FUDMA Journal of Sciences (FJS)
ISSN online: 2616-1370
ISSN print: 2645 - 2944
Vol. 10 No. 3, February, 2026, pp 245 – 251
DOI: https://doi.org/10.33003/fjs-2026-1003-4793

FRAMEWORK OF A LIGHTWEIGHT BLOCKCHAIN-BASED MODEL FOR SECURE INTERNET OF MEDICAL THINGS (IOMT) DATA MANAGEMENT

***[1]Leke Joseph Oloruntoba and [2]Afolayan Ayodele Obiniy**

[1]Kogi State Polytechnic Lokoja, Kogi State, Nigeria.
[2]Federal University Lokoja, Kogi State, Nigeria.

*Corresponding authors' lekejoe@gmail.com

ABSTRACT

The widespread adoption of the Internet of Medical Things (IoMT) is the main factor that brought about big changes in the healthcare system but also at the same time made the system struggle with major issues like data breaches, device incompatibility, scalability problems, delays, and cyber security risks. The conventional security procedures and central cloud storage systems are always limited if one looks at the throughput, cost of implementation, and failure points along with threats to security that are associated with them. This research proposed a lightweight blockchain-based system for the protection of IoMT data while concurrently tackling the issues of performance and scalability. The proposed system consists of six interconnected layers: IoMT device layer, lightweight encryption layer, interoperability layer, lightweight consensus layer, blockchain network layer, and the InterPlanetary File System (IPFS) storage layer. In this architecture, IPFS has been picked as a replacement for traditional cloud storage with an intention to allow decentralized, tamper-proof, and efficient management of medical data. A lightweight consensus mechanism which is specifically designed for IoMT devices that consume low power and are resource constrained is incorporated into the system to bring down transaction processing overhead and at the same time raise system responsiveness. The proposed framework provides a high level of throughput with a low latency when executing transactions ranging from 50 transactions to 5000 transactions. Furthermore, the framework has low computation time, reduced memory usage, minimal processor utilization and low energy consumption which confirms that it is efficient in terms of resource constrained IoMT devices. The results of this study demonstrate that the proposed framework provides an effective, secure and scalable solution for the management of IoMT data and therefore can be applied to real-time applications in healthcare.

Keywords: Internet of Medical Things (Iomt), Blockchain Technology, Interoperability, Data Security, Consensus Mechanism, Lightweight Cryptography

INTRODUCTION

Internet of Medical Things (IoMT) serve as transformative technologies in medical care by means of remote patient monitoring, real-time analytics, and enhanced clinical outcomes. However, IoMT systems contain sensitive data and typically run on devices possessing limited computational and deterioration capabilities, which, therefore, might call for their very own efficient yet secure frameworks. Traditional implementations of blockchains, such as the Proof-of-Work mechanism, place upon them computational-hardness requirements not suitable for IoMT environments. Another promising approach came recently with the integration of fog computation and lightweight consensus mechanisms (Cheikhrouhou et al., 2023). For sure, lightweight cryptographic primitives such as hybrid chaotic encryption methods have been shown to offer both security and efficiency in healthcare IoT (Rasheed & Kumar., 2025). In view of the, this paper describes the methodological framework for a lightweight blockchain model oriented toward IoMT in its six main phases. The intricate nature of IoMT ecosystems requires a methodical approach for designing a lightweight and secure blockchain framework. IoMT networks are inherently heterogeneous, comprising wearable sensors, implantable medical devices, cloud services, and Electronic Health Record (EHR) systems, each with varying computational and communication capabilities. According to Ghadi et al. (2024), blockchain integration in IoMT systems must satisfy three fundamental requirements while remaining compatible with low-power medical devices. These requirements include security, scalability, and interoperability. Therefore, a well-defined methodological framework is necessary to align encryption mechanisms with consensus protocols and interoperability layers, while minimizing the computational burden on resource-constrained IoMT devices.

The literature has recently pointed out how fog and edge computing can be harnessed to facilitate the secure sharing of IoMT data. Cheikhrouhou et al. (2023) stated that fog-assisted lightweight blockchain architecture reduces latency and improves real-time responsiveness, which is essential for any life-critical medical intervention. In parallel, Othman et al. (2025) present their hybrid distributed storage and blockchain model with ring-based access control, evidence that carefully crafted lightweight consensus- and storage-mechanism designs achieve transaction finality in milliseconds while ensuring patient privacy. These results emphasize that the design consideration and methodological framework of a lightweight blockchain-based IoMT model must give priority to efficiency, scalability, and regulatory requirements.

