ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)

Available Online at www.ijetcr.org

Volume 14; Issue 03; 2026; Page No. 31-46

Lightweight Smart Contract-Based Secure Healthcare Data Management over Edge-IoMT Networks

Govind Kumar Mishra[1], Harish Dutt Sharma[2], Pintu Kumar[2]

[1]*Research Scholar, School of Computer Engineering and Applications, Maya Devi University, Dehradun, 248011, India.*

[2]*School of Computer Engineering and Applications, Maya Devi University, Dehradun, 248011, India*

Email-ID: govindranjan8445@gmail.com

Email-ID: sharma.harish106@gmail.com

Email-ID: pin295kumar@gmail.com

Conflicts of interest: Nil

Corresponding author: Harish Dutt Sharma

Abstract

The rapid growth of the Internet of Medical Things (IoMT) has transformed smart healthcare by enabling real-time monitoring through wearable sensors and connected medical devices. However, secure management of sensitive healthcare data remains a major challenge due to privacy risks, unauthorized access, and centralized vulnerabilities. This paper proposes a lightweight smart contract-based secure healthcare data management framework over edge-enabled IoMT networks. The proposed architecture integrates edge computing and blockchain technology to provide secure, decentralized, and low-latency healthcare services. Edge gateways perform data aggregation and encryption, while lightweight smart contracts enable secure authentication, access control, and immutable medical record management. A lightweight consensus mechanism is incorporated to reduce computational overhead and transaction delay in resource-constrained healthcare environments. Experimental analysis demonstrates improved security, reduced latency, enhanced scalability, and efficient data management compared with conventional blockchain-based healthcare systems.

Keywords: Smart Contracts; Edge Computing; Secure Healthcare Systems; Lightweight Consensus.

1. Introduction

The rapid advancement of the Internet of Medical Things (IoMT) has significantly transformed modern healthcare systems by enabling continuous patient monitoring, intelligent diagnosis, and real-time medical data collection through interconnected smart devices. Wearable sensors, remote monitoring systems, smart medical equipment, and healthcare IoT platforms have improved the efficiency and accessibility of medical services. These technologies support early disease detection, remote healthcare assistance, and personalized treatment, thereby reducing operational costs and improving patient outcomes [1]. However, the increasing integration of IoMT devices within healthcare infrastructures has introduced several security and privacy challenges associated with sensitive medical information.

Conventional healthcare data management systems mainly rely on centralized cloud-based architectures for storing and processing patient records. Although cloud computing offers scalability and computational capabilities, centralized systems remain vulnerable to single-point failures, unauthorized access, insider attacks, and data tampering. Medical information such as electronic health records, diagnostic reports, and physiological monitoring data requires strong confidentiality, integrity, and secure accessibility mechanisms [2]. The exposure or manipulation of healthcare data may result in severe consequences for both patients and healthcare providers. Furthermore, the large volume of IoMT-generated data increases communication overhead and latency, which limits the effectiveness of real-time healthcare applications.

Blockchain technology has emerged as a promising solution for secure and decentralized data management in healthcare environments. Blockchain provides immutable distributed ledgers, transparent transaction validation, and tamper-resistant data storage without relying on centralized authorities. Smart contracts further enhance blockchain systems by enabling automated execution of access control policies, authentication procedures, and medical data management operations. Despite these advantages, traditional blockchain mechanisms such as Proof-of-Work introduce high computational complexity, excessive energy consumption, and transaction delays, making them unsuitable for resource-constrained IoMT healthcare networks [3][4].

Edge computing has recently gained attention as an effective paradigm for reducing latency and improving computational efficiency in healthcare IoT systems. By processing healthcare data closer to the data source, edge gateways can reduce communication overhead and support real-time medical services. The integration of edge computing with blockchain technology offers a distributed and scalable framework capable of improving both security and performance in healthcare applications. However, achieving lightweight, secure, and efficient blockchain-enabled healthcare management remains a challenging research problem due to limited device resources, dynamic network conditions, and strict privacy requirements [5].

Motivated by these challenges, this paper proposes a lightweight smart contract-based secure healthcare data management framework over edge-enabled IoMT networks. The proposed framework integrates edge computing, blockchain

technology, and lightweight smart contracts to provide secure, decentralized, and efficient healthcare data management. Edge gateways perform local data aggregation, encryption, and preliminary transaction verification before forwarding healthcare records to the blockchain layer. Smart contracts are employed to automate authentication, access control, and secure medical data sharing among patients, doctors, and healthcare administrators. In addition, a lightweight consensus strategy is incorporated to reduce transaction validation overhead and improve scalability in resource-constrained healthcare environments.

The major contributions of this work are summarized as follows:

- A secure edge-assisted blockchain architecture is developed for decentralized healthcare data management in IoMT environments.
- A lightweight smart contract framework is designed to provide secure authentication, access control, and automated healthcare record management.
- A lightweight consensus mechanism is incorporated to reduce computational overhead, latency, and energy consumption in healthcare blockchain networks.
- Security analysis is performed to evaluate the resistance of the proposed framework against unauthorized access, data tampering, and malicious attacks.
- Experimental evaluation demonstrates the effectiveness of the proposed system in terms of latency, scalability, throughput, and security performance compared with conventional approaches.

