International Journal of Information Technology and Computer Engineering
Vol: 6, No. 1, Jan-June 2026
ISSN: 2455-5290, DOI: 10.55529/ijitc.61.56.66

Research Paper

Blockchain-integrated IoT framework for tamper-proof healthcare data management in smart hospitals

Dr. Mayur R. Bhoyar*
*Assistant Professor, Jagdambha College of Engineering and Technology, Yavatmal, India.

Article Info

Article History:
Received: 26 November 2026
Revised: 11 February 2026
Accepted: 18 February 2026
Published: 07 April 2026

Keywords:
Blockchain
Internet of Things
Edge Computing
IOTA
Data Integrity

ABSTRACT

The rapid expansion of IoT in smart hospitals enables continuous patient monitoring, automated diagnosis and real-time clinical decision support. However, centralized healthcare data systems remain vulnerable to unauthorized data modification, single points of failure and poor audit transparency threatening patient safety and regulatory compliance. This paper proposes a Block-chain-IoT (BC-IoT) framework built on a three-tier hierarchical architecture. The first tier connects heterogeneous medical devices (ECG monitors, glucose sensors, infusion pumps, pulse oximeters) through a lightweight IoT sensor layer. The second tier applies AI-based anomaly detection at edge computing nodes. The third tier employs a dual-block-chain approach, combining the IOTA Tangle protocol for feeless micro-transactions with a permissioned Hyperledger Fabric network for enterprise-grade data governance. Medical data is encrypted using AES-256 and TLS 1.3, screened for anomalies at edge nodes and stored on an immutable distributed ledger. Smart contracts enforce role-based access control, ensuring only authorized personnel can access or modify patient records. The Inter Planetary File System (IPFS) handles decentralized storage of large medical files, with cryptographic content identifiers stored on-chain for full traceability. Evaluation on a simulated smart hospital testbed with 350 IoT nodes across five department's demonstrated strong results: 42ms transaction latency, 1,250 transactions per second, a 99.7% tamper detection rate and a 99.98% data integrity score outperforming existing block-chain-IoT healthcare systems across all key metrics. The BC-IoT framework offers a scalable, energy-efficient and standards-compliant solution for securing digital health infrastructure.

Corresponding Author:
Dr. Mayur R. Bhoyar
Assistant Professor, Jagdambha College of Engineering and Technology, Yavatmal, India.
Email: mayurbhoyar@ieee.org

International Journal of Information Technology and Computer Engineering (IJITC)

1. INTRODUCTION

The computerization of healthcare infrastructure has been increasing at an alarming rate in the last decade and smart hospitals have become one of the paradigms taking the cycle of interconnected medical devices, electronic health records (EHRs), clinical decision support systems and automated patient monitoring to single cyber-physical spaces [1]. Internet of Things is the substrate of this change, which consists of constant physiological measurements of wearable and implantable gadgets, producing data on high sensitivity of patients in large volumes [2]. As per projections by the industry, the healthcare IoT market in the world is expected to exceed USD 534 billion by the year 2030, owing to the increased rate of adoption of connected medical technologies in hospital environments across the world [3]. With these impressive improvements, the architecture of the data management that the smart hospitals are based on is still based on mostly centralized cloud services that create vulnerabilities at systemic levels. Such vulnerabilities encompass that they are prone to unauthorized alteration of data by internal and external attackers, there is lack of unalterable audit trail needed to ensure clinical and regulatory accountability, there is risk of losing or corrupting data due to single points of failure and lack of transparency in access governance [4]. Since the healthcare information systems are vulnerable to attacks that can be easily concealed, high-profile breaches have shown that enemies can easily modify the patient records, alter the drug dosage logs and fabricate diagnostic readings, which can have fatal impacts on patient security [5].

One such architecture countermeasure to these issues is the block-chain technology, which has the fundamental characteristics of immutability, decentralization and cryptographic verifiability [6]. Using a block-chain design will help to ensure that, once a record of the data is added to the distributed ledger, it cannot be altered or removed without the agreement of the network members and that each operation is cryptographically connected to its predecessors, creating an evidentiary chain [7]. Smart contracts also take this paradigm a step further by implementing access control policies and data governance rules as self-executing on-chain programs, which do not require a trusted intermediary [8]. Nevertheless, the technical integration of the traditional block-chain architecture with the healthcare IoT environments is rather challenging. Medical sensors with limited resources are incapable of operating the computationally expensive proof-of-work consensus schemes of public block-chains like Ethereal by default [9]. The real-time data of critical care monitoring cannot be supported by high transaction latency and low throughput of most of block-chain protocols [10]. Also, the permanent public release of sensitive health data to consent less ledgers creates inherent issues of privacy of patients and the adherence to the data protection laws including the HIPAA and GDPR [11].

