exchanges (HIEs) that ensure data is securely shared while maintaining confidentiality and integrity. Promotes seamless data flow while ensuring data security and privacy. Enable secure, verifiable identities for patients and

healthcare providers. Utilize decentralized identifiers (DIDs) for patients and providers, linked to their encrypted health data, providing complete control over their personal health records.

Reduces identity theft risks and enhances the security of user authentication processes. Promote secure sharing of de-identified healthcare data by incentivizing participation. Token-based models that reward individuals for securely contributing to research or data exchanges. Encourages secure data sharing and collaboration, enhancing data accessibility without compromising security. secure data gathered in real time from wearable's and IoT devices. Block chain uses hashing and encryption techniques to safely capture IoT-generated healthcare data, guaranteeing data security both during storage and transfer. allows health measures to be tracked in real time while protecting private information. Improve clinical trial and medical research data security and transparency.

Utilize block chain technology to provide a tamper-proof environment for research data, permission forms, and trial results. Increases trust and accountability in research activities, reducing fraudulent practices. Deploy a block chain-based healthcare system with specific features like distributed ledgers, smart contracts, and encryption mechanisms. Securely integrate patient data from various healthcare systems and IoT devices into the block chain network. Make sure that only authorized users can access particular data by defining and enforcing access control restrictions with smart contracts. Use smart contract rules that are incorporated to automate adherence to healthcare regulations. Perform thorough testing and security audits to ensure the system's integrity and protection against vulnerabilities.

Result

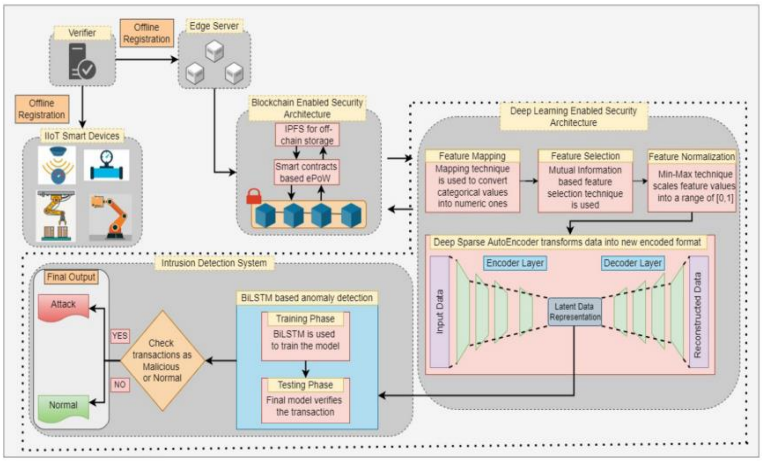
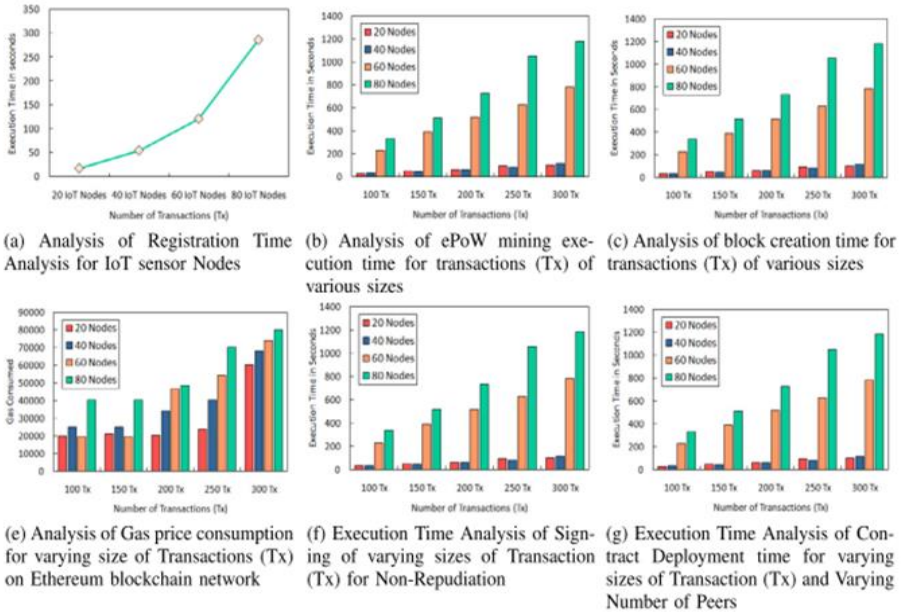


Fig 1: Deep learning with block chain coordination is suggested as a safe data transmission method for IoT-enabled healthcare systems.