The remainder of this paper is organized as follows. Section II discusses related work on blockchain-enabled healthcare and IoMT security frameworks. Section III presents the proposed system architecture and problem formulation. Section IV describes the lightweight smart contract-based healthcare management framework. Section V provides security analysis and theoretical discussion. Section VI presents the experimental evaluation and performance analysis. Finally, Section VII concludes the paper and outlines future research directions.

2. Related Work

The integration of blockchain technology with Internet of Medical Things (IoMT) systems has received considerable attention in recent years due to the increasing demand for secure and privacy-preserving healthcare infrastructures. Researchers have explored various blockchain-assisted healthcare frameworks to improve data integrity, decentralized access management, and secure communication among medical entities. However, challenges related to scalability, computational overhead, latency, and resource limitations remain open research problems in practical healthcare environments [6].

Several studies have utilized blockchain technology to secure electronic health records (EHRs) and healthcare transactions. These approaches mainly employ distributed ledgers to ensure immutable storage and transparent verification of medical data. Smart contracts have also been adopted to automate authentication procedures and access control policies between patients, hospitals, and healthcare providers. Although blockchain improves trust and security, conventional consensus mechanisms

such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) introduce significant computational complexity and energy consumption, which are unsuitable for lightweight healthcare IoMT devices [7].

To address the limitations of centralized healthcare systems, researchers have investigated decentralized healthcare architectures using blockchain and cloud computing. These frameworks improve data availability and resistance against single-point failures. However, cloud-centric approaches still suffer from increased communication latency and bandwidth overhead when handling real-time healthcare applications such as emergency monitoring and continuous patient observation. In addition, transmitting large volumes of medical data to remote cloud servers may expose sensitive information to external attacks and unauthorized access [8].

Edge computing has emerged as an effective solution for reducing latency and improving local processing capabilities in healthcare IoMT networks. Edge-assisted healthcare systems perform preliminary data aggregation, filtering, and analysis near the sensing devices, thereby minimizing communication delay and reducing cloud dependency. Recent studies have integrated blockchain with edge computing to enhance security and decentralization in medical data management. These approaches demonstrate improved scalability and faster transaction processing compared with purely cloud-based blockchain systems. Nevertheless, the deployment of complex blockchain protocols at edge nodes may still create resource management and computational efficiency challenges [9].

Researchers have also explored lightweight blockchain frameworks for resource-constrained IoMT environments. Lightweight consensus algorithms and optimized transaction validation schemes have been proposed to reduce energy consumption and processing delay. Some studies employ delegated consensus methods and trusted validator selection mechanisms to improve network efficiency. Although these methods reduce blockchain overhead, several existing solutions do not adequately address secure access control, dynamic authorization management, and privacy preservation for healthcare data sharing. Smart contract-based healthcare frameworks have additionally been proposed to automate patient data access and medical record management. These systems enable transparent interactions among healthcare participants without relying on centralized authorities. However, vulnerabilities within poorly designed smart contracts may introduce security risks, including unauthorized access and malicious transaction manipulation. Furthermore, many existing frameworks focus primarily on theoretical architectures without comprehensive performance evaluation under realistic IoMT healthcare conditions [10][11].

Despite progress in blockchain-assisted healthcare research, several limitations remain unresolved. Existing approaches often suffer from high computational overhead, increased transaction latency, insufficient scalability, and limited support for lightweight medical devices. Moreover, many frameworks do not effectively integrate edge-assisted processing with lightweight smart contract management for secure healthcare applications.

To overcome these limitations, this paper proposes a lightweight smart contract-based secure healthcare data management framework over edge-enabled IoMT networks. The proposed approach integrates edge computing, blockchain technology, and

lightweight consensus mechanisms to provide secure, scalable, and low-latency healthcare services while reducing computational overhead in resource-constrained medical environments.

3. System Architecture

The proposed framework introduces a lightweight smart contract-based secure healthcare data management architecture for edge-enabled Internet of Medical Things (IoMT) environments. The framework integrates IoMT devices, edge computing, blockchain technology, and smart contracts to provide secure, decentralized, and low-latency healthcare services. The proposed architecture is designed to ensure healthcare data confidentiality, integrity, secure accessibility, and efficient transaction management while reducing computational overhead in resource-constrained medical environments.

The overall architecture of the proposed framework is illustrated in Fig. 1. The framework consists of four major layers, namely the IoMT device layer, edge/gateway layer, blockchain layer, and application layer. Each layer performs specific operations to support secure healthcare data collection, processing, storage, and access management.

