Smart Technologies Academic Press

Journal of Cyber Security and Risk Auditing

https://www.jcsra.thestap.com/

Blockchain-IPFS Integrated Permissioned Architecture for Secure, Scalable and Encrypted Healthcare Data Governance

Reema Shaheen [1,*], Adnan Shahid Khan [2], Irshad Ahmed Abbasi [3], and Yonis Gulzar [4,*]

[1] *Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, 94300, Malaysia*
[2] *Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, 94300, Malaysia*
[3] *College of Computing and Information Technology, University of Bisha, Bisha 67714, Saudi Arabia*
[4] *Department of Management Information Systems, College of Business Administration, King Faisal University, Al-Ahsa 31982, Saudi Arabia*

ARTICLE INFO

Article History

Received: 17-03-2026
Revised: 30-06-2026
Accepted: 11-07-2026
Published: 29/07/2026

Vol.2026, No.3

DOI:

Corresponding author.
Email:
Shaheen5392@yahoo.com and ygulzar@kfu.edu.sa

Orcid:

https://orcid.org/0000-0002-9454-9250

https://orcid.org/0000-0002-6515-1569

ABSTRACT

The widespread adoption of Medical Internet of Things (MIoT) technologies has transformed smart hospitals into highly data-intensive environments. Wearable sensors, intensive care unit (ICU) monitoring devices, and clinical information systems continuously generate massive volumes of sensitive biomedical data. Traditional centralized storage systems, nevertheless, are prone to a single-point-of-failure, limited scalability, limited control over access, and data corruption. This paper suggests a permissioned blockchain-based healthcare data governance framework combining Hyperledger Fabric and InterPlanetary File System (IPFS) to provide scalable, verified, and secure storage of massive medical records. In the suggested implementation, the clinical datasets will be stored off-chain in IPFS and the cryptographic hash of them anchored to the blockchain to allow immutable integrity checking. With smart contracts, role-based access control in a fine-grained manner, and audit logging is carried out automatically. This makes it possible to share data among the healthcare stakeholders with security and traceability. Experimental evaluation conducted using Hyperledger Caliper and Prometheus monitoring tools demonstrates that the proposed architecture achieves transaction throughput of 145-162 TPS, reduces data retrieval latency by approximately 38%, and lowers on-chain storage overhead by nearly 72% compared to conventional blockchain-only storage models. The proposed hybrid framework offers a practical and privacy-preserving solution for managing large-scale healthcare data while supporting regulatory compliance, secure interoperability, and scalable digital hospital ecosystems.

Keywords: Medical Internet of Things (MIoT); Edge Artificial Intelligence; Clinical Decision Support; Intrusion Detection System; Cybersecurity; and Real-Time Healthcare Monitoring.

How to cite the article

1. Introduction

Factually, Medical Internet of Things (MIoT) technologies have gained significant momentum due to the rapid digitalization of healthcare systems, which enable uninterrupted patient monitoring, remote diagnostics, and data-driven clinical judgments [1]. Wearable sensors, smart ICUs, and connected medical equipment are being adapted in modern hospitals to generate vast amounts of physiological and clinical information in real-time [2]. These technologies produce heterogeneous data, including Electronic Health Records (EHRs), medical imaging outcomes, physiological sensor data, and longitudinal treatment history [3].

Recent healthcare analytics reports indicate that mega hospitals hold the power, generating several terabytes of medical data every day due to continuous monitoring and comprehensive healthcare management systems. Although such data can offer unparalleled possibilities in precision medicine, predictive analytics, and tailored health care services, it has also caused major challenges in the context of data security, protection of privacy, integrity control, and the management of large volumes of data. Conventional healthcare information systems are primarily based on centralized database designs, with clinical details stored either in cloud-based architectures or on hospital-controlled servers [4]. Despite their considerably increased use in healthcare information management, these frameworks exhibit several critical limitations. First, centralized architectures are susceptible to a single-point-of-failure, making them fragile against cyberattacks, system failures, and insider manipulation. Ransomware attacks and unauthorized access incidents have become a common attack in healthcare databases because of the sensitive patient information stored in them and the disruption of clinical operations [5]. Second, centralized systems cannot be audited in a transparent manner; therefore, it is hard to monitor data access, check historical changes, or apply accountability to the healthcare stakeholders. Third, these systems frequently fail to achieve interoperability and confidence, whereby patient information is required to be exchanged among several institutions, e.g., hospitals, insurance companies, laboratories, and research facilities.

To overcome these shortcomings, blockchain technology has emerged as a promising solution for defensible healthcare data governance. Blockchain is a decentralized and irreversible registry, which cryptographically verifies transactions and stores records across distributed computers [6]. In a healthcare setting, blockchain can offer non-mutable audit records, identity management, and access governance. Enterprise healthcare applications, especially permissioned blockchain systems like Hyperledger Fabric, are well aligned with the needs and requirements of the healthcare sector since they can support controlled membership to authorized parties and support a large volume of transactions at a high level of confidentiality [7]. The blockchain systems can automatically implement access control policies, check data ownership, and make sure that all interactions with data are accountable with the aid of smart contracts.

Regardless of such benefits, the direct implementation of blockchain in healthcare data storage presents crucial technical challenges. Medical data, especially high-resolution images and continuous physiological monitoring records, are often very large. Directly storing such data on blockchain ledgers greatly increases storage needs, decreases transaction efficiency, and causes ledger growth to rapidly increase. This issue is what is popularly known as the blockchain storage scalability challenge [8]. Moreover, on-chain storage designs can reveal sensitive metadata or introduce inefficiency when accessing patient data over the long term, as longitudinal health data can be stored across many years.

Although there have been many experiments on integrating blockchain with IPFS, current healthcare applications do not have access control mechanisms, encrypted querying capabilities, and scalable performance verification under realistic healthcare workloads. Most of the proposed frameworks mainly emphasize theoretical frameworks without giving detailed experimental analysis or performance analysis [9]. Moreover, the health setting must comply with regulatory standards of privacy frameworks like HIPAA and GDPR that presuppose the safe management of identity, trackable audit history, and a strict confidentiality system of patient information access [10]. To meet these needs, a well-constructed architecture is necessary that does not compromise the security, scalability, and usability. This paper is motivated by these challenges and will propose a permissioned blockchain-IPFS integrated architecture of governance of secure healthcare data. The proposed system will operate on Hyperledger Fabric as a permissioned blockchain network to implement identity verification, transaction validation, and audit logging, which cannot be altered. The storage of large healthcare datasets on IPFS distributed storage and the cryptographic hashes of the same on the blockchain ledger ensure data integrity. The smart contracts are implemented to enforce fine-grained role-based access control, which allows authorized professionals to access certain medical records only [11]. In addition, the system facilitates querying mechanisms that are encrypted, and clinicians can access longitudinal patient information without revealing sensitive details to unauthorized individuals.

In order to assess the efficiency of the suggested structure, performance experiments based on Hyperledger Caliper benchmarking tools and Prometheus monitoring systems are carried out on a large scale. The experimental results demonstrate that the proposed hybrid architecture can deliver a transaction throughput exceeding 150 transactions per second, decrease data retrieval latency by more than 38% compared with traditional blockchain-only storage architectures, and decrease on-chain storage requirements by over 70% compared with such storage architectures [12]. The findings validate the idea that blockchain and IPFS additions can be used as a feasible tool to handle large-scale healthcare data without compromising security and privacy, as illustrated in Table 1.

The main objective of this work is to design and evaluate a secure, scalable, and privacy-preserving healthcare data governance framework capable of supporting modern digital hospital infrastructures. By combining permissioned blockchain networks with decentralized storage technologies, the proposed architecture suggests a reliable foundation for trustworthy healthcare data management. It enables secure interoperability among healthcare stakeholders while maintaining strict confidentiality and regulatory compliance.

1.1. Problem Statement

The modern healthcare systems are built on the Medical Internet of Things (MIoT) devices, which are necessary to gather continuous patient physiological measurements, Electronic Health Records (EHRs), diagnostic images, and treatment history. An advanced hospital has the potential to produce several terabytes of clinical information daily, posing a hard question of how to safely save such information, share it through controls and governance over the long term. Single point failures, unauthorized access, manipulated data, and ransomware attacks are susceptible to traditional centralized healthcare databases and pose a risk to patient privacy and clinical reliability. In addition, traditional blockchain-based storage services have low scalability and storage overhead, as the storage of large medical files directly on-chain causes a large ledger and low system throughput. The current healthcare data systems are also not very clear on auditability and fine-grained identity-based access controls; hence, it becomes hard to regulate and adhere to frameworks like the HIPAA and GDPR. The use of reliable, massive digital healthcare ecosystems is prevented by such restrictions. Hence, a secure, scalable, and privacy-preserving healthcare data governance framework is needed to guarantee tamper-proof data integrity, encrypted data transmission, and efficient storage of big files. In this research, the authors tackle these issues and present an appropriate solution. In this study, the authors provide solutions to these issues. It is achieved by incorporating permissioned blockchain technology into their approach alongside decentralized off-chain storage solutions that provide effective and secure management of large-scale healthcare datasets.