In addition, authentication and privacy-preservation mechanisms also concern the study. Xie et al. (2024) presented a three-factor blockchain authentication scheme utilizing decentralized consensus and anonymity protection measures to protect against data leakage; in other words, the schemes cannot rely on central authority for secure data exchange among medical clusters. Likewise, Fugkeaw et al. (2023) propose the LightMED framework to combine lightweight attribute-based encryption with blockchain-enabled fog nodes to offer fine-grained access control to electronic medical records. These approaches show the methodological need of pairing lightweight encryption with decentralized authentication to balance ease of use with robust

data security in the IoMT. Lightweight cryptographic primitives are the other critical constituents of the proposed model. Aboshosha et al. (2025) presents a blockchain-driven hashing framework optimized for medical IoT devices, offering robust authentication with minimal energy overhead. Through these developments, cryptographic efficiency directly delineates the methodology of how an IoMT blockchain is constituted.

From a conceptual angle, Stefanescu et al., (2022) emphasize that "lightweight" blockchain frameworks must be understood across multiple methodological dimensions: architecture, consensus, authentication, cryptography, and storage. In alignment with this taxonomy, a six-phase methodological framework is advanced in this paper to govern these dimensions in a systematic fashion: IoMT architectural layering; lightweight encryption design; interoperability mechanisms; consensus adaptation; blockchain network integration; and distribute storage enabled by InterPlanetary File System (IPFS). Together, these phases collectively form a comprehensive theory for the design of a proficiently sleazy efficient IoMT data management framework, being compatible with constrained environments while still being compliant with data protection requirements such as Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR).

In line with this principle, this therefore intends to present a structured methodological model summarizing theoretical learning and practical implementation strategies. In mapping a clear methodological route, the work provides an avenue of later empirical confirmation and equips researchers and practitioners alike with a reusable skeleton for secure, scalable, and efficient IoMT data management.

Related Work

Several works as explore the security of IoMT using blockchain, for instance, privacy-preserving, permissioned blockchain frameworks are witnessed using Elliptic Curve Cryptography (ECC) and off-chain storage to strengthen confidentiality and authentication (Alabdulatif, 2024). Likewise, lightweight and weak encryption protocols emerged in 2025, integrating ECC-based blind signatures for IoMT security and anonymity needs (Samal, et al., 2025). Simultaneously, Ascon (a lightweight cryptographic algorithm) was being pushed as the de facto lightweight cipher for constrained devices from the standpoint of a pleasing balance between security and performance in the National Institute of Standards and Technology (NIST) standardization (Dobraunig et al., 2021). Comprehensive surveys emphasize lightweight security algorithms that feature low-power consumption, latency, and area footprint for IoT infrastructure (Singh et al., 2024). In contrast, blockchain-enabled IoMT authentication schemes with edge computing or mobile edge integration accentuate modular methodological design (Sharma et al., 2024).

Apart from authentication, researchers have also diverted their attention to lightweight consensus mechanisms designed to minimize computational overheads inherent to traditional protocols, such as those based on Proof-of-Work. Othman et al. (2025) present a hybrid distributed ledger with selective ring-based access control and transaction validation occurring at the millisecond level, thereby illustrating the possibility of employing blockchains in latency-sensitive IoMT scenarios. Along the same line, Cheikhrouhou et al. (2023) proposed fog computing integration with lightweight consensus to increase transaction throughput and ensure timely access to medical data. These methods emphasize that carefully crafted consensus algorithms form the methodological backbone of IoMT blockchain frameworks.

Another line of work focuses on secure and scalable storage integration. Aboshosha et al. (2025) proposed a blockchain-based lightweight hashing scheme for IoMT devices that, while reducing storage and computation requirements, does not decrease the level of guarantees regarding integrity. Furthermore, the use of decentralized storage systems, such as IPFS, has been proposed for secure off-chain handling of medical data with little redundancy (Jayabalan & Jeyanthi. 2022). It is very much in line with the need for a layered methodological framework that separates on-chain transactions from large-scale data storage for auditability.