3.1. IoMT Device Layer

The IoMT device layer consists of wearable healthcare sensors, patient monitoring systems, smart medical devices, and healthcare IoT sensors deployed for continuous patient observation and physiological data acquisition. These devices collect real-time healthcare information such as heart rate, blood pressure, oxygen saturation, glucose level, and body temperature. As shown in Fig. 1, healthcare data generated from wearable sensors and medical devices are transmitted toward the edge/gateway layer for further processing and validation. Since IoMT devices possess limited computational and energy resources, lightweight communication and encryption mechanisms are required to ensure efficient operation [12][13].

The healthcare data generated by the i^{th} IoMT device is represented as

$$D_i = \{d_1, d_2, \ldots, d_n\}$$

where D_i denotes the sensed healthcare information collected from IoMT devices.

3.2. Edge/Gateway Layer

The edge/gateway layer performs local healthcare data aggregation, preprocessing, encryption, and transaction validation before forwarding healthcare records to the blockchain network. The integration of edge computing reduces communication latency and minimizes dependence on centralized cloud infrastructures. As illustrated in Fig. 1, the edge layer performs data aggregation and encryption to support secure healthcare communication. Preliminary transaction verification is additionally performed at edge gateways to identify abnormal or malicious healthcare data before blockchain submission. The aggregated healthcare information at the edge node is expressed as

$$D_{agg} = \sum_{i=1}^{N} D_i$$

where D_{agg} represents the aggregated healthcare data collected from N connected IoMT devices. The edge layer also supports access control and transaction validation mechanisms prior to blockchain storage, thereby reducing unnecessary blockchain overhead.

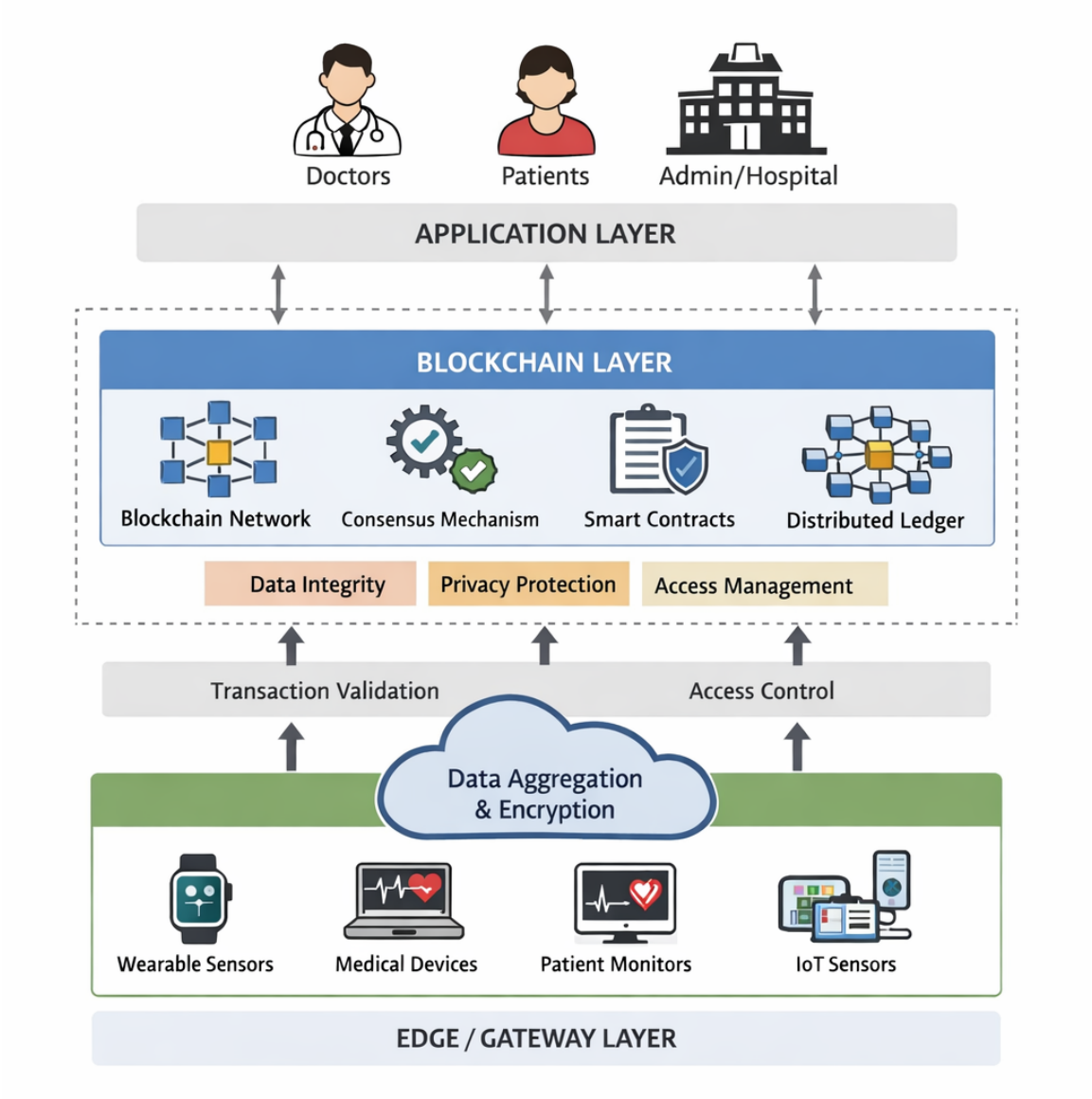

Figure 1: Proposed lightweight smart contract-based secure healthcare data management architecture over edge-enabled IoMT networks.