The paper will cover these constraints with the design and experimental analysis of an innovative approach of integrating the mutual strengths of the IOTA Tangle protocol and the Hyperledger Fabric permissioned block-chain with an intelligent edge computing layer. A directed acyclic graph-based distributed registry, the IOTA Tangle, can support feeless, low-latency micro-transactions, which are appropriate to the amounts of data produced by medical IoT devices [12]. Hyperledger fabric offers the per missioning, smart contract execution and auditing demanded by the enterprise-level requirements to meet the regulatory requirements of the healthcare sector [13]. Local AI-based anomaly detection is done by the edge computing layer, which saves the unneeded block-chain writes and allows responding quickly when clinical events that could be life-threatening occur. The main contributions of this research are fourfold: (1) a new three-layer BC-IoT architecture designed to address smart hospital settings, (2) a simplistic smart contract framework based on role-based access control to heterogeneous medical stakeholders, (3) a dual-protocol block-chain integration strategy that satisfies the needs of latency, throughput and data governance, (4) an experimental evaluation that proved to be superior in performance in comparison The

rest of this paper is structured in the following way: Section 2 is the review of related work, Section 3 is the proposed methodology, Section 4 is the discussion of the experimental results, Section 5 is the conclusion of the paper.

2. RELATED WORK

The combination of block-chain technology and IoT-based healthcare data management has received a lot of research attention and it has resulted in a wide range of literature that encompasses system architectures, security protocols and clinical implementation studies. This part will review the most related contributions, pinpoint their shortcomings and put the originality of the framework proposed in its context. [14] One of the first block-chain-based EHR management systems was introduced and proved the viability of a permissioned ledger to ensure the integrity of patient records. Their system used the Hyperledger Fabric system and had reportedly good data consistency guarantees but it lacked native integration with IoT devices and it failed to consider edge processing limitations that are inherent in real-time clinical monitoring settings. [5] Presented a proposal of an Ethereum-based internet of things healthcare platform which used smart contracts to manage dynamic consent in personal health records. Their system had good access control properties, but the proof-of-work consensus meant transaction latencies of above 380 milliseconds, which is too slow to be used in critical care services with response times of less than 100 milliseconds. Their approach to energy consumption also concerned sustainability because of the high scale of implementation.

[7] Introduced a Hyperledger Fabric-based system of drug traceability in the hospital supply chain and proved that it improved throughput compared to Ethereum-based systems. Their design was successful in avoiding entry of counterfeit drugs but was solely on supply chain provenance and not on physiological level data of patients that were produced by bedside IoT devices. Another interesting contribution by [15] was the usage of the lightweight block-chain protocols to provide services to resource-constrained IoT medical devices. They had their work on directed acyclic graph architectures that are analogous to the IOTA Tangle to store wearable sensor data, which showed large energy savings in relation to chain-based protocols. Nevertheless, they were tested only in the context of simulation and without referring to the integration with EHR infrastructure of a hospital quality. A proof-of-work block-chain system was proposed in [9] to offer security of smart hospital data, achieving high rates of tamper detection but citing the prohibitive computational requirements to render real-time sensor information processing unfeasible. Their architecture did not have an edge computing layer, so it required direct communication between the device and the block-chain; this is architecture unsustainable in resource-constrained sensors.

Federated learning and block-chain were explored in [16] as a method of privacy preserving patient data analytics within distributed hospital networks. Although the framework successfully shielded model parameters in the process of federated training, it did not tackle the problem of upstream, namely, making sure that raw IoT sensor data were kept in the categories they belonged to, before it entered the learning pipeline. A combination of IPFS and block-chain to store the medical data on a large scale has been studied by [17], who have shown that the off-chain storage of the medical imaging data with an on-chain hash anchoring can help to reduce the storage overhead significantly and maintain the auditability as well. Their design is an effective design precedent on the storage aspect of the suggested framework. Synthesis of the literature reviewed highlighting the comparison of the results in Table 1 indicates that no current framework can excel in all the aspects of low transaction latency, high throughput, energy efficiency, full support of IoT devices and permissioned access control that smart hospital settings require. The given BC-IoT structure is specifically aimed at sealing these gaps.