Interoperability and layered designs are also under investigation among researchers in the blockchain-based IoMT field. Farshadinia et al. (2025) presents a multi-layer model consisting of blockchain with Elliptic Curve Digital Signature Algorithm- Zhang-Safavi- Naini-Susilo Signature (ECDSA-ZSS) hybrid cryptography and credential auditing to allow for flexibility across heterogeneous devices. This resonates with the design principle of decomposing IoMT security into separate phases of encryption, authentication, consensus, and storage. Furthermore, surveys like Reegu et al. (2023) highlight interoperability standards and compliance with regulatory frameworks (such as HIPAA, G DPR) as a key aspect making any IoMT blockchain deployment practically viable.

In a more hybrid-driven approach, federated learning and blockchains are combined to allow real-time medical analytics and data privacy simultaneously. Ba et al. (2024) stated that, if implemented, federated IoMT frameworks distribute computation among medical devices while the blockchain instills trust and verifiability. Blockchain has emerged as a promising solution for enhancing transparency, security, and efficiency in modern data-driven systems (Okoli et al., 2024). This confluence of federated AI, lightweight crypto, and blockchain consensus serves to underscore the imperative for a methodologically crafted approach to secured and efficient IoMT data handling.

Finally, the existing literature suggests that in terms of lightweight cryptography, consensus optimization, and decentralized storage, significant progress has been made, but an end-to-end methodological framework is less discussed. This creates a knowledge gap that motivates this study, which constructs a six-phase blueprint and methodological framework of a lightweight blockchain model for secure IoMT data management, combining cryptographic efficiency, consensus flexibility, interoperability, and decentralized storage into one cohesive framework.

System analysis is an essential stage in the design of a blockchain-enabled IoMT framework, this determines the functional and non-functional requirements that will be met for the system to operate securely and efficiently. (Khatter, K & DevanjaliRelan., 2022). The IoMT devices are under severe constraints of computation, energy, and communication, while simultaneously working with highly sensitive medical data that demand high security preferences (Papaioannou et al., 2022). Therefore, analyzing the set of requirements for confidentiality, computational efficiency, scalability, interoperability, and consensus builds the foundation of a lightweight but secure methodological framework.

i. Data Confidentiality and Integrity: Medical data must remain confidential and must not be altered at any time during storage or transmission. Unauthorized disclosure or alteration breaches regulations such as HIPAA and GDPR and endangers patient safety (Quazi et al., 2024).

Immutability in blockchains is ensured for integrity, while lightweight cryptography primitives such as Ascon or elliptic curve cryptography (ECC) may ensure confidentiality in constrained environments for IoMT (Dobraunig et al., 2021; Robert et al., 2024)

ii. Low Overhead Computational Operations: IoMT devices generally have CPU capacity, memory, and energy constraints. Thus, heavyweight operations like RSA or Proof-of-Work (PoW) are unsuitable in this scenario. Hence, lightweight cryptographic mechanisms (such as Ascon, ChaCha-based schemes) and lightweight consensus protocols (such as Proof-of-Authentication) must be considered for minimizing computational overhead without compromising on security (Cheikhrouhou et al., 2023).

iii. System Scalability: With the fast surge in the number of IoMT devices, high-volume transaction and node accommodating capacity become a key consideration for the blockchain framework. Throughput and latency bottlenecks plague the traditional blockchain network, thereby limiting its use. A lightweight consensus layer coupled with distributed storage increases scalability by reducing on-chain storage overhead and increasing transaction throughput (Khan et al., 2025).

iv. Interoperability: IoMT ecosystems comprise diverse devices, sensors, and platforms that may span multiples vendors and protocols. A lack of interoperability inhibits efficient data sharing and integration with healthcare systems. Blockchain-based interoperability layers, together with standardized lightweight encryption and secure APIs, are the primary enablers of secret communication (Reegu et al., 2023).

v. Secure Consensus: Traditional consensus mechanisms, be it PoW or PoS, either consume considerable resources or cannot be deployed in time-bound healthcare settings. It demands a mechanism with very lightweight consensus that can secure decentralized trust, to not accumulating energy or latency overheads. Recent ones do, by way of example, using the BFT-based protocol or delegated lightweight consensus, show promise in constrained IoMT environments (Cheikhrouhou et al., 2023).