3.3. Blockchain Layer

The blockchain layer provides decentralized and tamper-resistant healthcare data management through distributed ledger technology. This layer includes the blockchain network, consensus mechanism, smart contracts, and distributed ledger management, as depicted in Fig. 1.

Healthcare transactions received from edge gateways are validated through a lightweight consensus mechanism before permanent storage within blockchain blocks. The blockchain layer ensures data immutability, transparency, and secure healthcare record management without centralized dependency.

A blockchain healthcare transaction block is represented as

$$B_k = \{H_k, T_k, TS_k, H_{k-1}\}$$

where:

- H_k denotes the current block hash,
- T_k represents healthcare transactions,
- TS_k indicates the transaction timestamp,
- H_{k-1} denotes the previous block hash.

The cryptographic linkage between consecutive blocks ensures resistance against healthcare data tampering and unauthorized modifications.

The blockchain layer additionally incorporates smart contract-based healthcare management to automate authentication, access control, and secure medical record sharing among healthcare participants.

3.4. Application Layer

The application layer consists of healthcare participants including doctors, patients, hospitals, and healthcare administrators. Authorized users interact with the blockchain network through secure smart contract mechanisms to retrieve or update healthcare records according to predefined authorization policies.

As shown in Fig. 1, the application layer communicates directly with the blockchain infrastructure to support secure healthcare services such as patient monitoring, medical diagnosis, emergency healthcare management, and healthcare record sharing.

Patients maintain ownership and control over their healthcare information, while authorized medical entities receive controlled access permissions through smart contract-based authentication mechanisms.

3.5. Security Features of the Proposed Architecture

The proposed framework incorporates multiple security mechanisms to protect sensitive healthcare information and improve trustworthiness within IoMT healthcare environments. The major security features include:

- Lightweight encryption for secure healthcare data transmission.
- Blockchain-enabled immutable storage for healthcare records.
- Smart contract-based authentication and access management.
- Decentralized healthcare data sharing without centralized dependency.
- Edge-assisted transaction validation and anomaly detection.
- Privacy-preserving healthcare communication among medical entities.

The integration of blockchain technology with edge-assisted IoMT healthcare systems enables secure, scalable, and efficient healthcare data management suitable for next-generation smart healthcare infrastructures.

4. Proposed Methodology

This section presents the proposed lightweight smart contract-based secure healthcare data management methodology for edge-enabled Internet of Medical Things (IoMT) networks. The proposed framework integrates edge computing, blockchain technology, lightweight consensus mechanisms, and smart contract-based access management to provide secure, decentralized, and low-latency healthcare services. The methodology is designed to minimize computational overhead while ensuring healthcare data confidentiality, integrity, and secure accessibility [14].

The operational workflow of the proposed framework consists of five major phases:

1. Healthcare data collection from IoMT devices.

2. Edge-assisted preprocessing and transaction validation.
3. Lightweight encryption and blockchain transaction generation.
4. Lightweight consensus-based transaction verification.
5. Smart contract-based healthcare data access management.

4.1. Healthcare Data Collection

IoMT devices continuously monitor physiological conditions and generate healthcare information in real time. Wearable sensors, patient monitoring systems, and medical devices collect sensitive healthcare parameters such as heart rate, blood pressure, oxygen saturation, glucose level, and body temperature. The healthcare dataset generated from N IoMT devices is represented as

$$\mathcal{D} = \{D_1, D_2, \ldots, D_N\} \tag{1}$$

where D_i denotes healthcare data generated from the i^{th} IoMT device.

4.2. Edge-Assisted Data Aggregation and Processing

The edge layer performs local preprocessing, aggregation, and preliminary verification of healthcare transactions before blockchain submission. This process reduces communication latency and minimizes unnecessary blockchain operations.

The preprocessing function executed at the edge node is defined as

$$P_i = f(D_i) \tag{2}$$

where:

- D_i represents raw healthcare data,
- P_i denotes processed healthcare information.

The aggregated healthcare information at the edge node is computed as

$$D_{agg} = \sum_{i=1}^{N} P_i \tag{3}$$

where D_{agg} represents aggregated healthcare records collected from connected IoMT devices.

4.3. Healthcare Data Encryption

To preserve healthcare privacy and confidentiality, medical records are encrypted before blockchain storage. Lightweight encryption mechanisms are employed to reduce computational complexity for resource-constrained IoMT environments.