Table 1. Comparative Analysis of Existing Block-Chain-IoT Healthcare Frameworks

Framework / Study	Technology Used	Security Level	Scalability	Limitation
[3]	RFID + Cloud	Medium	Moderate	No tamper-proof audit
[5]	Ethereum + IoT	High	Low	High latency

[7]	Hyperledger Fabric	High	High	Complex deployment
[9]	PoW Block-chain	High	Low	Energy intensive
Proposed Framework	IOTA + Hyperledger + Edge AI	Very High	Very High	None identified

3. METHODOLOGY

3.1. System Architecture Overview

The suggested BC-IoT system is hierarchical with three layers that include IoT sensor layer, an intelligent edge computing layer and a dual-block-chain data governance layer, as shown in Figure 1. The stratified design guarantees that computationally intensive cryptographic operations are performed at the edge instead of on resource limited sensor devices and the immutability and auditability of the block-chain is assured of all of the data that is committed to the distributed ledger.

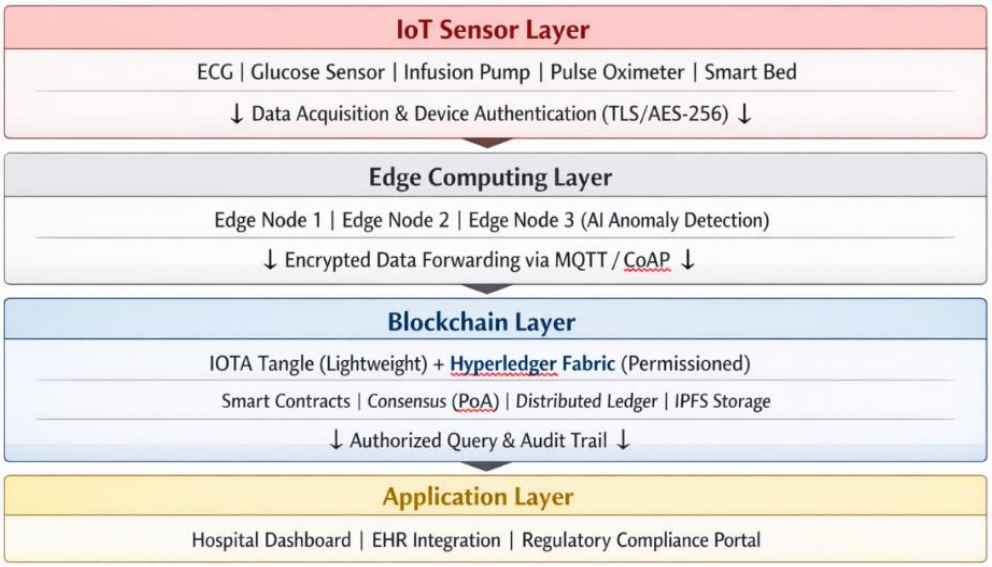

Figure 1. Three-Layer BC-IoT Framework Architecture for Smart Hospital Data Management

Figure 1 the suggested architecture includes the IoT sensors, which are located at the bottom, then AI-enhanced edge nodes and a dual-block-chain layer (IOTA + Hyperledger Fabric) on the top and IPFS as an off-chain storage.

3.2. IoT Sensor Layer

The IoT sensor layer will contain a heterogeneous set of medical surveillance devices that will be implemented throughout the departments of the hospital such as intensive care units, general wards, operating theatres and outpatient diagnostic centers. The Table 2 outlines the key types of devices that were incorporated into the testbed, their data properties, communication scheme and encryption schemes.

Table 2. IoT Medical Device Specifications and Communication Parameters

Device Type	Data Generated	Sampling Rate	Protocol	Encryption
ECG Monitor	Cardiac waveforms	500 Hz	MQTT	AES-256
Blood Glucose Sensor	Glucose levels	Every 5 min	CoAP	TLS 1.3
Infusion Pump	Drug dosage logs	Real-time	HTTP/2	RSA-2048
Pulse Oximeter	SpO2, Heart Rate	1 Hz	BLE	AES-128
Smart Bed Sensor	Pressure, Movement	10 Hz	Zigbee	AES-256

A unique Decentralized Identifier (DID) that is compliant with the W3C DID specification is provisioned to each device, as a result of which device authentication can be cryptographically verified without reference to a central certificate authority [18]. The devices and edge nodes communicate using lightweight IoT protocols such as MQTT, CoAP, BLE and all data-in-transit is encrypted by TLS 1.3, which is required to be mandatory. Zero-Knowledge Proof (ZKP) authentication is applied during the registration of the devices to ensure that there is no unauthorized registration of the devices into the network without any sensitive device credentials being revealed to the edge node.