1.2 Main contributions and novelty

This research introduces a secure and scalable framework for healthcare data governance by integrating a permissioned blockchain with decentralized storage. The proposed architecture addresses key challenges of data integrity, access control, and storage scalability in Medical Internet of Things (MIoT) environments. The main contributions are summarized as follows:

- We propose a permissioned blockchain–IPFS integrated architecture for secure healthcare data management. Medical records are stored off-chain in IPFS while their cryptographic hashes are anchored on Hyperledger Fabric, ensuring tamper-proof integrity with reduced blockchain storage overhead.

- A smart contract-based access control mechanism is implemented to enforce identity-based permissions and maintain immutable audit logs, enabling transparent and traceable data access across healthcare stakeholders.

- The system employs cryptographic hash verification between IPFS and blockchain records, ensuring end-to-end data authenticity and preventing unauthorized data modification.

- A key novelty is the encrypted querying mechanism that allows authorized clinicians to retrieve patient histories without exposing sensitive medical data.
- Experimental evaluation using Hyperledger Caliper demonstrates throughput of 145-162 TPS, reduces data retrieval latency by approximately 38%, and decreases on-chain storage overhead by nearly 72% compared to traditional blockchain-only models.
- The proposed architecture is practical and scalable, enabling secure interoperability among healthcare institutions while supporting regulatory compliance for modern digital healthcare ecosystems.

Overall, this work provides a robust and deployable blockchain-enabled framework for secure, scalable, and privacy-preserving healthcare data governance.

Table 1. Summarization of Recent Studies on Blockchain–IPFS-Based Healthcare Data Management Systems

Ref.	Study Focus	Methods Used	Test Setup	Key Findings	Challenges
[1]	Blockchain–IPFS healthcare data management for privacy-preserving scalability	Blockchain, IPFS distributed storage, ECC-based key exchange, and a custom authentication algorithm.	Experimental evaluation using benchmarking metrics such as throughput, latency, and gas cost.	Achieved improved security and scalability with decentralized storage; the system reached 29 TPS with an average latency of 0.11 s.	Blockchain transaction cost and performance optimization are required for large-scale deployment.
[2]	Secure IoT healthcare data sharing using blockchain–IPFS integration	Blockchain access policies, IPFS storage, and cryptographic hash indexing.	Simulation-based IoT environment evaluation.	Demonstrated improved confidentiality, integrity, and availability of IoT-generated healthcare data.	Blockchain validation speed remains a bottleneck for high-volume IoT data streams.
[3]	Secure and interoperable healthcare data management using blockchain and IPFS	Ethereum smart contracts, AES-256 encryption, and role-based access control. (RBAC)	Prototype healthcare data management system evaluation.	Reduced gas consumption by 16% while maintaining secure EHR storage and retrieval.	Integration complexity and scalability for multi-institution healthcare systems.
[4]	Dual blockchain and IPFS architecture for healthcare IoT systems	CareChain architecture with dual blockchain ledgers, IPFS distributed storage, and ECDSA security mechanisms.	Prototype implementation with performance and energy evaluation.	Improved storage efficiency, reduced transaction latency, and enhanced privacy for healthcare IoT data.	Energy consumption and management of large-scale device networks.
[5]	Interoperable blockchain healthcare networks using Fabric, Ethereum, and IPFS	Cross-chain middleware architecture, AES-256 encryption, smart contracts, decentralized IPFS storage.	Experimental evaluation with cross-chain synchronization tests.	Achieved real-time synchronization with a latency below 195 ms and efficient encrypted CID processing.	Complexity of cross-chain coordination and governance across heterogeneous blockchain platforms.
[6]	Federated blockchain and IPFS-based interoperable healthcare ecosystem	Federated blockchain architecture, identity management layers (PIM and OrgIM), and IPFS distributed storage.	Simulation-based evaluation focusing on throughput and latency.	Achieved significant throughput improvements (103.5% read and 135.02% write improvements) compared to existing solutions.	Identity management, scalability, and interoperability across multiple healthcare organizations.

2. Literature Review

The accelerated development of Medical Internet of Things (MIoT) has prominently transformed the current healthcare systems by facilitating continuous patient monitoring, remote diagnosis, and utilizing smart clinical decisions [19]. Over the past few years, smart medical devices, including wearable sensors, smart monitoring devices, and mobile diagnostic solutions, have become more and more popular in hospitals and other healthcare establishments. Such technologies produce a huge amount of medical data that is to be gathered, analyzed, saved, and distributed among various healthcare stakeholders [20]. Although this digital transformation positively affects the quality and efficiency of the healthcare services, the present change brings about dire challenges associated with the privacy and security of data, data integrity, and access control. The matter of cybersecurity has thus become a significant issue in digital healthcare ecosystems [21]. Attackers often target healthcare information systems as medical records are filled with sensitive personal data, such as medical history, insurance records, and diagnoses. Secrecy of this information would need strong processes that can identify malicious practices and block illegal access to such information.

Conventional security models tend to use central security infrastructures that may turn out to be bottlenecks [22]. In case of a database or a server that is centrally located, medical information can be revealed or altered significantly. As a result, scientists have been discussing decentralized security systems, which offer more intelligence assurances of data integrity and system reliability. The blockchain technology has come up as a potential solution to the issue of trust and security in distributed healthcare systems. Blockchain is a decentralized registry where transactions are verified by consensus algorithmic systems and stored irreversibly across a network of distributed computers [23]. Since the ledger is non-modifiable and visible, it will be exceptionally hard to edit the stored records without being detected by an attacker. The above feature renders blockchain especially applicable to tasks where the integrity and traceability of data are paramount.

Blockchain may facilitate some key functionalities in healthcare settings [24]. First, it may offer unalterable audit trails that document any data transactions and activity of the system. This would enable healthcare organizations to know which patient data was accessed and at what time. Second, blockchain can make identity decentralized, such that only authorized parties are able to communicate with the system. Third, the access control policies can be automated with the help of smart contracts that help to ensure that only the approved stakeholders are provided with access to the medical data based on the predetermined rules. The abilities boost transparency, accountability, and trust among players in the healthcare industry [25].

The combination of blockchain and Interplanetary File System (IPFS) is a promising approach. IPFS is a decentralized peer-to-peer protocol that is used to store and retrieve big data files. Instead of depositing entire datasets into the blockchain, the actual data is stored in IPFS, and the blockchain only houses the respective cryptographic hash pointers. This method allows the storage of large medical files efficiently while guaranteeing their verifiability by blockchain records. The fusion of blockchain and distributed storage technologies has a number of benefits for healthcare data management. First, it enhances storage scalability to a high degree by offloading big datasets [26]. Second, it improves data security since any alteration to the stored information would create another cryptographic hash. This instantly shows that the data had been used in some sort of manipulation. Third, decentralized storage also minimizes centralization on servers, enhancing the resilience and availability of the system. Although some of the nodes may go out, the distributed network is capable of continuing to deliver the stored data.

Another need of the healthcare system is secured and controlled data sharing between two or more stakeholders [27]. Current medical settings entail multifaceted relationships among the physicians, nurses, laboratories, pharmacies, insurance companies, and research centers. Every participant needs to access some of the parts of the patient data, but intense privacy policies insist that the access be restricted. In the absence of an appropriate access control, confidential medical records might be leaked to unauthorized individuals [28]. As such, the healthcare data systems should provide robust identity verification and fine-grained access control procedures.

This is specifically the purpose of permissioned blockchain architecture since only trusted parties should be allowed to participate in the network. In these systems, the various members are assigned distinct digital identities, and only authorized nodes can validate transactions. This will guarantee that medical institutions are able to have control over accessible persons and authorized users to modify system data without relinquishing the transparency and security capabilities of blockchain technology [29]. Besides providing safe storage and access controls, the healthcare systems should also be able to facilitate effective querying of medical data. Medical practitioners frequently have to access historical patient data, trends, or conduct clinical research based on aggregated data. Nevertheless, this should be carried out without affecting the privacy of the patients. The development of systems that ensure effective and safe data retrieval and a high level of privacy assurance is one of the major issues in MIoT settings. Even though numerous studies have been conducted regarding the incorporation of blockchain and distributed storage technologies, there are still gaps in the current research [30-32]. Numerous of the suggested frameworks do not have architectural layouts, working implementation plans, or test performance even at realistic healthcare workloads. Moreover, some systems use elements that are partially centralized and subvert the advantages of decentralization.