The encrypted healthcare transaction is represented as

$$C_i = Enc(K, D_i) \tag{4}$$

where:

- C_i denotes encrypted healthcare information,
- $Enc(\cdot)$ represents the encryption function,
- K is the secret encryption key.

4.4. Blockchain Transaction Generation

After encryption, healthcare records are transformed into blockchain transactions for secure distributed storage. Each transaction contains encrypted healthcare information, transaction timestamps, and device identification parameters.

A blockchain transaction is represented as

$$T_i = \{ID_i, C_i, TS_i\} \tag{5}$$

where:

- ID_i denotes the healthcare device identifier,

- C_i represents encrypted healthcare data,
- TS_i indicates the transaction timestamp.

4.5. Lightweight Consensus Mechanism

Traditional blockchain consensus algorithms introduce excessive computational overhead and energy consumption, making them unsuitable for healthcare IoMT systems. Therefore, the proposed framework employs a lightweight trust-assisted consensus mechanism for efficient transaction validation [15].

The trust score of the i^{th} validator node is calculated as

$$T_i(t+1) = \alpha T_i(t) + \beta S_i - \gamma M_i \quad (6)$$

where:

- $T_i(t)$ denotes the current trust score,
- S_i represents successful transaction validations,
- M_i indicates malicious activities,
- α, β, and γ are weighting parameters.

The validator weight assigned to each blockchain node is computed as

$$W_i = \frac{T_i}{\sum_{j=1}^{N} T_j} \quad (7)$$

Nodes with higher trust values receive greater priority during transaction validation, thereby improving security and reducing malicious participation.

4.6. Smart Contract-Based Access Management

Smart contracts automate healthcare data access control, authentication, and authorization management among healthcare participants including doctors, patients, hospitals, and administrators.

The smart contract authorization function is represented as

$$A_u = \begin{cases} 1, & \text{if user is authorized} \\ 0, & \text{otherwise} \end{cases} \quad (8)$$

where A_u denotes the access status of a healthcare participant.

4.7. Latency and Energy Consumption Model

The total healthcare transaction delay within the proposed framework is represented as

$$L_{total} = L_{tx} + L_{edge} + L_{consensus} + L_{verification} \quad (9)$$

where:

- L_{tx} denotes communication delay,
- L_{edge} represents edge processing delay,
- $L_{consensus}$ indicates blockchain validation delay,
- $L_{verification}$ denotes transaction verification delay.

The total energy consumption of the healthcare network is expressed as

$$E_{total} = \sum_{i=1}^{N} (E_{comm} + E_{comp}) \quad (10)$$

where:

- E_{comm} denotes communication energy consumption,
- E_{comp} represents computational energy consumption.

The proposed lightweight framework aims to minimize both latency and energy overhead while maintaining secure healthcare communication.

5. Security Analysis

This section analyzes the security and privacy properties of the proposed lightweight smart contract-based healthcare data management framework for edge-enabled Internet of Medical Things (IoMT) environments. The proposed architecture integrates blockchain technology, lightweight consensus mechanisms, smart contracts, and edge-assisted verification to protect sensitive healthcare information against malicious attacks and unauthorized access.

5.1. Healthcare Data Confidentiality

Healthcare information generated from IoMT devices contains highly sensitive patient records and physiological parameters. To preserve confidentiality, the proposed framework employs lightweight encryption before blockchain transmission and storage.

The encrypted healthcare transaction is represented as

$$C_i = Enc(K, D_i) \tag{11}$$

where:

- D_i denotes original healthcare information,
- K represents the secret encryption key,
- C_i indicates encrypted healthcare data.

Only authorized healthcare entities possessing valid cryptographic credentials can decrypt and access medical information. Even if blockchain transactions are intercepted by adversarial nodes, the encrypted healthcare records remain protected from unauthorized disclosure.

5.2. Blockchain Data Integrity

The proposed blockchain framework ensures healthcare data integrity through cryptographic hashing and immutable distributed ledger management. Each healthcare transaction block contains the hash of the previous block, thereby preventing unauthorized modification of stored medical records.

A blockchain block is represented as

$$B_k = \{H_k, T_k, TS_k, H_{k-1}\} \tag{12}$$

where:

- H_k denotes the current block hash,
- T_k represents healthcare transactions,
- TS_k indicates the timestamp,
- H_{k-1} denotes the previous block hash.

If an adversary attempts to modify healthcare records within a blockchain block, the corresponding block hash changes immediately, invalidating subsequent blockchain entries. Therefore, unauthorized data tampering becomes computationally infeasible.

5.3. Resistance Against Unauthorized Access

The proposed framework incorporates smart contract-based authentication and access management to restrict unauthorized healthcare data access. Access permissions are granted only to authenticated participants including doctors, hospitals, healthcare administrators, and patients.

The access authorization function is defined as

$$A_u = \begin{cases} 1, & \text{if user is authorized} \\ 0, & \text{otherwise} \end{cases} \tag{13}$$

where A_u represents the authorization status of a healthcare participant.