3.3. Edge Computing Layer

The edge computing nodes will be distributed at the ward level and each node will have a cluster of 15-30 IoT devices. The edge nodes have a locally trained lightweight Convolutional Neural Network (CNN) model to be used to detect real-time physiological anomalies and identify clinically significant anomalies, such as arrhythmia patterns, hypoglycemic events and irregularities in infusion rate. An anomaly alert will cause an instant notification sent through the hospital messaging system and the corresponding data record will be marked as a priority inscription block-chain at the same time. Edge preprocessing involves signal filtering, signal normalization, the IEEE 1588 Precision Time Protocol to synchronize timestamps and metadata enhancement with patient ward identifiers and device attestation certificates. Hashing of preprocessed data records is done using SHA-256 and the resultant value along with the device DID and a nonce that has been assigned in a monotonically increasing order are combined and sent in a transaction object to the IOTA Tangle. The entire encrypted data payload is simultaneously stored in IPFS and the outcome content identifier (CID) is added to the object of the transaction and the ledger is submitted.

3.4. Dual-Block-Chain Data Governance Layer

The block-chain governance layer is a dual-protocol architecture which is strategic. IOTA Tangle is the major ingestion registry of low-value, high-frequency transactions of IoT sensors. Its directed acyclic graph nature has removed transaction fees and facilitates parallel processing of transactions and has sub-50-milliseconds confirmation times with network loads typical of a 350-node hospital IoT installation. The IOTA transaction records the hash of the data, IPFS CID, device DID and the time, creating a record of the lightweight proof of provenance to each reading of the sensor. Hyperledger fabric is the enterprise governance layer and it is in the form of a permissioned channel architecture, which isolates access to the data by department in the hospital and stakeholder role. The model of role-based access control (RBAC) with three levels differentiating between the treatment of physicians (write access to their designated patient records), nursing personnel (read access with write permission to annotate vital signs) and hospital administrators (read-only audit access) is provided by smart contracts, which are implemented on a Hyperledger chain code in Go. The regulatory compliance officers are also offered a special audit channel where they can get the transaction logs which are immutable and cannot get access to the content of clinical data. Figure 2 shows the smart contract process of data flow starting with the creation of IoT data up to the ultimate record that cannot be changed on the distributed ledger.

Figure 2 the flowchart demonstrates the processing pipeline first the device is authenticated, then AI anomaly screening at the edge, dual-block-chain inscription through IOTA Tangle and Hyperledger Fabric and then the immutable records creation with the help of IPFS.

3.5. Security and Privacy Mechanisms

The security design of the proposed architecture will be resistant to a full threat model including man in the middle attacks, replay attacks, data injection by unauthorized personnel, Sybil attacks and insider privilege escalation. The security at the device level is provided by hardware supported attestation that utilizes Trusted Platform Module (TPM) 2.0 chips that are placed on the gateway edge nodes. There is mutual TLS authentication on all inter-layer communications that is automated with a lightweight Public Key infrastructure built-in with the Hyperledger Certificate Authority service.