Therefore, this system analysis underlines that for a lightweight methodological basis of blockchain IoMT data management to be effective, it should guarantee data confidentiality and integrity, survive under resource-constrained settings, scale with demand, afford interoperability among heterogeneous devices, and embed the consensus into a lightweight security suit. These requirements then set the basis for stated design decisions outlined in the subsequent sub section.

MATERIALS AND METHODS

The research implemented a design-based methodology to create a lightweight blockchain system which protects Internet of Medical Things (IoMT) data through secure data management. The method evaluated system performance through architectural design. The requirement analysis identified essential system requirements which included security needs and scalability requirements and interoperability standards and performance efficiency expectations. The requirements led to the creation of a multi-layer architectural system which combined lightweight encryption for data security with blockchain technology for permanent data storage and various systems to enable cross platform communication.

Mathematical modeling is used to establish essential system parameters which include throughput and latency and encryption efficiency to create a foundation for performance assessment. The system design used a modular incremental method which permitted separate development and system component integration. It consists of six main components which include the lightweight encryption layer and blockchain layer and interoperability layer which provide different functions for the IoMT ecosystem. The framework was implemented through Python programming language modeling which took place in the Google Colab environment that enables system simulation through its blockchain computational power, also evaluation of the proposed framework performance used two main metrics which included throughput and latency.

System Design

The system design acts as the primary structural layout of the proposed lightweight blockchain-based IoMT framework, showing the integration of the major layers and components. It specifies how encryption, consensus, interoperability, and storage mechanisms are manipulated to provide security, efficiency, and scalability to environments where resources are limited. The design, therefore, becomes very important for the IoMT systems as it introduces means whereby theory can be put into practice while meeting the requirements of health security standards (Oloruntoba et al; Cheikhrouhou et al., 2023).

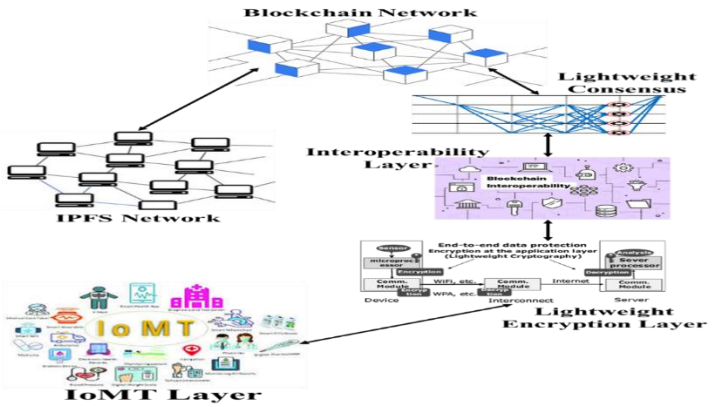

Figure 1: Architectural Framework

Architectural Framework

The architecture is composed of six layers:

i. IoMT Devices Layer (Data Collection): The real-time health data from wearables and sensors including heart rate and blood pressure measurements must be pre-processed through filtering and compression before encryption and transmission.
ii. Lightweight Encryption Layer: The system employs ECC together with AES-128 for affordable data encryption and SHA-256 to maintain data integrity while protecting communications from end to end.
iii. Blockchain Layer (Core Infrastructure): The permissioned blockchain system provides secured storage and smart contracts enable automated access verification while maintaining immutable audit trails to fulfill compliance requirements.
iv. Lightweight Consensus Algorithm: The PoA and DPoS consensus algorithms operate with low energy consumption to provide fast transaction validation while being optimized for IoMT device requirements.
v. Interoperability Layer: The system supports cross-chain data exchange and multiple system compatibility through standard APIs that integrate with electronic health records for multi-platform data sharing.
vi. IPFS Layer (Decentralized Storage): Medical files encrypted for storage reside in IPFS and blockchain maintains file hash pointers to minimize blockchain bloat while enhancing system scalability.

Mathematical formulation for the IoMT Blockchain Framework

This gives a formal mathematical description of major operations and performance parameters of the proposed IoMT Blockchain Framework. It involves data security, lightweight consensus mechanism, blockchain performance, IPFS storage, and interoperability. Optimization of the framework will be based on efficient data security and scalability considerations.