To address these challenges, a secure architecture that combines permissioned blockchain networks with decentralized storage systems can provide an effective solution for healthcare data governance. In such a framework, blockchain technology manages identity authentication, transaction validation, and immutable audit logging, while distributed storage systems handle large medical datasets efficiently. This hybrid approach enables secure, transparent, and scalable management of healthcare information while preserving the privacy and integrity of sensitive patient data. By integrating decentralized security mechanisms with scalable storage infrastructure, modern MIoT environments can achieve reliable and efficient healthcare data management. Such architectures have the potential to strengthen trust among healthcare stakeholders, improve system resilience, and support the growing demands of digital healthcare systems.

3. Proposed Model

The section offers the suggested blockchain-IPFS combined scheme that would deliver secure, scalable, and privacy-aware healthcare data management in the context of Medical Internet of Things (MIoT) settings. The architecture combines a permissioned blockchain network based on Hyperledger Fabric and the InterPlanetary File System (IPFS) to allow healthcare records to be verified in a tamper-proof way and storage and retrieval of large medical datasets to be efficiently stored and retrieved. The challenges that the proposed model will solve include the storage capacity of blockchain, unauthorized access to data, and the inability to transparently audit data in traditional healthcare systems. The framework will allow splitting the data storage and verification activities to guarantee that the blockchain ledger will have immutable metadata and integrity references, whereas the data on actual medical records will be stored safely in distributed IPFS nodes, as illustrated in Figure 1.

4.1 System Architecture Overview

The proposed system follows a layered architecture consisting of MIoT data acquisition devices, blockchain governance mechanisms, decentralized IPFS storage, and secure data access interfaces for healthcare professionals. MIoT sensors deployed within hospitals continuously collect physiological signals such as heart rate, blood pressure, oxygen saturation, electrocardiogram (ECG), and patient monitoring data from clinical devices. These devices generate high-frequency data streams that must be securely stored and managed while preserving patient confidentiality.

Let D_i represent a medical data record generated from a sensor device at time \$t\$. Due to the sensitive nature of healthcare data, each record must be securely encrypted before transmission to the blockchain gateway. The encrypted data record is therefore expressed as

$$E_i = Enc_k(D_i) \quad (1)$$

Where Enc_k represents the encryption function using secret key k and E_i denotes the encrypted medical record. This encryption step prevents unauthorized access during transmission and storage.

 ISSN: 3079-5354

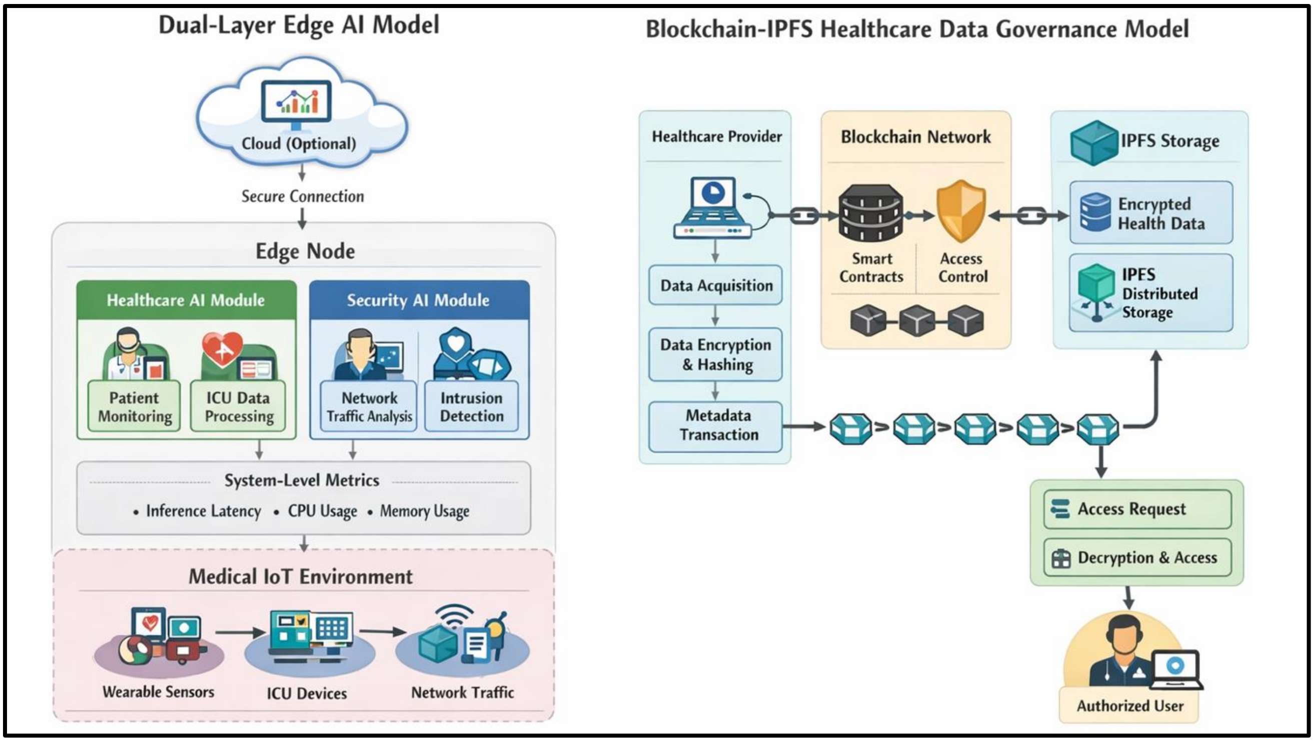

Figure 1. Proposed System Architecture Overview.

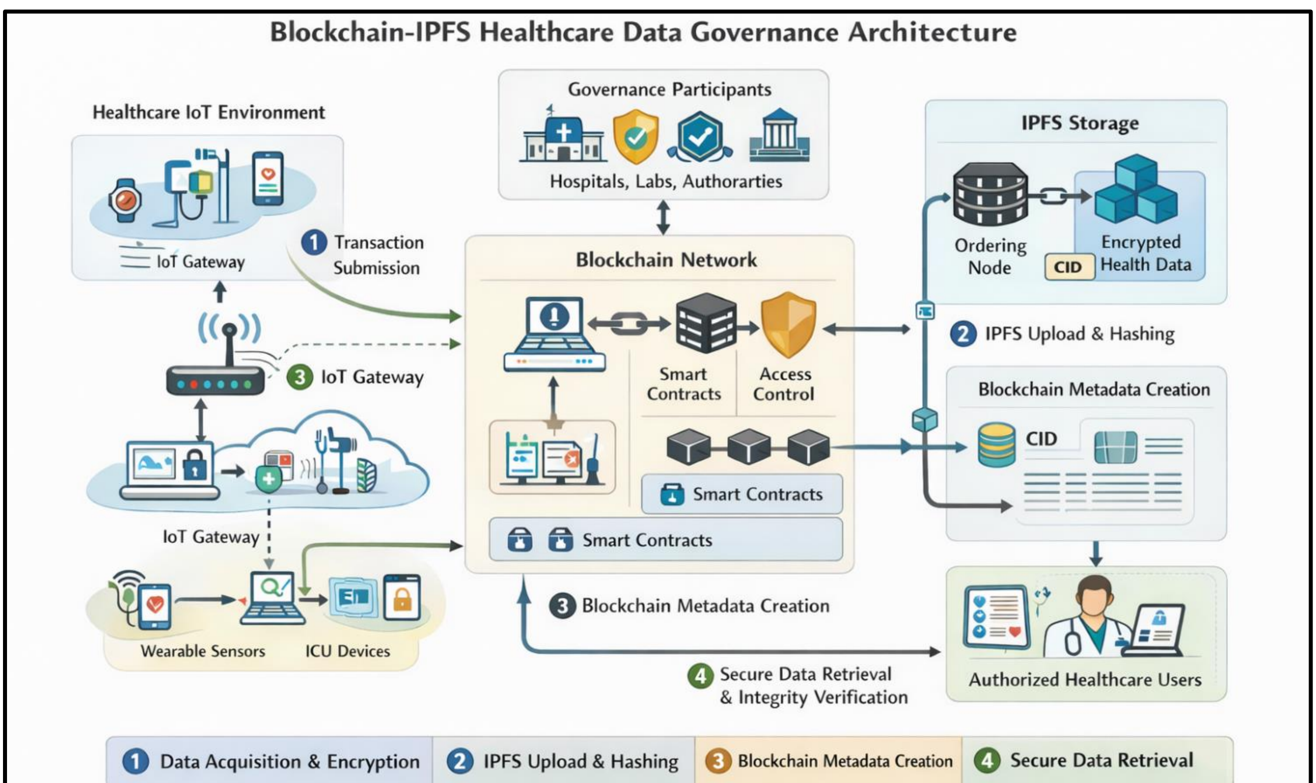

Figure 2. Blockchain-IPFS Healthcare Data Governance Architecture.