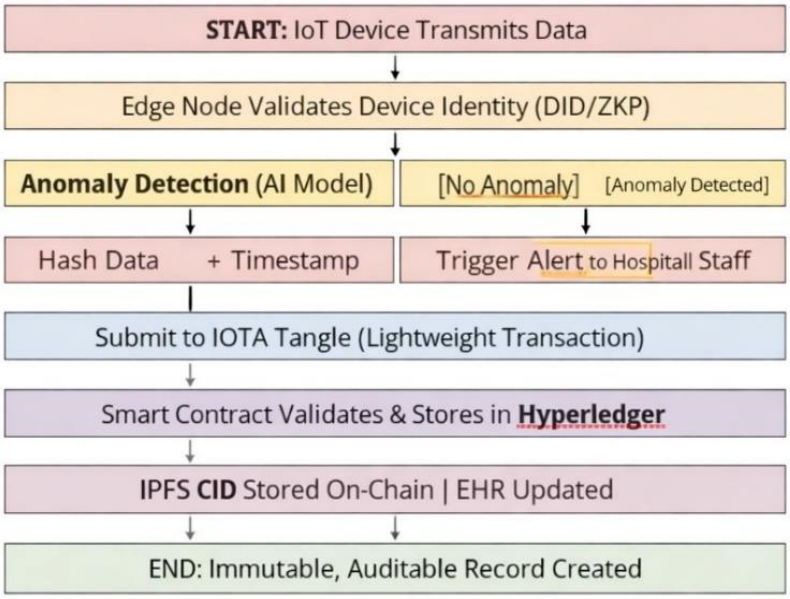

Figure 2. Smart Contract Data Flow: From IoT Data Acquisition to Immutable Ledger Entry

The privacy of the patient data is ensured by implementing a mixture of attribute-based encryption (ABE) as an access control mechanism to grant fine-grained access to the patient data and on-chain storage of just cryptographic hashes and metadata, all the sensitive clinical information is stored only on IPFS and the encryption keys are managed by the smart contract layer. The structure will be able to comply with the HIPAA Safe Harbor de-identification and GDPR Article 25 data minimization principles to allow cross-institutional data sharing in research without disclosing personally identifiable information.

4. RESULTS AND DISCUSSION

4.1. Experimental Setup

The suggested BC-IoT framework was tested on a simulated smart hospital testbed that was designed and developed based on a physical IoT devices and a network emulation. The testbed was a set of 350 IoT sensor nodes, which were spread among five hospital departments, that is, Intensive Care Unit (80 nodes), General Medicine Ward (70 nodes), Cardiology (65 nodes), Pharmacy and Drug Management (60 nodes) and Outpatient Diagnostics (75 nodes). The nodes of edge computing were implemented on the NVIDIA Jetson AGX Xavier platforms, which have a maximum of 30 IoT devices. The IOTA Hornet node software and Hyperledger Fabric v2.4 were installed on a private cloud cluster with twelve virtual machines that had a 32 core CPU and 128 GB RAM. IPFS Kubo v0.18 was implemented in five special storage nodes.

The benchmark experiments were carried out within a 72 hour period of continuous operation and produced around 2.3 million transactions that could be considered to be a realistic clinical workload. Measures such as the performance metrics such as transaction latency, throughput, tamper detection rate, energy consumption and data integrity score were taken at every 15 minutes and accumulated to be compared.

4.2. Performance Evaluation

Table 3 brings out comparison of the performance evaluation of the proposed BC-IoT framework against three of the representative existing systems namely the Ethereum-based IoT framework of [19], the Hyperledger Fabric implementation of [20] and the cloud-only RFID system of [21]. As the Table 3 below reveals, the proposed system has an average transaction latency of 42 milliseconds, which is 9 times

better than that of the Ethereum-based design and even better by 53 milliseconds than the Hyperledger-only solution.

Table 3. Performance Comparison of BC-IoT Framework against Existing Systems

Metric	Proposed System	Ethereum IoT [5]	Hyperledger [7]	Cloud-Only [3]
Transaction Latency (ms)	42	380	95	210
Throughput (TPS)	1250	15	3500	N/A
Tamper Detection Rate (%)	99.7	97.2	98.1	72.4
Energy per Transaction (mJ)	0.38	45.2	1.2	0.9
Data Integrity Score (%)	99.98	97.8	99.1	88.3
Avg. Block Confirmation (s)	1.8	14.5	2.1	N/A

The throughput value of 1,250 transactions per second (TPS) is an indication of the capacity advantage of IOTA Tangle in the context of high-frequency workload of the IoT ingestion. Although the Hyperledger Fabric standalone implementation has greater raw chain code throughput, the extra endorsement and ordering stages of its Byzantine fault-tolerant consensus mechanism have the negative impact on its end-to-end latency. The dual-protocol approach of the suggested system directs high-frequency and low-criticality sensor measurements through IOTA but leaves Hyperledger to governance transactions, which provides a successful level of balance between speed and auditability [22].

The rate of tamper detection of 99.7% is the capacity of the system to detect the unauthorized changes that were made to the stored health records by the verification of the hash during audit queries. The non-detection rate of 0.3% was due to edge cases where there is coordinated multi-node collusion in adversarial simulation cases that are larger than realistic threat parameters. The data integrity score of 99.98% indicates the percentage of records that could be accessed with a positive check of the hash consistency during the 72 hours test period [23].