Key Variables and Parameters Definitions

i. D_i: Data generated by the i-Th IoMT device.
ii. $E(D_i, K)$ Encryption function, where D_i is encrypted using key$K$.
iii. $H(D)$: Cryptographic hash of data$D$.
iv. T: Transaction submitted to the blockchain.
v. P: Probability of successful transaction validation in the consensus algorithm.
vi. N_b: Total number of blockchain nodes.
vii. N_v: Number of validator nodes.
viii. T_b: Block creation time.
ix. R_t: Average response time for transaction processing.
x. C_t: Computational cost of processing a transaction.
xi. S_{IPFS}: Storage size required for encrypted data on IPFS.
xii. L_t: Latency for retrieving data from IPFS.
xiii. D_{inter}: Interoperability delay for cross-chain communication.
xiv. B: Network bandwidth for data transmission.
xv. M_i: Size of the message exchanged in the interoperability layer.
xvi. $L_{threshold}$: Maximum allowable end-to-end latency3.4 The Proposed Algorithm

Step 1: Initialization

i. Configure IoMT devices for data collection and encryption.
ii. Connect to blockchain and IPFS networks.
iii. Define minimum thresholds for system parameters:

Step 2: Data Collection and Encryption

For each IoMT device i

$C_e = O(||D_i|| . \log k)$,

Where $||D_i||$ is the size of the data?

1. Encrypt the data using key K:

$E(D_i, K)$

2. Generate a hash for data integrity verification:

$H(D_i) = Hash\ (E(D_i, K))$

3. Encrypt the data using key K:

$E(D_i, K)$

4. Generate a hash for data integrity verification:

$H(D_i) = Hash\ (E(D_i, K))$

Step 3: Data Storage in IPFS

i. Store $E(D_i, K)$ in IPFS and obtain$IPFS_Hash$.
ii. Compute the total storage size required:

$S_{IPFS} = ||\ E(D_i, K)|| + ||H(D_i)||$

iii. Verify that $S_{IPFS} \leq S_{max}$SIPFS:

If false, raise a storage capacity error.

Step 4: Blockchain Integration

i. Create a transaction T containing:

Device ID, Timestamp,$IPFS_{Hash} and\ H(D_i)$.

ii. Sign the transaction T using the device's private key:

$Signed\_T\ = Sign(T, Private\_Key)$

iii. Submit $Signed\_T$ to the blockchain network.
iv. Measure transaction validation probability:

$P = \frac{1}{N_v}$

v. Validate that $P \geq P_{min}$:

If false, raise a consensus error.

Step 5: Consensus Mechanism

i. Implement lightweight consensus (e.g., Proof of Authority):
   a. Compute the time complexity of consensus:
   $T_c = O(\log N_b)$
   Where N_b is the total number of nodes?
   b. Calculate the response time:
   $R_t = T_c\ (\frac{T_b}{N_v})$
   Where T_b is the block creation time?
ii. Add $Signed\_T$ to the blockchain upon successful validation.

Step 6: Performance Metrics Calculation

i. Compute blockchain throughput (TPS):

$TPS = (\frac{N_t}{T_b})$

Where N_t is the number of transactions in a block?

ii. Compute data retrieval latency from IPFS:

$L_t = (\frac{S_{IPFS}}{\mathrm{B}})$

Where B is the network bandwidth?

Step 7: Data Retrieval and Access Control

i. For authorized users:
   a. Query the blockchain for$IPFS_Hash\ \ and\ H\ (D_i)$.
   b. Retrieve encrypted data from IPFS using PFS_Hash.
   c. Verify data integrity by comparing:

$S_{IPFS} = Hash\left(E(D_i, K)\right) with\ (D_i)$

If they do not match, raise an integrity error.

d. Decrypt the data to obtain D_i:

$D_i = Decrypt\ (E(D_i, K), K)$

Step 8: Interoperability Operations

For cross-chain or external interactions:

i. Compute the interoperability delay:

$D_{inter} = \sum (\frac{M_i}{B_i})$

Summing over all chains.

ii. Ensure compatibility with external systems for data exchange.

Step 9: End-to-End Latency Evaluation

i. Compute total latency:

$L_{total} = L_d + L_c + L_t + D_{inter}$

where:

L_d: Latency for data collection. $L_c = R_t$: Consensus latency. L_t: Latency for IPFS storage/retrieval. D_{inter}: Interoperability delay.

ii. Validate that $L_{total} \leq L_{total}$:

If false, raise a latency error.