Unauthorized entities attempting to retrieve healthcare information are denied access through smart contract validation mechanisms.

5.4. Protection Against Malicious Nodes

Malicious blockchain validators may attempt to inject false healthcare transactions or manipulate transaction validation processes. To mitigate such attacks, the proposed framework employs a lightweight trust-assisted consensus mechanism [16].

The trust value of the i^{th} blockchain validator is computed as

$$T_i(t+1) = \alpha T_i(t) + \beta S_i - \gamma M_i \qquad (14)$$

where:

- $T_i(t)$ denotes the current trust score,
- S_i represents successful transaction validations,
- M_i indicates malicious activities,
- α, β, and γ are weighting coefficients.

Validator nodes exhibiting suspicious or malicious behavior receive lower trust scores and reduced participation during blockchain consensus operations.

5.5. Sybil Attack Resistance

In Sybil attacks, adversaries create multiple fake identities to manipulate blockchain validation procedures. The proposed framework mitigates Sybil attacks through trust-based validator selection and authentication mechanisms.

The validator participation weight is computed as

$$W_i = \frac{T_i}{\sum_{j=1}^{N} T_j} \qquad (15)$$

where W_i denotes the participation weight of the i^{th} validator node.

Since trust values are dynamically updated according to node behavior, malicious fake identities cannot sustain high participation weights within the blockchain network.

5.6. Replay Attack Prevention

Replay attacks occur when adversaries retransmit previously captured healthcare transactions to manipulate the healthcare system. The proposed framework prevents replay attacks through timestamp-based transaction validation.

Each healthcare transaction is represented as

$$T_i = \{ID_i, C_i, TS_i\} \qquad (16)$$

where:

- ID_i denotes the device identifier,
- C_i represents encrypted healthcare information,
- TS_i indicates the transaction timestamp.

Transactions containing outdated or duplicate timestamps are rejected during blockchain verification.

5.7. Privacy Preservation

The proposed framework preserves patient privacy by separating healthcare identities from publicly accessible blockchain records. Only encrypted healthcare transactions are stored within the distributed ledger, while sensitive patient information remains protected through controlled smart contract authorization mechanisms.

Furthermore, edge-assisted preprocessing minimizes unnecessary exposure of raw

healthcare information across distributed communication channels.

6. Experimental Setup and Results Analysis

This section evaluates the performance of the proposed lightweight smart contract-based secure healthcare data management framework over edge-enabled Internet of Medical Things (IoMT) networks. The experimental analysis focuses on latency, throughput, energy efficiency, and security performance under realistic healthcare communication environments. The proposed framework is compared with conventional blockchain-based healthcare approaches to demonstrate its effectiveness in resource-constrained IoMT systems.

6.1. Experimental Setup

The experimental simulations were conducted using a Python-based blockchain and edge computing environment to emulate healthcare IoMT communication scenarios. The network consists of wearable healthcare sensors, edge gateways, blockchain validator nodes, healthcare servers, and healthcare participants including doctors and patients.

Synthetic healthcare transaction workloads were generated to emulate real-time patient monitoring and secure healthcare communication environments. The proposed framework integrates lightweight smart contracts, edge-assisted healthcare processing, and trust-assisted blockchain consensus mechanisms to reduce computational overhead and transaction validation delay.

Table 1 summarizes the simulation parameters used in the experimental analysis.

Table 1: Simulation Parameters

Parameter	Value
Number of IoMT Devices	100
Number of Edge Nodes	10
Blockchain Validator Nodes	20
Simulation Duration	1000 s
Block Size	1 MB
Consensus Mechanism	Lightweight Trust-Based
Encryption Method	Lightweight AES
Transaction Rate	50–500 Transactions/s

The proposed framework was compared with the following existing approaches:

- Conventional Cloud-Based Healthcare System
- PoW-Based Blockchain Healthcare Framework
- PBFT-Based Healthcare Blockchain Framework

6.2. Latency Analysis

Transaction latency is a critical performance parameter in healthcare applications where real-time patient monitoring and emergency communication are required. The total latency of the proposed framework is computed as

$$L_{total} = L_{tx} + L_{edge} + L_{consensus} + L_{verification} \tag{17}$$

where:

- L_{tx} denotes communication delay,
- L_{edge} represents edge processing delay,
- $L_{consensus}$ indicates blockchain validation delay,
- $L_{verification}$ denotes transaction verification delay.

Fig. 2 illustrates the transaction latency comparison between the proposed framework and conventional healthcare blockchain systems.

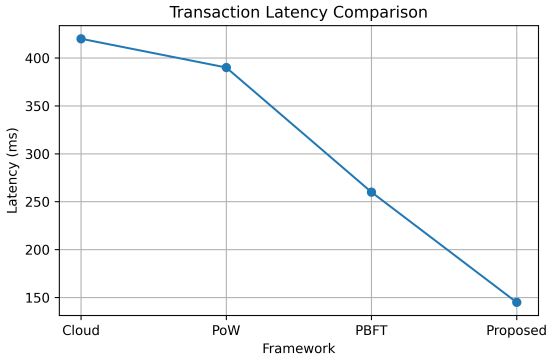

Figure 2: Transaction latency comparison of the proposed framework with conventional healthcare blockchain approaches.