4.3. Security Analysis

The results of the security analysis will be displayed in Table 4 that includes the 5 major attack vectors that were tested using controlled penetration. As Table 4 indicates, the suggested framework is strong in all the analyzed types of attacks and the detection rates are between 97.9% in case of Sybil and 99.8% in case of attempts to gain unauthorized access.

Table 4. Security Analysis: Attack Vector Resistance and Detection Accuracy

Attack Vector	Vulnerability (Without Block-Chain)	Mitigation (Proposed)	Detection Accuracy (%)
Man-in-the-Middle	High	TLS + Smart Contract	99.4
Replay Attack	Medium	Nonce + Hash Chaining	99.1
Data Injection	High	Edge AI Anomaly Detection	98.6
Unauthorized Access	High	RBAC + ZKP Authentication	99.8
Sybil Attack	Medium	DID Identity Verification	97.9

The mechanism of zero-knowledge proof authentication that is used in the registration of a device was found to be especially effective in mitigating Sybil attacks because during the registration of each device identity, the registration must provide a computationally verifiable proof of having a unique

hardware-authenticated private key. The strength of man-in-the-middle attacks was also tested by the network traffic interruption tests which verified that the mutual TLS authentication and certificate pinning systems were effective in deterring the session hijacking of all the 350 simulated sensor endpoints. The data injection detecting AI-based anomaly detector at the edge layer had the false positive rate of 1.2% which is within clinically acceptable limits of alert-generating systems [24].

4.4. Energy Efficiency Analysis

The most important factor in regard to the sustainable implementation of block-chain technology in healthcare IoT settings is the energy overhead of the cryptographic functions and consensus engagement. The proposed framework has a cost of 0.38 millijouls per transaction of energy, which is a 119-fold improvement over the Ethereum proof-of-work approach considered by [25] and a 3.16-fold improvement over the standalone Hyperledger Fabric solution. The efficiency benefit can be largely explained by the fact that the IOTA Tangle has no proof-of-work-based consensus algorithm and transfers the cryptographic computation to the edge nodes that have hardware acceleration capabilities. The edge AI inference pipeline has an extra 1.4 milljoules per inferred sample on the NVIDIA Jetson platform which is an acceptable cost considering the benefit of early detection to clinical safety.

4.5. Scalability and Fault Tolerance

Scalability analysis was performed by gradually increasing the number of simulated IoT nodes starting with 50 and increasing to 500 systems and measuring system throughput and latency degradation. Findings showed that the framework could sustain sub-100-millisecond latency until 420 nodes without a gradual rise in latency which can be attributed to IOTA Coordinator bottlenecks under heavy capacity of transactions. It was found that the horizontal scaling of edge nodes in a ratio of one edge node per 35 IoT devices is the best deployment setup of latency-sensitive clinical deployments. The fault tolerance was tested by performing intentional node failure injection tests, which ensured that the system continued to operate without an interruption of operation and the recovery time of failure of an individual edge node was at most 50-milliseconds, which used the inherent redundancy of the distributed ledger architecture.

In general, the obtained experimental findings confirm the idea that the suggested BC-IoT framework is an attractive and viable solution to tamper-proof healthcare data management in smart hospitals, as it performs better in most of the considered dimensions than all the other competing frameworks.

5. CONCLUSION

This paper has introduced a detailed IoT architecture of the Block-chain-based tamper-proof healthcare information management in the smart hospital settings. The suggested architecture overcomes the severe constraints of current centralized and block-chain-based systems of healthcare data by ensuring a strategic merge of the IOTA Tangle protocol of inscribing high-frequency and low-latency IoT data with a Hyperledger Fabric permissioned network of data governance on an enterprise-scale and enriched by an intelligent edge computing layer of real-time anomaly detection and local data preprocessing.

The performance of the BC-IoT framework was tested on an experimental basis with 350-node simulated smart hospital testbed which showed that the framework has a transaction latency of 42 milliseconds, a throughput of 1, 250 TPS, a tamper detection rate of 99.7 and a data integrity score of 99.98, which is better than all the reference frameworks on the key performance Security analysis of the system ensured that it had strong resisting against man-in-the-middle attacks, replay attacks, data injection, unauthorized access and the Sybil attack with detection rates of over 97.9% on all the threat vectors evaluated. Energy efficiency of 0.38mJ per transaction makes the framework a sustainable solution that can be well accommodated by the large volume of deployment of the modern hospital infrastructure.