Figure 1 illustrates how many parties share information. This system comprises a number of communication entities, such as Internet of Things devices (Sdi), verifiers (V), and edge servers (EDGE). Prior to their position within the network, V is responsible for registering each participating entity. The resources and processing power of the Sdi are limited. Among other things, this covers proximity sensors, water quality, and pressure. Identifying objects, assessing equipment leaks, and detecting non-regulatory water quality are their respective uses. Every Sdi can send and receive data over the Internet since they all have an Internet connection. EDGE includes industrial computers and data analysis servers. To carry out mining operations. Data poisoning attempts are thus prevented by this level, which also keeps an eye on the data source, owner, final destination, alternate routes, security measures, and security enabling authority. The DSAE technique transforms the original data into a new format, significantly reducing the dimensionality of the datasets when DL is enabled in the security architecture. The following goes into great detail on how these designs work.



(a) Analysis of Registration Time Analysis for IoT sensor Nodes

(b) Analysis of ePoW mining execution time for transactions (Tx) of various sizes

(c) Analysis of block creation time for transactions (Tx) of various sizes

(e) Analysis of Gas price consumption for varying size of Transactions (Tx) on Ethereum blockchain network

(f) Execution Time Analysis of Signing of varying sizes of Transaction (Tx) for Non-Repudiation

(g) Execution Time Analysis of Contract Deployment time for varying sizes of Transaction (Tx) and Varying Number of Peers

Fig 2: Analysis of the outcome for a security architecture provided by block chain.

Figure 2a shows how the number of nodes gradually increases the registration time. Similarly, the duration of the suggested ePoW consensus process is depicted in Fig. 2b. Three hundred Texas and a maximum of 80 IoT nodes are used to test the BDSDT architecture. It has been observed that a transaction takes longer to complete when there are more nodes involved. Figures 2c and 2d show the creation and access times of blocks.

We can observe that time is stable up to 40 nodes and 300 Tx. However, the time required to create a block and access them grows as the number of nodes increases from 60 to 80. The gas price utilization for smart contract access is depicted in Fig. 2e, and it gradually grows as the number of IoT nodes and Tx climbs. To guarantee non-repudiation, the BDSDT framework requires participating IoT nodes to sign for a set amount of time. The signature time required for the participating IoT nodes to modify Tx is shown in Fig. 2f. A similar pattern is seen when Tx and the number of IoT nodes increase over time. The time required to implement the suggested smart contracts in the network is depicted in Fig. 2g. There is a noticeable increase in time up to 40 nodes and 300 Tx. However, time also increases as the number of nodes rises with Tx.