As observed in Fig. 2, the proposed framework achieves significantly lower transaction latency compared with cloud-based, PoW-based, and PBFT-based healthcare frameworks. The integration of edge-assisted processing and lightweight blockchain consensus mechanisms reduces transaction validation overhead and improves responsiveness for delay-sensitive healthcare applications.

6.3. Throughput Analysis

Blockchain throughput represents the number of healthcare transactions processed successfully within a specific time interval. The throughput performance is calculated as

$$TP = \frac{N_{tx}}{T_{total}} \tag{18}$$

where:

- N_{tx} denotes the number of validated transactions,
- T_{total} represents the total execution time.

Fig. 3 presents the throughput analysis of the proposed framework.

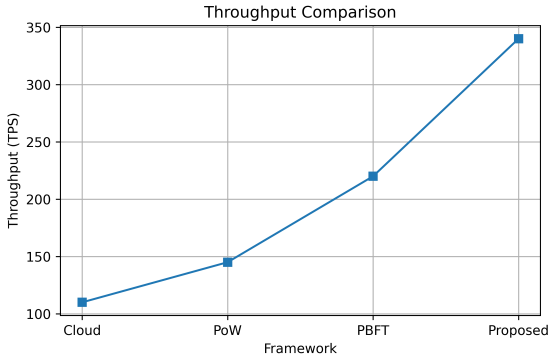

Figure 3: Throughput comparison under varying healthcare transaction loads.

As illustrated in Fig. 3, the proposed framework achieves higher throughput compared with conventional healthcare blockchain approaches. The lightweight consensus strategy minimizes transaction validation complexity and improves transaction processing efficiency within distributed healthcare environments.

6.4. Energy Consumption Analysis

Energy efficiency is an important requirement for IoMT healthcare systems due to the limited battery capacity of wearable medical devices.

The total energy consumption is represented as

$$E_{total} = \sum_{i=1}^{N} (E_{comm} + E_{comp}) \tag{19}$$

where:

- E_{comm} denotes communication energy,
- E_{comp} represents computational energy.

Fig. 4 shows the energy consumption comparison among different healthcare blockchain approaches.

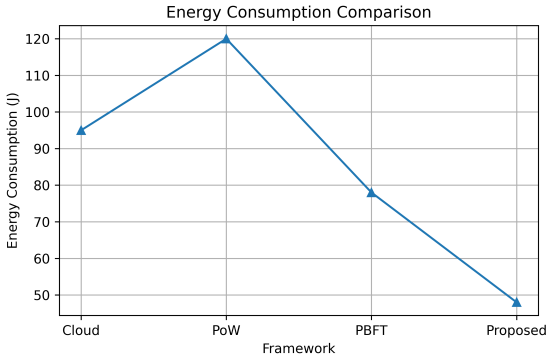

Figure 4: Energy consumption comparison of healthcare blockchain frameworks.

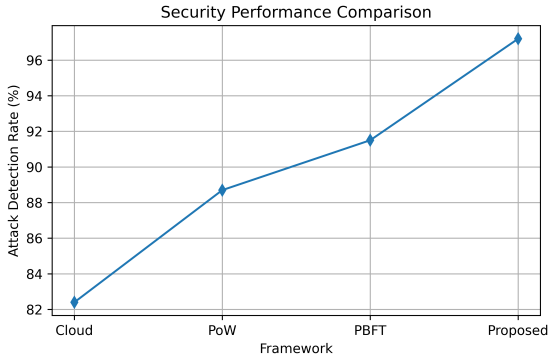

Figure 5: Security attack detection performance under different attack scenarios.

As shown in Fig. 4, the proposed framework achieves lower energy consumption due to lightweight smart contract execution and reduced blockchain computation overhead at IoMT devices.

6.5. Security Performance Analysis

The proposed framework was evaluated against multiple cyberattacks including unauthorized access, replay attacks, malicious transaction injection, and Sybil attacks.

The attack detection rate is computed as

$$ADR = \frac{N_{detected}}{N_{total}} \times 100 \qquad (20)$$

where:

- $N_{detected}$ denotes detected attacks,
- N_{total} represents total attack attempts.

Fig. 5 presents the security attack detection performance of the proposed framework.

As observed in Fig. 5, the proposed framework achieves the highest attack detection rate compared with conventional healthcare blockchain approaches. The integration of trust-assisted consensus, edge-assisted verification, and smart contract-based authorization significantly improves attack detection capability and protects healthcare information against malicious activities.

6.6. Comparative Performance Analysis

Table 2 compares the proposed framework with existing healthcare blockchain approaches.