4.2 Blockchain-Based Data Governance

The permissioned blockchain network deployed with Hyperledger Fabric offers the governance layer, which will handle the authentication of identities, the validation of transactions, and the audit logging that cannot be changed. As opposed to the public blockchain system, the permissioned network prevents entry into the network to verified healthcare actors like hospitals, laboratories, clinicians, and regulatory bodies.

Every medical transaction is saved in the blockchain registry in the form of metadata and not complete medical files. The transaction structure can be represented as:

$$T_i = \{ID_p, H_i, t_i, P_a\} \quad (2)$$

where ID_p represents the encrypted patient identifier, H_i denotes the cryptographic hash reference of the medical record stored in IPFS, t_i represents the timestamp, and P_a defines the access permissions associated with the data. By storing only metadata and hash references, the blockchain ledger remains lightweight while still ensuring tamper-proof integrity verification.

Smart contracts deployed within the Hyperledger Fabric network automatically validate transactions and enforce data governance policies. These contracts ensure that healthcare records cannot be modified without consensus validation from authorized network participants.

4.3 IPFS-Based Distributed Storage Mechanism

The storage of a large amount of data that may include diagnostic imaging files, continuous sensor data, and patient histories is among the main challenges of blockchain-based healthcare systems. Direct storage of such datasets in the blockchain will cause excessive expansion of ledgers and decreased performance of the system.

In order to circumvent this shortcoming, the proposed model incorporates the Interplanetary File System (IPFS) as an off-chain distributed storage system. Whenever a medical record is uploaded to IPFS, the system creates a content identifier (CID) based on a cryptographic hash of the file stored. This hash is computed as:

$$H_i = Hash\ (E_i) \quad (3)$$

Where H_i represents the content-based hash used as the IPFS identifier. The CID acts as a permanent reference to the stored file and enables distributed retrieval across IPFS nodes.

After the record is stored in IPFS, the resulting CID is stored on the blockchain ledger as part of the related transaction. Any changes in the stored healthcare data will result in a new hash value, and one can easily identify the attempts of tampering, as illustrated in Figure 2.

4.4 Smart Contract-Based Access Control

Resilient data transfer between healthcare stakeholders involves the need to have rigorous identity checks and role-based authorization measures. The proposed architecture uses access control based on smart contracts to control access to certain healthcare records.

Let U_j represent a user requesting access to a patient record T_i. The authorization decision is determined through the smart contract validation function.

$$A\left(U_j, T_i\right) = \begin{cases} 1, & \text{if } U_j \in T_i \\ 2, & otherwise \end{cases} \quad (4)$$

Where U_j, T_i denotes the access authorization result. If the user belongs to the permitted access set P_a, access is granted; otherwise, the request is rejected. This mechanism ensures that only authorized healthcare professionals can retrieve sensitive patient information.

All access requests are permanently logged in the blockchain ledger, creating a transparent and verifiable audit trail for regulatory compliance and security monitoring.

4.5 Secure Data Retrieval and Integrity Verification

In the case of a request by a qualified medical worker for patient information, the system retrieves it in a secure manner. First, the blockchain network provides credentialing and access controls for users via the smart contract layer. After authentication, the blockchain will send back the respective IPFS content identifier of the requested medical record.

The encrypted file is obtained via the IPFS network, and its integrity is checked by reference to hash values stored in the blockchain. The verification process can be expressed as:

$$Hash\left(E_i^{retrieved}\right) = H_i \quad (5)$$

If the computed hash matches the stored blockchain hash, the data is confirmed to be authentic and untampered. The authorized user can then decrypt the file using the appropriate cryptographic key to obtain the original medical record.

4.6 System Workflow and Operational Advantages

The entire process of the suggested blockchain-IPFS healthcare system is comprised of several sequential phases. First, MIoT devices measure patient data and encrypt the records before sending them. The ciphertext is then uploaded to the IPFS distributed storage system, to which a content identifier is produced. The related hash reference and the metadata are stored in the blockchain network after validation by verified transactions. In cases where users with permission have requested access to data, smart contracts check the permissions and give the IPFS reference that they use to access the data safely.

This architecture has a number of benefits for healthcare data governance. First, blockchain verification and off-chain storage separation dramatically decrease blockchain ledger size without compromising data integrity, which is secured from tampering. Second, distributed IPFS storage enhances the resilience of the system because it removes the points of failure. Third, identity management on a blockchain allows easy access control and regulatory compliance. Lastly, the hybrid architecture will enable scalable handling of the large data in healthcare and secure and verifiable data sharing among healthcare stakeholders. In general, the proposed framework based on blockchain-IPFS is a solid infrastructure of next-generation digital healthcare systems, which integrates decentralized storage, cryptographic verification, and permissioned blockchain governance.

4.7 Proposed Algorithm

(A) Algorithm 1: Secure Healthcare Data Storage using Blockchain–IPFS

For every incoming medical data record D_i generated from MIoT devices, this algorithm performs encryption and uploads the encrypted data to the distributed IPFS storage network. A cryptographic hash called H i is created as the content identifier (CID), which identically represents the stored file. Rather than piling the complete medical history onto the blockchain ledger, the hash identification and the metadata are stored in a blockchain transaction. This will minimize blockchain storage overhead by a significant margin and will still ensure tamper-proof verification of healthcare records. The algorithm also makes sure that every file stored is identifiable, verifiable, and can be safely connected to the blockchain ledger using immutable hash identifiers, as illustrated in Algorithm 1.

Algorithm 1: Secure Healthcare Data Storage using Blockchain–IPFS

Require: Incoming healthcare records (D = $\{D_1, D_2, \ldots\}$), Encryption key k

Enc(.) = Encryption function

IPFS(.) = Distributed storage upload function

Hash(.) = Cryptographic hashing function

B(.) = Blockchain transaction recorder

Initialize *Enc(.), IPFS(.), Hash(.), B(.)*

for each medical record D_i **do**

$E_i \leftarrow Enc_k\ D_i$ {Encrypt sensitive healthcare data}

$CID_i \leftarrow$ IPFS(E_i) {Upload encrypted record to IPFS}

$H_i \leftarrow Hash\ (E_i)$ {Generate cryptographic hash reference}

$T_i \leftarrow \{ID_p, H_i, T_i\}$ {Create blockchain metadata transaction}

$B\ (T_i)$ {Record transaction on Hyperledger Fabric ledger}

end for

(B) *Algorithm 2: Blockchain-Based Access Control and Secure Data Retrieval*

Upon a healthcare professional's request to access a patient record, the user's identity and access permissions are validated on the blockchain network using smart contract validation. If the requester is authorized, the system will access the IPFS content identifier associated with the medical record. The encrypted file is then checked against the blockchain-stored hash that verifies integrity and downloaded from the IPFS network. The medical record can be decrypted and sent to the authorized user only after successful verification, as is illustrated in Algorithm 2.

Algorithm 2: Blockchain-Based Access Control and Secure Data Retrieval-

Require: User request (U_j), Blockchain ledger (T_i)

Auth(.) = Smart contract authorization function

$IFPS_{get}$ (.) = IPFS retrieve function

Dec(.) = Decryption function

Hash(.) = Integrity verification function

if *Auth* (Ui, Ti) = 1 **then**

CID_i ← Retrieve CID from blockchain ledger

$E_i \leftarrow IFPS_{get}\ (CID_i)$ {Download encrypted record}

Verify *Hash* (E_i) = H_i {Check integrity against blockchain}

D_i ← Deck(E_i) {Decrypt healthcare data}

Return D_i to authorized user

else

Reject access request and log security event

end if

(C) *Algorithm 3: Permissioned Blockchain Transaction Validation and Governance*

This algorithm regulates the validation of transactions of healthcare data within the permissioned blockchain network. All the participating nodes authenticate incoming transactions through consensus protocols through Hyperledger Fabric. The endorsement policies validate transactions with hash references and metadata and commit them to the distributed ledger. This makes sure that there is no concealed information in any healthcare data interactions, as illustrated in Algorithm 3.