Step 10: Output Results

i. Return $T, IPFS\_Hash, L_{total}\ and\ TPS$.

ii. Log performance metrics for optimization.

End

Implementation and Performance Evaluation

This section focuses on the functionality evaluation and performance evaluation of the proposed framework, using latency and throughput metrics.

Implementation Setup

The proposed lightweight blockchain-based IoMT framework was implemented through Python programming which was executed within the Google Colab environment. This platform is used because it enables simulation of blockchain operations through its ability to scale and computational performance.

The implementation integrates key components of the framework, including:

i. Lightweight encryption mechanism

ii. Blockchain layer for secure data storage

iii. Interoperability layer for cross-system communication

Simulation experiments were conducted using different transaction volumes between 50 and 5000 transactions to assess how the system performed with different workload levels.

Performance Metrics

The proposed framework performance evaluation used essential performance metrics as the evaluation method.

Throughput (Transactions per Second, TPS): Measures the number of transactions processed per second.

i. Latency (ms): Represents the time required to validate and commit transactions.

ii. Processing Time (seconds): Indicates the time taken to execute transactions.

iii. Resource Efficiency: Includes computation time, memory usage, processor utilization, and battery consumption for cryptographic operations.

The selected metrics evaluate the framework efficiency and scalability and its performance in resource-constrained IoMT environments.

RESULTS AND DISCUSSION

Result and Analysis

Performance of the lightweight blockchain-based Internet of Medical Things framework was evaluated testing its throughput and latency metrics across various transaction volumes which spanned from 50 transactions to 5000 transactions. The results are summarized in Table 4.1 and illustrated in Figures 4.1, 4.2 and 4.3.

Throughput Performance

The throughput results show that the framework maintains high transaction processing rates during all testing conditions. The system handles more than 5 million transactions per second with peak throughput of 5.81 million transactions per second when handling 50 to 500 transactions. The system maintains high throughput which extends from 3.8 million transactions per second to 5.5 million transactions per second when transaction volumes increase from 500 to 5000, but performance decreases at higher workloads due to computational overhead.

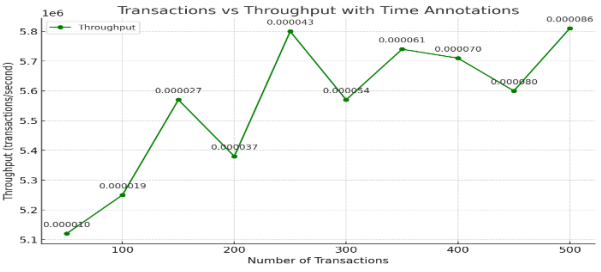

Figure 1: Throughput Analysis of 50-500 Transactions

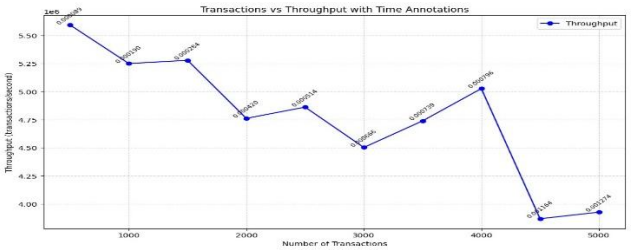

Figure 2: Throughput Analysis of (500-5000) Transactions

Latency Performance

The latency analysis demonstrates that the system delivers response times which remain extremely low throughout all transaction volume levels. The system shows latency between 0.01 millisecond and 0.10 millisecond for 50 to 500 transactions which establishes its capacity to process transactions in near real-time. The system shows latency of about 2.31 milliseconds when handling 5000 transactions because of the need to process larger workloads. The framework maintains acceptable latency levels for IoMT applications which need to operate with strict time requirements.