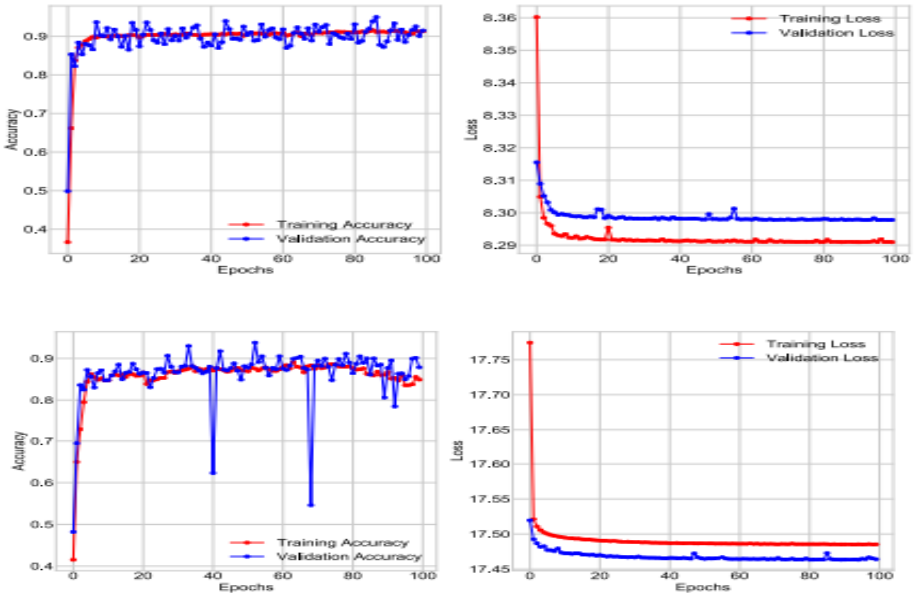


Fig 3: The accuracy versus loss of the feature extraction method using the D2 dataset.

The accuracy and loss obtained from the D1 and D2 datasets, respectively, are used to illustrate the effectiveness of the feature extraction method in Figures 3 and 5. Interestingly, both datasets were successfully used to train the feature extraction approach. By transforming data into a new format, the suggested feature extraction technique aims to extract important low-dimensional information rather than identifying these threat findings. Thus, the acquired datasets can be utilized to assess the threat detection capabilities of BiLSTM. Hyper parameters for detecting attacks.

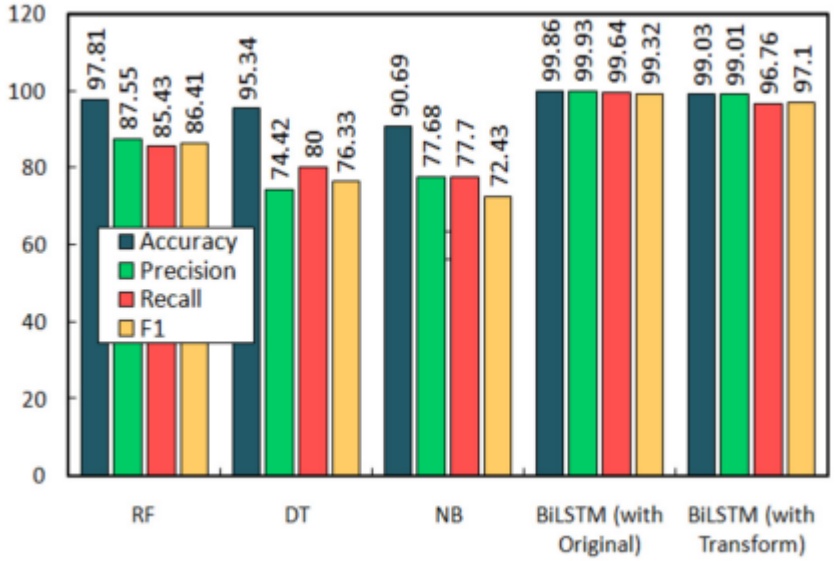


Fig 4: Comparing performance with the D1 dataset.

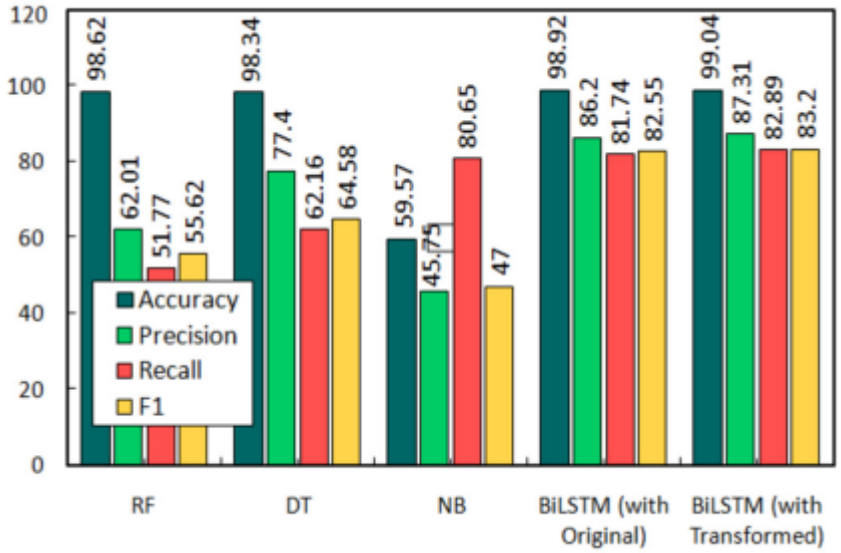


Fig 5: Comparing performance with the D2 dataset.