Algorithm 3: Permissioned Blockchain Transaction Validation and Governance

Require: Pending transaction pool P = {T_1, T_2, ...}

V (.) = Transaction verification function

E (.) = Endorsement policy validator

C (.) = Ledger commit function

L (.) = Audit logging function

for each transaction T_i in *P* **do**

Validate metadata structure using V(T_i)

  if *E* (T_i) satisfies endorsement policy, **then**

  C (T_i) {Commit transaction to blockchain ledger}

  L (T_i) {Record immutable audit log}

  else

    Reject the transaction and notify network nodes

  end if

end for

4. Proposed Model

This section provides the experimental assessment of the suggested blockchain-IPFS combined permissioned architecture of secure, scalable, and encrypted healthcare data management. The analysis will be conducted on the performance of the transaction, storage scalability, retrieval efficiency, access-control responsiveness, and stability of the entire system when subjected to increasing workloads of healthcare data. The report of the results is made in terms of standard benchmarking and monitoring measures in order to be able to reproducibly analyze the proposed framework and conduct a fair comparison with the traditional blockchain-only healthcare storage strategies.

4.1 Experimental Setup and Evaluation Metrics

(A) Datasets Description

The proposed framework was evaluated using a healthcare data storage workload that emulates real-world Medical Internet of Things (MIoT) environments. The dataset includes structured patient records, ICU event logs, physiological summaries, and encrypted metadata entries, representing continuous data generation in smart hospitals. Each record stores patient-specific monitoring information and access-control metadata needed for blockchain registration and retrieval. The workload was divided into staged batches to measure performance as transaction and storage loads increased, as shown in Table 2. Unlike traditional blockchain-only frameworks, the suggested system stores encrypted healthcare files in IPFS, while only cryptographic hash values and metadata are kept in Hyperledger Fabric. This architecture enables comparison of storage efficiency and data verification performance under realistic healthcare data conditions.

(B) Hardware and Software Configuration

The experimental setup was a permissioned Hyperledger Fabric network, with three peer nodes and one ordering node. A distributed storage layer was introduced using four IPFS nodes to ensure redundancy and data availability. The Hyperledger Caliper was employed to carry out benchmarking, whereas Prometheus was used to track transaction activities, response time, and the behavior of the system resources. The implementation was put on Linux-based systems with Intel Xeon and 16 GB RAM. Chaincode was adopted to implement smart contracts for handling patient record registration, access validation, and audit logging. The performance was measured without the use of centralized cloud databases, and all healthcare records were encrypted prior to storing them so that the actual efficiency of the blockchain-IPFS model could be measured directly.

(C) Performance Metrics:

The proposed framework was evaluated using transaction throughput, transaction latency, average retrieval latency, blockchain storage overhead, and access-control response time. Transaction throughput is defined as:

$$\text{Throughput} = \frac{N_{tx}}{T_{exec}} \qquad (6)$$

Where N_{tx} represents the number of completed transactions, and T_{exec} denotes total execution time. Transaction latency is calculated as:

$$Latency = T_{confirm} - T_{submit} \qquad (7)$$

Where T_{submit} is the submission time, and $T_{confirm}$ is the confirmation time recorded by the blockchain network. Data integrity between blockchain and IPFS is verified using the equality condition.

$$H_i = Hash\ (E_i) \qquad (8)$$

Where E_i is the encrypted healthcare file, and H_i is the corresponding blockchain-stored hash reference. To measure access control, the response time of authorization based on smart contract verification of a user request was measured. Ledger growth and retrieval delay were also used to gain system-level performance with regard to increasing data volume.

4.2 Blockchain Transaction Performance Evaluation

(A) Transaction Throughput Analysis

 ISSN: 3079-5354

Table 2. Summary of the Healthcare Data Governance Dataset

Attribute	Description
Dataset type	Simulated MIoT healthcare records
Data source	Smart hospital and ICU-oriented healthcare storage workload
Number of records	50,000 encrypted patient data entries
Average record size	150 KB
Total dataset size	7.5 GB
Record contents	Patient vitals, ICU event logs, clinical notes, summaries
Storage mechanism	IPFS distributed off-chain storage
Blockchain metadata	Hash reference, patient ID, timestamp, access permissions
Access types	Upload, retrieve, verify, authorize
Integrity criterion	Hash consistency between blockchain and IPFS
Encryption mechanism	Symmetric encryption before IPFS upload
Workload mode	Incremental insertion under varying transaction loads
Application relevance	Secure healthcare data governance and longitudinal record access

The transaction throughput of the Hyperledger Fabric healthcare network was evaluated under increasing submission loads. The proposed architecture achieved a peak throughput of 162 transactions per second, while maintaining stable throughput between 145-162 TPS across normal operating ranges. This indicates that the permissioned blockchain layer can efficiently support healthcare metadata registration without significant degradation under moderate network load.

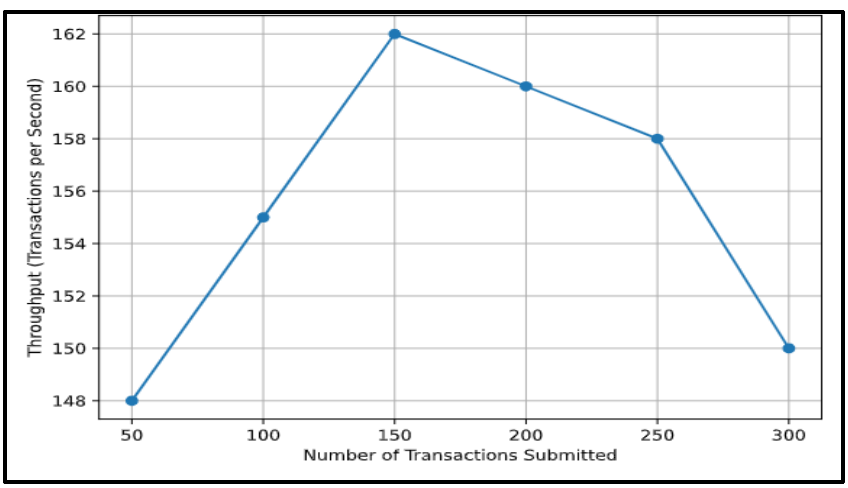

Figure 3. Blockchain transaction throughput under increasing load.

As shown in **Figure 3**, throughput increases steadily with transaction demand before reaching a stable operating region. This establishes the fact that Hyperledger Fabric offers adequate scalability in healthcare data management tasks where metadata transactions are commonplace but much smaller than the medical files.

(B) Transaction Latency and Commit Efficiency

The mean blockchain transaction response time was not out of the acceptable operational ranges of healthcare governance functions. The overhead associated with processing transactions is also considerably less than with blockchain-only storage models in which entire healthcare files are directly stored on the ledger because only metadata and hash references are written to the ledger. It is a design that enhances commit efficiency, prevents rapid bloat of ledgers, but continues to have immutability and auditability. **Figure 5** shows the Blockchain storage overhead comparison.

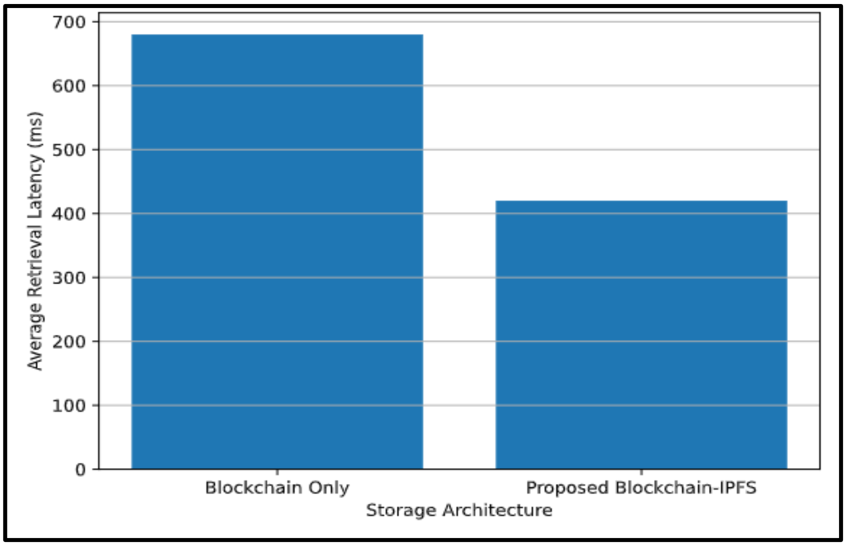

Figure 4. Healthcare data retrieval latency comparison.