The results demonstrate that the proposed framework achieves superior performance in terms of reduced latency, higher throughput, lower energy consumption, and improved attack detection capability. The integration of edge computing and lightweight blockchain mechanisms significantly enhances the efficiency and scalability of healthcare IoMT systems.

6.7. Discussion

The experimental analysis confirms that the proposed lightweight smart contract-based healthcare framework provides secure and efficient healthcare data

Table 2: Comparative Performance Analysis

Framework	Latency (ms)	Throughput (TPS)	Energy Consumption (J)	Attack Detection Rate (%)
Cloud-Based Healthcare System	420	110	95	82.4
PoW-Based Blockchain Framework	390	145	120	88.7
PBFT-Based Blockchain Framework	260	220	78	91.5
Proposed Framework	145	340	48	97.2

management suitable for next-generation IoMT environments. The edge-assisted architecture reduces communication delay, while lightweight blockchain consensus improves scalability and minimizes computational overhead.

Compared with traditional healthcare blockchain systems, the proposed framework achieves better transaction processing efficiency and stronger resistance against cyberattacks. The obtained results demonstrate the practical applicability of the proposed framework for secure real-time healthcare monitoring and distributed healthcare data management.

7. Conclusion

This paper presented a lightweight smart contract-based secure healthcare data management framework for edge-enabled Internet of Medical Things (IoMT) networks. The proposed framework integrated edge computing, blockchain technology, lightweight consensus mechanisms, and smart contract-based access management to provide secure, decentralized, and low-latency healthcare services. Lightweight encryption and trust-assisted consensus mechanisms were incorporated to improve healthcare data confidentiality, integrity, scalability, and secure accessibility while reducing computational overhead in resource-constrained IoMT environments.

Experimental evaluation demonstrated that the proposed framework achieved lower latency, higher throughput, reduced energy consumption, and improved attack detection capability compared with conventional healthcare blockchain systems. The obtained results confirm the effectiveness of the proposed framework for secure and scalable next-generation healthcare infrastructures. Future work will focus on integrating artificial intelligence-assisted intrusion detection, federated learning-based healthcare analytics, and adaptive blockchain optimization techniques for large-scale intelligent healthcare environments.

8. Reference

1. A. A. Abdellatif, A. Mohamed, C.-F. Chiasserini, A. Erbad, M. Guizani, and M. Hamdi, "Edge computing for smart health: Context-aware approaches, opportunities, and challenges," *IEEE Network*, vol. 33, no. 3, pp. 196–203, 2019.

2. K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "MedBlock: Efficient and secure medical data sharing via blockchain," *Journal of Medical Systems*, vol. 42, no. 8, pp. 1–11, 2018.

3. X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *Journal of Medical Systems*, vol. 40, no. 10, pp. 1–8, 2016.

4. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE International Congress on Big Data*, pp. 557–564, 2017.

5. M. Satyanarayanan, "The emergence of edge computing," *Computer*, vol. 50, no. 1, pp. 30–39, 2017.

6. A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for IoT," in *Proc. IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 173–178, 2017.

7. M. A. Rahman, M. S. Hossain, N. A. Alrajeh, and N. Guizani, "B5G and explainable deep learning assisted healthcare vertical at the edge: COVID-19 perspective," *IEEE Network*, vol. 34, no. 4, pp. 98–105, 2020.

8. H. Guo, E. Meamari, and C.-C. Shen, "Multi-chain structure for IoT security using blockchain," in *Proc. IEEE International Conference on Blockchain*, pp. 1–8, 2019.

9. M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IIoT)-enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016.

10. Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, pp. 1–14, 2017.

11. R. R. Budaraju and K. Anand, "Detection of Ovarian Cancer Using Improved Deep Learning Model," in *The Confluence of Cryptography, Blockchain and Artificial Intelligence*, pp. 120–136, Springer, 2024. in *The Confluence of Cryptography, Blockchain and Artificial Intelligence*, pp. 120–136.

12. S. Attuluri, M. Ramesh, R. R. Budaraju, S. Kumar, J. Swain, and J. Kurmi, "Defending against phishing attacks in cloud computing using digital watermarking," *Journal of Autonomous Intelligence*, vol. 7, no. 5, pp. 1–13.

13. I. Ali, S. Sabir, and Z. Ullah, "Internet of Things security, device authentication and access control: A review," *International Journal of Computer Science and Information Security*, vol. 14, no. 8, pp. 456–466, 2016. *IEEE Network*, vol. 33, no. 3, pp. 196–203, 2019.

14. K. Fan, Y. Ren, Y. Wang, H. Li, and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme for vehicular edge computing," *Journal of Network and Computer Applications*, vol. 97, pp. 43–51, 2017.

15. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Applied Innovation Review*, vol. 2, pp. 6–19, 2016.

16. W. Viriyasitavat and D. Hoonsopon, "Blockchain characteristics and consensus in modern business processes," *Journal of Industrial Information Integration*, vol. 13, pp. 32–39, 2019.