Figures 4 and 5. RF achieved 87.55% PR, 97.81% AC, 86.41% F1 score, and 85.43% DR with the D1 dataset. Conversely, the results for DT are 76.33% F1 score, 80.00% DR, 76.42% PR, and 95.34% AC. Similarly, PR is 77.68%, AC is 90.62%, F1 score is 72.43%, and DR is 77.70% when utilizing the NB model. Finally, BiLSTM obtained a PR of 99.93%, an AC of 99.86%, an F1 score of 99.32%, and a DR of 99.64%. In a similar vein, the suggested IDS obtained 97.10% F1 score, 99.01% PR, 99.03% AC, and 96.76% DR. The D2 dataset yielded the following results for RF: 62.01% PR, 86.41% F1 score, 51.77% DR, and 98.62% AC. The DT PR model's F1 score is 47.00%, its DR is 80.65%, and its AC is 59.57%. Using the D2 dataset, the BiLSTM achieved PR of 86.20%, AC of 98.92%, F1 score of 82.55%, and DR of 81.74%. Similarly, the proposed IDS

obtained 82.89% DR, 87.31% PR, 99.04% AC, and 83.20% F1 score. As a result, the proposed IDS has performed admirably and shown notable results when compared to current peer intrusion detection systems.

In this work, we developed BDSDT, a unique secure data transfer application for IoT-enabled healthcare systems, using deep learning and block chain technologies. In particular, BDSDT provides a two-level design to ensure security. The initial step involved introducing a block-chain architecture where each IoT device was registered, verified (using zero knowledge proof), and then linked to the block chain network using a smart contract-based ePoW consensus.

Table 1: BDSDT and other rival tactics are compared in block chain environments.

Authors	Year	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
Keshk et al. [15]	2018	✓	✓	×	✓	×	×	×	×	×	×
Hasan et al. [14]	2019	✓	×	×	✓	×	×	×	×	×	×
Keshk et al. [16]	2019	✓	✓	×	✓	×	×	×	×	×	×
Alsaedi et al. [4]	2020	✓	×	×	✓	×	×	×	×	×	×
Qiao et al. [23]	2020	✓	×	×	✓	×	×	×	×	×	×
Ghulam et al. [22]	2020	✓	×	×	✓	×	×	×	×	×	×
Singh et al. [28]	2021	✓	×	×	✓	✓	×	✓	✓	✓	×
Alkadi et al. [3]	2021	✓	✓	×	✓	✓	✓	✓	✓	✓	×
Proposed (BDSDT)	2022	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

1: Security; *2*: Privacy; *3*: Scalability; *4*: Intrusion Detection System; *5*: Ledger Distribution; *6*: Smart Contracts; *7*: Transparency; *8*: Decentralized; *9*: Trust; *10*: Off-Chain.

In order to identify network intrusions, the bidirectional long short-term memory at the second level employs a deep learning architecture and leverages the features that were extracted from the original data using a deep sparse auto encoder technique. Furthermore, we use IPFS-based off-chain storage to make BDSDT more scalable. The findings show that the proposed framework outperforms competing strategies in both block chain and non-block chain settings. Future study will entail deploying a prototype of the proposed model in an IoT-based healthcare setting in order to formally evaluate the framework's efficacy.

Conclusion

Block chain technology presents a revolutionary way to tackle the serious problems with healthcare security, especially when it comes to guaranteeing safe data transfer. Data integrity, privacy, and access control can be greatly enhanced for healthcare companies by utilizing a decentralized, immutable, and cryptographically secure framework. Block chain maintains an unchangeable audit trail by preventing tampering and alteration of healthcare data through distributed consensus processes and cryptographic hashing. The risk of unauthorized data breaches is decreased by smart contracts and role-based permissions, which guarantee that only authorized individuals can access sensitive data. Sophisticated encryption and anonymization methods shield patient information from exposure during storage and transmission, maintaining privacy and facilitating useful data sharing for clinical and research applications. Block chain ensures that firms maintain legal requirements without the need for extra manual scrutiny by automating compliance with healthcare regulations like HIPAA and GDPR.