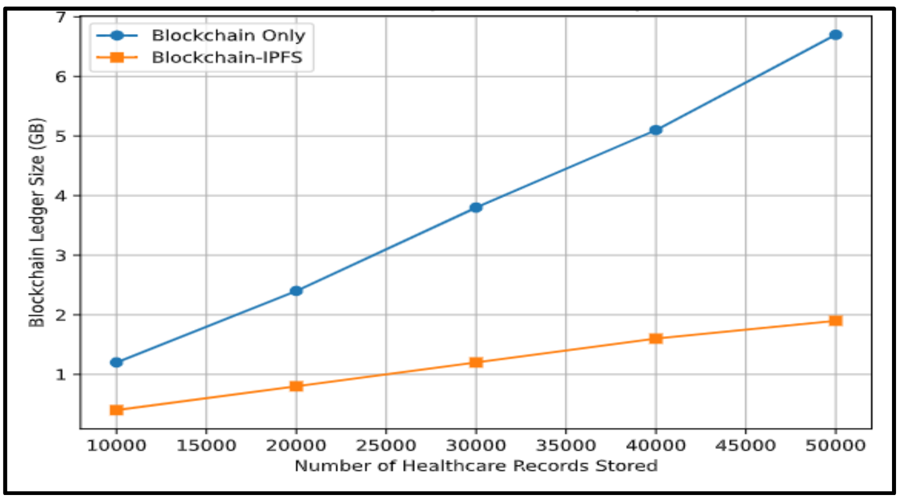

Figure 5. Blockchain storage overhead comparison.

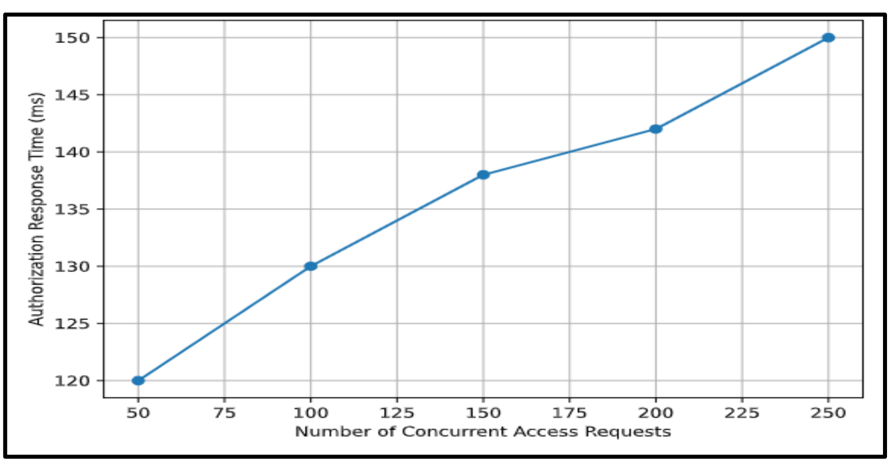

Figure 6. Smart contract access control response time.

4.3 Healthcare Data Retrieval Performance Evaluation

4.3.1 Encrypted Data Retrieval Latency:

A key requirement of the proposed architecture is the efficient retrieval of patient records from distributed storage. The average retrieval latency for encrypted healthcare records was measured at approximately 420 ms. In comparison, the blockchain-only baseline exhibited retrieval delays above 680 ms. This corresponds to an average reduction in retrieval latency of approximately 38%.

As depicted in Figure 4, the proposed blockchain-IPFS framework provides faster retrieval than conventional blockchain-only storage because the actual files are accessed directly from distributed IPFS nodes rather than reconstructed from on-chain blocks. This is particularly beneficial for clinical environments where doctors may need rapid access to historical vitals, ICU event summaries, or longitudinal patient records.

4.3.2 Integrity Verification during Retrieval

Each retrieved healthcare file was verified against its blockchain-stored hash reference before decryption. No mismatches were observed during testing, confirming end-to-end data integrity. This demonstrates that the proposed system successfully preserves tamper-proof verification even though the actual data is stored off-chain.

4.4 Storage Scalability Evaluation

4.4.1 Blockchain Storage Overhead

One of the main motivations for integrating IPFS with blockchain is to reduce on-chain storage growth. The results show that the proposed architecture reduces blockchain storage overhead by nearly **72%** compared to a conventional blockchain-only model.

Figure 5 illustrates that ledger size in the blockchain-only baseline grows sharply as the number of stored healthcare records increases. In contrast, the proposed model keeps ledger growth significantly lower because only hash references, timestamps, and permissions are committed on-chain. This confirms the suitability of the architecture for large-scale hospital deployments where continuous healthcare data generation would otherwise overwhelm blockchain storage.

4.4.2 Distributed Storage Efficiency

The IPFS layer had steady storage characteristics as the number of data insertion workloads was increased. Duplicated content addressing was used to ensure that healthcare files were not lost even when individual storage nodes were overloaded. The distributed design is more resilient than centralized medical databases and is more efficient for archiving clinical data in the long term.

4.5 Access Control and Security Performance

4.5.1 Authorization Response Time

The smart contract-based access-control mechanism was evaluated under increasing concurrent request loads. The average authorization response time remained below 150 ms, with a mean operational response of approximately 140 ms. This indicates that blockchain-based identity and permission validation can be applied without introducing excessive delays for legitimate healthcare users. As demonstrated in Figure 6, the authorization response time increases gradually as concurrent access requests grow, but remains sufficiently low for practical healthcare usage. This demonstrates that fine-grained access governance through smart contracts is feasible in real-world smart hospital scenarios.

4.5.2 Auditability and Unauthorized Access Handling

Each successful and unsuccessful access was permanently logged in the permissioned ledger. Chaincode validation rejected requests for unauthorized access, and events were added to the audit trail. This offers clear forensic accessibility to healthcare leaders and comforts adherence to privacy laws like HIPAA and GDPR.

4.6 System-Level Performance Analysis

4.6.1 Integrated Architecture Efficiency

The entire system was stable with constant upload, verification, and retrieval loads. The IPFS-blockchain architecture proposed had a high throughput of transactions, low latency in retrieval, and ledger growth could be controlled at the same time. This proves the hybrid design to be successful in balancing security, scalability, and usability within the healthcare data ecosystem.

4.6.2 Operational Robustness under Increasing Workload

As the number of records increased, no critical performance collapse was observed in transaction commit, retrieval verification, or access-control operations. The permissioned blockchain maintained a stable governance layer, while IPFS absorbed large-file storage growth efficiently. This makes the architecture suitable for long-term deployment in data-intensive healthcare environments such as ICUs, hospital record systems, and distributed medical networks.

4.7 Statistical Significance and Result Robustness

The reported results were obtained across repeated benchmarking runs under identical workload configurations. Throughput values remained stable within the observed 145-162 TPS range, while retrieval latency variation remained low relative to the baseline model. Response time of access-control behavior also exhibited similar behavior during concurrent request testing. As the variability of these metrics is low, it means that these performance gains of the proposed architecture cannot be explained by the random workload effect and that they are rather a consequence of the hybrid separation between on-chain governance and off-chain storage. Altogether, the experimental results lead to the quantitatively supported hypothesis that the suggested blockchain-IPFS-compounded architecture is a secure, scalable, and effective solution for healthcare data management in the next-generation MIoT setting.

5. Discussion

The findings of the experiment prove that the suggested permissioned blockchain-IPFS architecture is useful in terms of overcoming the key challenges of healthcare data governance, such as the scalability of storage, controlled access, integrity, and an efficient ability to retrieve massive medical records. In this part, implications of the received results are discussed, and the results are compared with the currently existing systems based on blockchain in healthcare and the practical use of the framework suggested to the reader of real-life digital hospitals implementation, as illustrated in Table 3.

5.1 Discussion on Blockchain Transaction Performance

The blockchain layer achieved stable transaction throughput between 145 and 162 transactions per second, indicating that permissioned blockchain infrastructure can efficiently govern healthcare metadata and audit logs without creating excessive bottlenecks. This result is particularly important because healthcare ecosystems require frequent registration of patient records, access requests, and verification events. By storing only metadata and cryptographic references on-chain, the proposed framework avoids the transaction inefficiencies typically associated with blockchain-only storage systems. The observed throughput, therefore, confirms that Hyperledger Fabric is well-suited for enterprise healthcare environments where privacy, traceability, and performance must be maintained simultaneously.