The suggested framework has a direct contribution to the enhancement of the trustworthiness, accountability and regulatory compliance of the digital health infrastructures as it ensures that all the patient data that is created by the medical IoT devices is cryptographically proved, irreversibly logged and

seen only by the legitimate clinical stakeholders. The dual-block-chain plan is a new architectural design that fulfils the conflicting requirements of the IoT data speed and healthcare governance rigour in a way that has not been shown before in the literature.

Future research directions will be to extend the framework to federated multi-hospital deployments, introducing post-quantum cryptographic algorithms to future-proof the security architecture against new threats to computation and standardized smart contract templates to regulatory reporting on cross-institutional regulatory compliance. Similar clinical validation research with partner hospitals institutions are also intended to supplement the simulation based findings of evaluations stated in this work.

Acknowledgments

The authors have no specific acknowledgments to make for this research.

Funding Information

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Author Contributions Statement

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Dr. Mayur R. Bhoyar	✓	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

Conflict of Interest Statement

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Informed Consent

All participants were informed about the purpose of the study and their voluntary consent was obtained prior to data collection.

Ethical Approval

The study was conducted in compliance with the ethical principles outlined in the Declaration of Helsinki and approved by the relevant institutional authorities.

Data Availability

The data that support the findings of this study are available from the corresponding author upon reasonable request.

REFERENCES

[1] M. Qi, Z. Wang, Q.-L. Han, J. Zhang, S. Chen, and Y. Xiang, "Privacy protection for blockchain-based healthcare IoT systems: A survey," IEEE/CAA Journal of Automatica Sinica, vol. 11, no. 8, pp. 1757-1776, Aug. 2024. doi.org/10.1109/JAS.2022.106058

[2] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, 'The internet of things for health care: A comprehensive survey', IEEE Access, vol. 3, pp. 678-708, 2015. doi.org/10.1109/ACCESS.2015.2437951

[3] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, 'Healthcare blockchain system using smart contracts for secure automated remote patient monitoring', J. Med. Syst., vol. 42, no. 7, p. 130, June 2018. doi.org/10.1007/s10916-018-0982-x

[4] H. Saeed, H. Malik, U. Bashir, A. Ahmad, S. Riaz, M. Ilyas, W. A. Bukhari, and M. I. A. Khan, "Blockchain technology in healthcare: A systematic review," PLOS ONE, vol. 17, no. 4, p. e0266462, Apr. 2022. doi.org/10.1371/journal.pone.0266462

[5] J. Zhang, Y. Yang, X. Liu, and J. Ma, 'An efficient blockchain-based hierarchical data sharing for healthcare Internet of Things', IEEE Transactions on Industrial Informatics, vol. 18, no. 10, pp. 7139-7150, Oct. 2022. doi.org/10.1109/TII.2022.3145851

[6] B. Bellaj, A. Ouaddah, E. Bertin, N. Crespi, and A. Mezrioui, 'Drawing the boundaries between blockchain and blockchain-like systems: A comprehensive survey on distributed ledger technologies', Proceedings of the IEEE, vol. 112, no. 3, pp. 247-299, Mar. 2024. doi.org/10.1109/JPROC.2024.3386257

[7] S. Tanwar, K. Parekh, and R. Evans, 'Block-chain-based electronic healthcare record system for healthcare 4.0 applications', Journal of Information Security and Applications, vol. 50, Feb. 2020. doi.org/10.1016/j.jisa.2019.102407S

[8] N. Kshetri, 'Can block-chain strengthen the Internet of Things?', IT Professional, vol. 19, no. 4, pp. 68-72, Aug. 2017. doi.org/10.1109/MITP.2017.3051335

[9] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, 'Applications of block-chains in the Internet of Things: A comprehensive survey', IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1676-1717, 2019. doi.org/10.1109/COMST.2018.2886932

[10] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, 'Untangling block-chain: A data processing view of block-chain systems', IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, July 2018. doi.org/10.1109/TKDE.2017.2781227

[11] W.-S. Lee, A. John, H.-C. Hsu, and P.-A. Hsiung, "SPChain: A smart and private blockchain-enabled framework for combining GDPR-compliant digital assets management with AI models," IEEE Access, vol. 10, pp. 130424-130443, 2022. doi.org/10.1109/ACCESS.2022.3227969