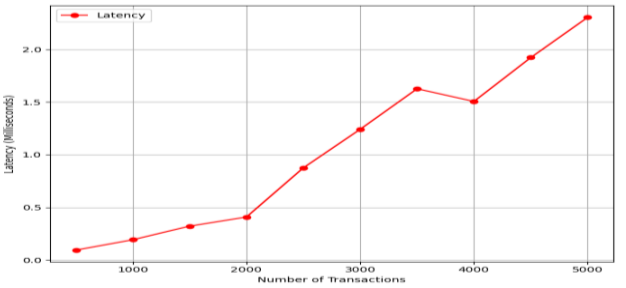

Figure 3: Latency Analysis (500-5000)

Security Analysis

This section assesses how effectively the proposed lightweight cryptographic system protects IoMT data through its evaluation of computation time memory usage processor consumption and battery consumption. The proposed framework demonstrates its efficiency through computation time of 0.012 seconds and memory requirement of 0.95 kilobytes and processor use of 0.1 percent and energy demand of 1.10×10^{-7} watts. The framework shows improved efficiency when used with IoMT devices because it outperforms traditional security methods which include AES RSA and AESRSA. The results demonstrate that the proposed method establishes both secure data protection and lightweight security for IoMT environments.

Table 4: Security Evaluation of Proposed Framework

Data Size	Cryptography	Computation Time (S)	Computing Memory (KB)	Processor Consumption (%)	Battery Consumption (W)
500 kb	AES	0.025	2.37	0	1.56E-05
500 kb	RSA	5.487	2.08	0.7	0.004141
500 kb	AESRSA	5.502	4.17	0.7	0.005091
500 kb	Proposed Framework	0.012	0.95	0.1	1.10E-07

Discussion

The proposed lightweight blockchain-based framework shows strong potential for IoMT data management because it achieves three essential requirements which real-time healthcare applications need. The combination of lightweight cryptography with data protection methods enables secure data transmission through encrypted channels while requiring minimal processing power which matches the needs of resource constraint devices also custom consensus mechanism provides two benefits by enabling secure transaction validation and efficient transaction processing while using minimal system resources. The framework evaluation process has relied on simulation tests which create challenges for field testing. The system design verifies that a secure blockchain framework which uses low resources can provide scalable security for IoMT systems.

CONCLUSION

This study presented a lightweight blockchain-based framework for secure and efficient data management in Internet of Medical Things (IoMT) environments. This framework uses lightweight encryption, blockchain technology, and interoperability to address the issues of security, scalability, and resource constraints in digital healthcare. The results from implementing and evaluating the proposed framework showed that it performs well at varying transaction volume levels (i.e., both high and low) and achieves high throughput and low latency, thus enabling real-time processing of data and secure communication between devices within the IoMT application. While there were some minor differences in performance (e.g., lower throughput and higher latencies) at higher transaction volumes, acceptable levels of performance were maintained throughout the tests demonstrating that this framework has good scalability. Future work may focus on further optimization techniques, such as enhanced consensus mechanisms and parallel processing, to improve performance under extreme workloads also on real life implementation in healthcare facilities. In summary, this study has provided the foundation for a very effective solution to securely manage IoMT data, thus supporting further research and development of lightweight blockchain implementations within the healthcare sector.

REFERENCES

Aboshosha, B.W., Zayed, M.M., khalifa, H.S. (2025). Enhancing Internet of Things security in healthcare using a blockchain-driven lightweight hashing system. *Beni-Suef Univ J Basic Appl Sci* 14, 56 (2025). https://doi.org/10.1186/s43088-025-00644-8

Alabdulatif, A. (2025). Blockchain-Based Privacy-Preserving Authentication and Access Control Model for E-Health Users. Information 2025, 16, 219. https://doi.org/10.3390/info16030219

Ba, A.F., Yingchi, M., Muhammad, A.U. (2025). Blockchain federated learning with sparsity for IoMT devices. *Cluster Comput* 28, 47. https://doi.org/10.1007/s10586-024-04810-y

Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., & Moosavi, S. R. (2023). A lightweight blockchain and fog-enabled secure remote patient monitoring

system. *Internet of Things*, 22, 100691. https://doi.org/10.1016/j.iot.2023.100691

Dobraunig, C., Eichlseder, M., Mendel, F. (2021). Ascon v1.2: Lightweight Authenticated Encryption and Hashing. *J Cryptol* 34, 33 . https://doi.org/10.1007/s00145-021-09398-9

Farshadinia, H., Barati, A., & Barati, H. (2025). Designing a layered framework to secure data via improved multi-stage lightweight cryptography in IoT–cloud systems. *arXiv preprint arXiv:2509.01717*. https://arxiv.org/abs/2509.01717

Fugkeaw, S., Wirz, L., & Hak, L. (2023). Secure and lightweight blockchain-enabled access control for fog-assisted IoT cloud based electronic medical records sharing. *IEEE access*, *11*, 62998-63012.