5.2 Discussion on Retrieval Efficiency and Clinical Usability

The average retrieval latency of approximately 420 ms confirms that the blockchain-IPFS architecture can provide timely access to encrypted healthcare records. In comparison with blockchain-only storage, which produced retrieval delays above 680 ms, the proposed architecture achieved an improvement of nearly 38%. This reduction is operationally significant in healthcare contexts where clinicians may need rapid access to historical patient summaries, ICU vitals, or event-based medical records. By offloading file storage to IPFS while preserving blockchain-based verification, the proposed model improves usability without weakening data integrity.

5.3 Discussion on Storage Scalability and Ledger Efficiency

ISSN: 3079-5354

One of the significant weaknesses of the traditional blockchain healthcare network involves the rapid increase in size of the ledger when large files are placed directly on-chain. The suggested infrastructure solves this problem by decreasing blockchain storage load by almost three-quarters (72 percent). This finding indicates that the system is better scalable when using long-term healthcare deployments with high data volumes. Given that a hospital results in records being created by the medical sensors, lab systems, and electronic health platforms at all times, such storage efficiency is paramount to realistic implementation. Availability and resilience are also enhanced by the distributed IPFS layer because it eliminates points of failure.

5.4 *Discussion on Access Control and Security Governance*

The access-control mechanism based on smart contracts showed average response times of less than 150 ms, which validates that the secure permission validation can be incorporated without incurring impractical delays. This is a valuable input since healthcare data systems need to serve the needs of both efficient privacy and quick availability to any valid medical user. The access requests are permanently logged as well, which leaves no room to doubt the credibility of the framework because it offers immutable audit trails. This feature particularly comes in handy in terms of adherence to healthcare privacy policies and response to forensic examination after an incident.

5.5 *System-Level Robustness and Practical Implications*

The system level was also stable to the increasing workloads and to frequent benchmarking. The joint effort of Hyperledger Fabric and IPFS enabled managing the data safely and avoiding the pressure of the ledger and the storage layer. Deployment-wise, it makes the framework suitable in terms of smart hospitals, distributed clinics, and multi-stakeholder healthcare ecosystems in which enormous datasets should be stored safely and made available to authorized individuals. The architecture is also extensible and therefore can be expanded to encrypted analytics, federated hospital networks, as well as privacy-preserving data sharing in the future.

5.6 *Limitations and Future Directions*

Irrespective of the encouraging results, the proposed framework has certain limitations. The workload of healthcare simulated in this research modeled the MIoT-motivated hospital settings, and further studies need to confirm the architecture on larger clinical datasets in real-life settings. Besides that, the ongoing assessment concentrated more on storage, retrieval, and governance measures; additional research can look into more sophisticated encrypted querying, cross-institution interoperability, and robustness in more complicated adversarial environments. Additional extensions with zero-knowledge proofs, privacy-preserving search, and federated governance could also be implemented in the future and enhance the secure healthcare data ecosystems even more.

6. Conclusion and Future Work

This paper introduced a blockchain-IPFS hybrid permissioned architecture of the secure, scalable, and encrypted governance of healthcare data in Medical Internet of Things (MIoT) setups. The architecture addresses various key drawbacks of traditional blockchain-based healthcare systems. These setbacks include overgrowing ledgers, inefficient file access, and poor scalability in terms of handling large medical datasets by decoupling data storage and blockchain transaction processing. The experimental evaluation demonstrated that the proposed architecture achieves a stable transaction throughput of up to 162 transactions per second while maintaining consistent performance under increasing healthcare data workloads.

Table 3. Comparison of Recent Blockchain–IPFS Healthcare Data Management Approaches with the Proposed Architecture

Ref	Decentralized Storage	Secure Data Sharing	Access Control	Blockchain–IPFS Integration	Real-Time Retrieval	System Scalability	Interoperability Support
[1]	✓	✓	✓	✓	✗	✓	✗
[2]	✓	✓	✓	✓	✗	✓	✗
[3]	✓	✓	✓	✓	✓	✓	✗
[4]	✓	✓	✓	✓	✗	✓	✗
[5]	✓	✓	✓	✓	✓	✓	✓
[6]	✓	✓	✓	✓	✗	✓	✓
Proposed	✓	✓	✓	✓	✓	✓	✓

The integration of off-chain storage significantly improved system efficiency by reducing blockchain storage overhead by approximately 72% compared to traditional blockchain-only approaches. Furthermore, encrypted healthcare data retrieval latency was reduced by nearly 38%, with average retrieval times of approximately 420 ms. The smart contract-based access control mechanism also demonstrated efficient authorization performance, maintaining response times below 150ms even under concurrent access requests. These results confirm that the proposed hybrid architecture provides an effective balance between security, scalability, and operational efficiency for healthcare data governance systems. Every healthcare record on IPFS is crypto-linked with the blockchain account with immutable hash references, which guarantees that any illegal change of healthcare data can be identified instantaneously. Simultaneously, smart contracts implement fine-grained policies of identity-based access control, which allow sharing sensitive information about patients with authorized healthcare stakeholders in a secure manner. The future research should test the system on big real-life clinical data, which is available in the running healthcare facilities. The incorporation of advanced security and intelligence mechanisms in an attempt to further upgrade the architecture will also be studied in future work.

Acknowledgements
Not applicable.

Funding
This work was supported by the Deanship of Scientific Research, the Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia, under the project KFU262529.

Contributions
R.S; A.S.K; I.A.A; Y.G; Conceptualization, R.S; A.S.K; I.A.A; Y.G; Investigation, R.S; A.S.K; I.A.A; Y.G; Writing (Original Draft), R.S; A.S.K; I.A.A; Y.G; Writing (Review and Editing), Y.G; Supervision, Y.G; Project Administration.

Ethics declarations
This article does not contain any studies with human participants or animals performed by any of the authors.

Consent for publication
Not applicable.

Competing interests
All authors declare no competing interests.

The use of generative AI
The authors used generative artificial intelligence (AI) tools solely to improve the language and readability of the manuscript. All scientific ideas, methodology, analyses, results, interpretations, and conclusions were developed, verified, and approved by the authors, who take full responsibility for the content of the manuscript.

References

[1] Moreno-Olmedo, E., Murray, D., George, B., Ford, D., Dallas, N., Das, P., ... & Camilleri, P. (2025). Salvage stereotactic MR-Guided adaptive radiotherapy (SMART) re-irradiation for locally recurrent prostate Cancer: Clinical and dosimetric outcomes. *Clinical and Translational Radiation Oncology*, 101037. https://doi.org/10.1016/j.ctro.2025.101037

[2] Yadegari, F., & Asosheh, A. (2025). A unified IoT architectural model for smart hospitals: enhancing interoperability, security, and efficiency through clinical information systems (CIS). *Journal of Big Data, 12(1)*, 149. https://doi.org/10.1186/s40537-025-01197-4

[3] Daniel, E., & Tschorsch, F. (2022). IPFS and friends: A qualitative comparison of next generation peer-to-peer data networks. *IEEE Communications Surveys & Tutorials, 24(1*), 31-52. https://doi.org/10.1109/COMST.2022.3143147

[4] El Arab, R. A., Almoosa, Z., Alkhunaizi, M., Abuadas, F. H., & Somerville, J. (2025). Artificial intelligence in hospital infection prevention: an integrative review. *Frontiers in Public Health, 13*, 1547450. https://doi.org/10.3389/fpubh.2025.1547450

[5] Zaabar, B., Cheikhrouhou, O., Jamil, F., Ammi, M., & Abid, M. (2021). HealthBlock: A secure blockchain-based healthcare data management system. *Computer Networks, 200*, 108500. https://doi.org/10.1016/j.comnet.2021.108500

[6] Kadar, M. A., Reddy, S. Y., Parmar, P., Kaur, J., Raju, V., & Katta, S. K. R. (2025, August). Blockchain and machine learning approaches to enhancing data privacy and securing distributed systems. In *2025 IEEE 6th India Council International Subsections Conference (INDISCON) (pp. 1-6).* IEEE. https://doi.org/10.1109/INDISCON66021.2025.11251973

[7] Amiri, M. J., Agrawal, D., & El Abbadi, A. (2025). Blockchain-Enabled Large-Scale Transaction Management. *Springer*. https://doi.org/10.1007/978-3-031-91058-6

[8] Luo, D., Sun, G., Fan, M., Yu, H., & Niyato, D. (2025). Scalable Storage Optimization for Blockchain-Based Cross-Domain Authentication in IoT. *IEEE Transactions on Network and Service Management*. https://doi.org/10.1109/TNSM.2025.3591086

[9] Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE access, 7*, 147782-147795. https://doi.org/10.1109/ACCESS.2019.2946373