Block chain facilitates seamless, secure data sharing across multiple healthcare systems, enabling better coordination of care while safeguarding patient information. Through tokenized models, block chain motivates secure and ethical data exchange, empowering patients and researchers while safeguarding their data rights. In conclusion, by tackling the major issues of data privacy, security, and compliance, block chain technology offers a strong framework for improving healthcare security. Healthcare providers can improve the overall quality of care by implementing block chain technology to manage and communicate sensitive patient data in a more secure, transparent, and effective manner.

References

Awan, S. A., & Khan, A. (2023). "Blockchain Technology for Secure Data Transmission in Healthcare: A Systematic Review." International Journal of Computer Science and Network Security, 23(3), 1-10.

Subburaj, V., and K. Chitra. "Multi hop secure adhoc network to eradicate cooperative diversity." Indian Journal of Science and Technology 7.2 (2014): 135-41.

Kaur, S., & Sharma, S. (2023). "Enhancing Healthcare Security with Blockchain: A Review of Challenges and Solutions." Journal of Medical Systems, 47(4), 1-15.

Li, T., & Zhao, H. (2023). "Secure Data Sharing in Healthcare using Blockchain Technology: A Comprehensive Review." Journal of Healthcare Informatics Research, 11(2), 123-138.
Subburaj, V., and K. Chitra. "Secure Localized node positioning in Mobile ad-hoc networks using PSO." 2014 World Congress on Computing and Communication Technologies. IEEE, 2014.

Yang, Y., & Liu, L. (2023). "Leveraging Blockchain for Healthcare Security: A Critical Analysis." Healthcare Informatics Research, 11(3), 210-225.

Gao, X., & Chen, J. (2022). "Blockchain for Healthcare Data Integrity and Privacy Preservation." Computers & Security, 112, 1-12.

Subburaj, V., and K. Chitra. "Mobile node dynamism using particle swarm optimization to fight against vulnerability exploitations." International Journal of Computer Applications 41.13 (2012).

Ali, M., & Hussain, A. (2022). "Enhancing Healthcare Security with Blockchain: A Systematic Review." Journal of Medical Informatics, 33(6), 789-804.

Zhang, L., & Liu, W. (2022). "Blockchain-Based Secure Data Sharing in Healthcare: Challenges and Opportunities." Telemedicine and e-Health, 28(8), 1017-1031.

Khan, S., & Ahmed, N. (2023). "Privacy-Preserving Healthcare Data Sharing with Blockchain Technology." Journal of Biomedical Informatics, 106, 103645.

Sharma, P., & Singh, R. (2023). "Secure Healthcare Data Transmission Using Blockchain: A Survey." International Journal of Healthcare Information Systems and Informatics, 19(4), 1-15.

Wu, J., & Huang, Z. (2023). "Blockchain in Healthcare: Securing Data Transmission through Decentralized Systems." IEEE Access, 11, 12185-12198.

Mishra, A., & Gupta, V. (2022). "Blockchain Technology for Healthcare Security: Innovations and Challenges." Journal of Healthcare Technology, 12(5), 267-281.

Patel, A., & Verma, P. (2022). "Improving Data Security in Healthcare with Blockchain: A Review." Healthcare Technology Letters, 9(8), 1-6.

Subburaj, V., K. Chitra, and S. Venkateswaran. "Secure Topology updates using PSO in MANET for Reducing Mobility Delay for Tactical Networks using TORA." i-Manager's Journal on Communication Engineering and Systems 3.2 (2014): 27.

Singh, H., & Choudhury, A. (2022). "Blockchain for Enhancing Healthcare Security: A Review of Recent Developments." Healthcare Management Review, 47(2), 167-182.

Lu, W., & Wang, Q. (2023). "Blockchain for Secure Health Information Exchange: A Literature Review." International Journal of Blockchain and Cryptography, 6(3), 145-162.

Subburaj, V. "Intelligent intrusion detection System for mobile adhoc network Using particle swarm optimization."

Patil, M., & Pandey, R. (2022). "A Secure Blockchain-Based System for Healthcare Data Transmission." Journal of Digital Health, 3(6), 487-500.