Ghadi, Y.Y., Mazhar, T., Shahzad, T. *et al.* The role of blockchain to secure internet of medical things. *Sci Rep* 14, 18422 (2024). https://doi.org/10.1038/s41598-024-68529-x

Jayabalan, J & Jeyanthi, N. (2022). Scalable blockchain model using offchain IPFS storage for healthcare data security and privacy, J. Parallel Distrib. Comput., vol. 164, pp. 152–167, Jun. 2022, https://doi.org/10.1016/j.jpdc.2022.03.009

Khan, M., et al. (2025). Lightweight Privacy Preservation Authentication Protocol for IoMT using ECC. SAGE Journal.

Khatter, K & DevanjaliRelan. (2022). Non-functional requirements for blockchain enabled medical supply chain. *Int J Syst Assur Eng Manag* 13, 1219–1231 (2022). https://doi.org/10.1007/s13198-021-01418-y

Okoli, F. U., Oludiji, S. M., Ofoegbunam, E. I., Oyesiji, A. O., & Akindiya, O. M. (2024). Blockchain Technology for Land Registration In Nigeria: A Review of Opportunities and Challenges. *Fudma Journal of Sciences*, 8(6), 252-257. https://doi.org/10.33003/fjs-2024-0806-2919

Oloruntoba, L. J., Obiniyi, A. (2025). Trends in the Application of Blockchain Technology to the Internet of Medical Things (IoMT). Direct Research Journal of Engineering and InformationTechnology,13(3),29-34. https://journals.directresearchpublisher.org/index.php/drjeit/article/view/469

Othman, S.B., Getahun, M.(2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. *Sci Rep* 15, 12358 (2025). https://doi.org/10.1038/s41598-025-95531-8

Papaioannou, M., Karageorgou, M., Mantas, G. (2022). A Survey on Security Threats and Countermeasures in Internet of Medical Things (IoMT). Trans Emerging Tel Tech. 2022;33:e4049. https://doi.org/10.1002/ett.4049

Quazi, F., Khanna, A., nalluri, S., & Gorrepati, N. (2024). Data Security & Privacy in Healthcare. International Journal of Global Innovations and Solutions (IJGIS). https://doi.org/10.21428/e90189c8.4e2c586a

Rasheed, A,M., & Kumar, R,M,S. (2025) Efficient lightweight cryptographic solutions for enhancing data security in healthcare systems based on IoT. Front. Comput. Sci. 7:1522184. doi: https://doi.org/10.3389/fcomp.2025.1522184

Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G., & Dziyauddin, R. A. (2023). Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System. *Sustainability*, *15*(8), 6337.

Robert, W., Denis, A., Thomas, A., Samuel, A., Kabiito, S. P., Morish, Z., & Ali, G. (2024). A comprehensive review on cryptographic techniques for securing Internet of Medical Things: A state-of-the-art, applications, security attacks, mitigation measures, and future research direction. *Mesopotamian Journal of Artificial Intelligence in Healthcare*, *2024*, 135–169. https://doi.org/10.58496/MJAIH/2024/016

Samal, K., Sunanda, S,K, Jena, D., Patnaik, S. (2025) A lightweight privacy preservation authentication protocol for IoMT using ECC based blind signature. *International Journal of Engineering Business Management*. 2025;17. doi:10.1177/18479790251318538

Singh, S., Sharma, P.K., Moon, S.Y. (2024). Advanced lightweight encryption algorithms for IoT devices: survey, challenges and solutions. *J Ambient Intell Human Comput* 15, 1625–1642 (2024). https://doi.org/10.1007/s12652-017-0494-4

Stefanescu, D., Montalvillo, L., Galán-García, P., Unzilla, J., & Urbieta, A. (2022). A Systematic Literature Review of Lightweight Blockchain for IoT," in IEEE Access, vol. 10, pp. 123138-123159, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3224222.

Xie, H., Zheng, J., He, T. *et al.* A blockchain-based ubiquitous entity authentication and management scheme with homomorphic encryption for FANET. *Peer-to-Peer Netw. Appl.* **17**, 569–584 (2024). https://doi.org/10.1007/s12083-024-01624-y