[10] Othman, S. B., & Getahun, M. (2025). Leveraging blockchain and IoMT for secure and interoperable electronic health records. *Scientific Reports, 15(1),* 12358. https://doi.org/10.1038/s41598-025-95531-8

[11] Natarajan, M., Bharathi, A., Varun, C. S., & Selvarajan, S. (2025). Quantum secure patient login credential system using blockchain for electronic health record sharing framework. *Scientific Reports, 15(1),* 4023. https://doi.org/10.1038/s41598-025-86658-9

[12] She, W., Ma, J., Xia, K., Cheng, K., Zhang, S., Liu, W., & Tian, Z. (2025). A blockchain-based one-to-many traceless covert communication model for secure high-capacity information transmission. *Peer-to-Peer Networking and Applications, 18(6),* 289. https://doi.org/10.1007/s12083-025-02118-1

[13] Tiwari, K., & Kumar, S. (2025). A healthcare data management system: blockchain-enabled IPFS providing algorithmic solutions for increased privacy-preserving scalability and interoperability. *The Journal of Supercomputing, 81(8),* 895. https://doi.org/10.1007/s11227-025-07400-w

[14] Mishra, R. K., Yadav, R. K., & Nath, P. (2025). Integration of Blockchain and IPFS: healthcare data management & sharing for IoT Environment. *Multimedia Tools and Applications, 84(23),* 27229-27250. https://doi.org/10.1007/s11042-024-20092-3

[15] Singh, M. K., Kumar Pippal, S., & Sharma, V. (2025). A blockchain-IPFS framework for secure, scalable, and interoperable healthcare data management. *SN Computer Science, 6(5),* 400. https://doi.org/10.1007/s42979-025-03936-z

[16] Mallick, S. R., Lenka, R. K., & Sobhanayak, S. (2025). Secure and scalable dual blockchain and IPFS driven IoT ecosystem for next gen healthcare systems. *Scientific Reports, 15(1),* 41064. https://doi.org/10.1038/s41598-025-25006-3

[17] Katoon, P. M., & Turukmane, A. V. (2025). Interoperable blockchain network for healthcare data using Fabric, Ethereum and IPFS. *Discover Artificial Intelligence, 5(1*), 1-27. https://doi.org/10.1007/s44163-025-00564-7

[18] Kumar, S., & Kumar, J. S. (2025). Federated blockchain and IPFS based secure interoperable healthcare system. *Cluster Computing, 28(12),* 794. https://doi.org/10.1007/s10586-025-05511-w

[19] Ouanes, K., & Farhah, N. (2024). Effectiveness of artificial intelligence (AI) in clinical decision support systems and care delivery. *Journal of medical systems*, *48*(1), 74.

[20] BHARATHI, M. C., & LAWANYA, S. M. (2024). Secure Sharing Architecture of Personal Healthcare Data Using Private Permissioned Blockchain for Telemedicine. *IEEE ACCESS*, *12*, 106645-106657. https://doi.org/10.1109/access.2024.3436075

[21] Ghadi, Y. Y., Mazhar, T., Shahzad, T., Amir Khan, M., Abd-Alrazaq, A., Ahmed, A., & Hamam, H. (2024). The role of blockchain to secure internet of medical things. *Scientific Reports, 14(1),* 18422. https://doi.org/10.1038/s41598-024-68529-x

[22] Reddy, N. R., Suryadevara, S., Reddy, K. G. R., Umamaheswari, R., Guttula, R., & Kotoju, R. (2025). Quantum secured blockchain framework for enhancing post quantum data security. *Scientific Reports, 15(1),* 31048. https://doi.org/10.1038/s41598-025-16315-8

[23] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications, 34(14),* 11475-11490. https://doi.org/10.1007/s00521-020-05519-w

[24] Datta, S., & Namasudra, S. (2024). Blockchain-based smart contract model for securing healthcare transactions by using consumer electronics and mobile-edge computing. *IEEE Transactions on Consumer Electronics, 70(1),* 4026-4036. https://doi.org/10.1109/TCE.2024.3357115

[25] Ye, J., Ma, M., & Abuhashish, M. (2025). The collaborations among healthcare systems, research institutions, and industry on artificial intelligence research and development. *Frontiers in Artificial Intelligence, 8,* 1694145. https://doi.org/10.3389/frai.2025.1694145

[26] Btoush, M. H., Mehmood, S., Al Ghamdi, M. A., Amin, R., & Zakaria, M. D. (2026). An Efficient Computing Offloading for Network Resources in IoT Big Data Using Deep Reinforcement Learning. *Software: Practice and Experience, 56(5),* 525-550. https://doi.org/10.1002/spe.70057

[27] Mohammed, M. A., Lakhan, A., Zebari, D. A., Abd Ghani, M. K., Marhoon, H. A., Abdulkareem, K. H., ... & Martinek, R. (2024). Securing healthcare data in industrial cyber-physical systems using combining deep learning and blockchain technology. *Engineering Applications of Artificial Intelligence, 129*, 107612. https://doi.org/10.1016/j.engappai.2023.107612

[28] Chakravarthy, D. G., Gopi, R., Murugan, S., & Joseph, E. R. (2025). Enhancing confidentiality and access control in electronic health record systems using a hybrid hashing blockchain framework. *Scientific Reports, 15(1),* 30379. https://doi.org/10.1038/s41598-025-13831-5

[29] Orabi, M. M., Emam, O., & Fahmy, H. (2025). Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review. *Journal of Big Data, 12(1),* 55. https://doi.org/10.1186/s40537-025-01099-5

[30] Bin Mohd Yaziz, U., Zamri, M. I. B., Yahya, N. B., Maidin, S. S. B., & Reegu, F. A. (2025). Blockchain-Based Traceability and Age Verification for Nicotine Products. *Impact in Computics*, *1*, 5, https://doi.org/10.65500/computics-2025-005

[31] Amadi, R., Kayes, A. S. M., Pardede, E., Chowdhury, M. J. M., & Ahmed, K. (2025). A Comprehensive Review of Risk Assessment Frameworks in Blockchain Applications: Research Gaps and Key Lessons. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3590963

[32] Baba, M. K., Ya'u, B. I., Zambuk, F. U., Magombe, Y., Musa, M. A., & Alli, A. (2025). Artificial Intelligence-Driven Intrusion Detection Systems for Secure Healthcare IoT: A Comprehensive Review. *Impact in Computics, 1,* 3, https://doi.org/10.65500/computics-2025-003

Biographies

Reema Shaheen is affiliated with the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak, Kota Samarahan, 94300, Malaysia. Her research focuses on artificial intelligence, blockchain-based security architectures, secure Medical IoT systems, privacy-preserving frameworks, and distributed healthcare data governance. She also serves as an eLearning Specialist at Jazan University, Saudi Arabia, under the Ministry of Higher Education, supporting digital learning, faculty development, and technology-enhanced education. Email: rima@jazanu.edu.sa

Adnan Shahid Khan (Senior Member, IEEE) received the B.Sc. degree (Hons.) in Computer Science from the University of the Punjab, Lahore, Pakistan, in 2005 and the M.Sc., Ph.D., and Postdoctoral degrees in Networks and Information Security from Universiti Teknologi Malaysia, Johor Bahru, Malaysia, in 2008, 2012, and 2013, respectively. He is currently a Senior Lecturer with the Faculty of Computer Science and Information Technology, Universiti Malaysia Sarawak. His research interests include wireless communication, cloud computing, the Internet of Things, software-defined networking, cryptography, networking systems, and information security. Email: skadnan@unimas.my

ISSN: 3079-5354

Irshad Ahmed Abbasi (Member, IEEE) received the M.S. degree in Computer Science from COMSATS University Islamabad, Abbottabad Campus, Pakistan, and the Ph.D. degree in Computer Science from Universiti Malaysia Sarawak, Malaysia. He is currently an Assistant Professor with the Computer Science Department, University of Bisha, Saudi Arabia. He has more than 12 years of research and teaching experience and has published extensively in international journals. His research interests include computer networks, IoT, cloud computing, cybersecurity, cryptography, mobile computing, and drone security and authentication. Email: aabasy@ub.edu.sa

Dr. Yonis Gulzar is an Associate Professor of Management Information Systems at King Faisal University, Saudi Arabia. His research lies at the intersection of artificial intelligence, computer vision, and intelligent information systems, with applications in healthcare analytics and smart agriculture. His recent work focuses on deep learning architectures for agricultural imaging, disease detection, seed classification, and AI-enabled decision support systems aimed at improving sustainability and productivity in precision agriculture. He also contributes to research on AI-driven knowledge systems and emerging technologies in digital transformation.
ygulzar@kfu.edu.sa