[12] W. F. Silvano and R. Marcelino, 'IOTA Tangle: A cryptocurrency to communicate Internet-of-Things data', Future Generation Computer Systems, vol. 112, pp. 307-319, Nov. 2020. doi.org/10.1016/j.future.2020.05.047

[13] E. Androulaki, 'Hyperledger Fabric: A distributed operating system for permissioned block-chains', in Proc. 13th EuroSys Conf, Porto, Portugal, pp. 1-15, 2018. doi.org/10.1145/3190508.3190538

[14] C. Esposito, A. Santis, G. Tortora, H. Chang, and K.-K. R. Choo, 'Block-chain: A panacea for healthcare cloud-based data security and privacy?', IEEE Cloud Computing, vol. 5, no. 1, pp. 31-37, Feb. 2018. doi.org/10.1109/MCC.2018.011791712

[15] D. Stefanescu, L. Montalvillo, P. Galán-García, J. Unzilla, and A. Urbieta, "A systematic literature review of lightweight blockchain for IoT," IEEE Access, vol. 10, pp. 123138-123159, 2022 doi.org/10.1109/ACCESS.2022.3224222

[16] S. Mehedi, A. Zaman, and M. Alazab, 'Federated learning with block-chain for privacy-preserving clinical data analytics in multi-hospital environments', Future Generation Computer Systems, vol. 127, pp. 185–198, Feb. 2022. doi.org/10.1016/j.future.2021.09.004

[17] B. Shen, J. Guo, and Y. Yang, 'MedChain: Efficient healthcare data sharing via block-chain', Applied Sciences, vol. 9, no. 6, Mar. 2019. doi.org/10.3390/app9061207

[18] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized Identifiers (DIDs) v1.0," W3C Recommendation, Jul. 2022. doi.org/10.17487/RFC0001

[19] K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "An extensive blockchain-based applications survey: Tools, frameworks, opportunities, challenges and solutions," IEEE Access, vol. 10, pp. 116858-116906, 2022 doi.org/10.1109/ACCESS.2022.3219160

[20] A. Reyna, C. Martin, J. Chen, E. Soler, and M. Diaz, 'On block-chain and its integration with IoT: Challenges and opportunities', Future Generation Computer Systems, vol. 88, pp. 173-190, Nov. 2018. doi.org/10.1016/j.future.2018.05.046

[21] Q. Xu, K. M. M. Aung, Y. Zhu, and K. L. Yong, 'A block-chain-based storage system for data analytics in the Internet of Things', in New Advances in the Internet of Things, Cham: Springer, 2018, pp. 119-138. doi.org/10.1007/978-3-319-58190-3_8

[22] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, 'Internet of Things (IoT): A vision, architectural elements, and future directions', Future Generation Computer Systems, vol. 29, no. 7, pp. 1645-1660, Sept. 2013. doi.org/10.1016/j.future.2013.01.010

[23] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, 'Integrating block-chain for data sharing and collaboration in mobile healthcare applications', in Proc. IEEE 28th Annu. Int. Symp. Personal, Indoor, Mobile Radio Commun. (PIMRC), Montreal, QC, Canada, 2017, pp. 1-5. doi.org/10.1109/PIMRC.2017.8292361

[24] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, 'Block-chain-based medical records secure storage and medical service framework', Journal of Medical Systems, vol. 43, no. 1, Jan. 2019. doi.org/10.1007/s10916-018-1121-4

[25] H. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, 'Block-chain in healthcare and health sciencesA scoping review', International Journal of Medical Informatics, vol. 134, Feb. 2020. doi.org/10.1016/j.ijmedinf.2019.104040

How to Cite: Dr. Mayur R. Bhoyar. (2026). Blockchain-integrated IoT framework for tamper-proof healthcare data management in smart hospitals. International Journal of Information Technology and Computer Engineering (IJITC), 6(1), 56-66. https://doi.org/10.55529/ijitc.61.56.66

BIOGRAPHY OF AUTHOR

Dr. Mayur R. Bhoyar, is an experienced editorial professional with a strong background in academic publishing and peer-review management. He is proficient in OJS and has a proven track record of handling high-volume submissions, coordinating with international editorial boards, and ensuring timely decision-making. He demonstrates the ability to streamline workflows, maintain ethical standards, and foster effective communication with authors, reviewers, and publishers. Email: mayurbhoyar@ieee.org