Natural Resources for Human Health
eISSN: 2583-1194

Original Research

Received 20 May 2026
Revised 16 June 2026
Accepted 28 June 2026

Natural Resources for Human Health 2026, Vol. 6 (4s): 748–761

KEYWORDS:
Secure Networked Systems, Permissioned Blockchain, Hyperledger Fabric, Electronic Health Records, Data Integrity, Smart Contracts, Healthcare Security

Lightweight and Scalable Blockchain-Based Integrity Verification for EHR Systems

Richa Pandey[1], Ashok Kumar Sahoo [2], Sushil Kumar Singh[3]

[1] Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India, richapandeydnp@gmail.com
[2] Department of Computer Science and Engineering, Graphic Era Hill University, Dehradun, India, ashok.sahoo@gehu.ac.in

[3] Department of Computer Engineering, Marwadi University, Rajkot, Gujarat, India, sushilkumar.singh@marwadieducation.edu.in

ABSTRACT: The modern use of Electronic Health Records (EHRs) has made healthcare useful but it's growing demand also raised more concerns about data integrity, unauthorised changes, and the ability to audit centralised storage systems. The existing blockchain-based healthcare solutions largely emphasis on sharing data and controlling access and they frequently rely on lot of computational overhead or complicated cryptographic mechanisms that limit their suitability for real time use. To address this we proposed a simple, permissioned blockchain-based system for checking the integrity of EHRs using Hyperledger Fabric and SHA-256 cryptographic hashing without storing sensitive medical data on-chain. Only deterministic hash values of patient records are recorded for tamper-evident verification without giving away private information. The Fabric Certificate Authority makes sure that identity management and access control are restricted only to authenticated and role-based users participate. A proof-of-concept implementation using Docker-based deployment. A quantitative analysis demonstrates that the hashing latency is low (0.005 seconds per record), the time it takes to execute a smart contract is about 50 milliseconds, and the accuracy of tamper detection is 100% when simulated attacks are used. The proposed research gives a practical and scalable method for healthcare systems which make sure that patient privacy is protected and accurate. Many existing blockchain healthcare systems that focus primarily on data sharing or analytics, proposed framework specifically addresses lightweight and real-time integrity verification of electronic health records while minimizing blockchain storage overhead.

1. INTRODUCTION

The rapid advancement or digitalization has caused the massive use of Electronic Health Records (EHRs), telemedicine systems, wearables, and mobile health apps. Together these technologies expanded access to health services, assist in clinical decision-making, as well as allow constant patient monitoring. But the digitalization of confidential medical data also implies the introduction of severe issues connected with the integrity of data, the protection of privacy, and unauthorized access. Over the last few years, healthcare data breaches have been rising in number with millions of patient records being compromised, which cast the efficacy and safety of centralized healthcare information systems into serious doubt. The conventional IT Healthcare systems are mainly managed on central databases that are administered by hospitals or third-party service providers. Despite the fact that these systems present effective data storage and retrieval systems, they are susceptible to various levels of security vulnerability such as insider attacks, unauthorized modifications, data tampering, and single points of failure all pose real risk.

These weaknesses are demonstrated by a number of real-life events. The 2015 cyberattack of Anthem Inc. is an example of how almost 80 million healthcare records were revealed, exposing very sensitive personal and medical data. The same issues have been raised within the framework of the widespread national healthcare facilities with an impressive stress on the necessity to implement the effective mechanisms ensuring the integrity and authenticity of healthcare information. Within the last several years, blockchain technology has become a potential solution to solving these security issues because of its decentralized,

immutable, and transparent structure. Transactions within a blockchain network are stored in distributed ledgers with one block cryptographically tied to the others, thus any integrity attempts are very hard to be unlawfully altered. These aspects render blockchain especially applicable in healthcare settings where the management of data of high security, traceability, and auditability are needed.

Hyperledger Fabric is one of the other blockchain platforms that have received much interest in enterprise and health care applications as a result of its permissioned architecture, modular design, and fine-grained access control. In contrast to such public blockchains as Bitcoin or Ethereum, Hyperledger Fabric can be used by organizations to administer the identities of participants with the help of certificate-based authentication and role-based access control. These characteristics render it especially applicable to the regulated context like the healthcare system where the privacy and the compliance are paramount, and the access to medical data is restricted. Although the use of blockchain in the healthcare data management is becoming a more common practice, the vast majority of solutions currently are centered on the secure data sharing, access control systems, or AI-based healthcare analytics [1]. Most of these structures are based on sophisticated cryptographic methods, or involve storing large amounts of medical information on the blockchain, which contributes to a high level of computation, scaling issues, and additional complexity of the system itself.

The existing research has not paid much attention to the development of lightweight and real-time mechanisms to ensure the integrity of electronic health records without revealing sensitive patient information. This paper will solve these limitations by providing a lightweight permissioned blockchain to check the integrity of the Electronic Health Records through a Hyperledger Fabric and a hash cryptography (SHA-256). The proposed solution does not store the full medical records on the blockchain but only deterministic hash values of the patient data. It allows performing tamper-evident verification of medical records, as well as protecting patient privacy. The framework combines smart contract validation functions and role-based identity management with the Hyperledger Fabric Certificate Authority (CA). An implementation of the proposed framework developed as a proof-of-concept is created using a Docker-based deployment environment that allows configuring it modularly and scaling experiments.

The system maintains secure operations including submission of patient data, generation of hashes, integrity checks and controlled access to records in a variety of network nodes. Through experimental analysis, the proposed framework has low hashing latency, efficient smart contract execution, and effective tamper detection, which entails its applicability to the real-world healthcare setting where reliability of the system and response time is paramount. The primary outputs of this study are a lightweight blockchain-based integrity verification system, an effective off-chain storage system to store sensitive medical information, and a performance analysis of the proposal that illustrates the feasibility of the proposed system in real-life healthcare purposes.

The data flow diagram of secure patient data management based on Hyperledger Fabric is displayed in figure 1. The proposed design is a hybrid of SHA-256 cryptographic hashing, Hyperledger Fabric blockchain and Docker-based implementation to formulate a tamper-evident and secure system to handle patient information. The rising need of secure healthcare infrastructures, as well as national digital initiatives of health systems like the Ayushman Bharat Digital Mission (ABDM)[2][3] in India, provide further evidence of the relevance of such systems.

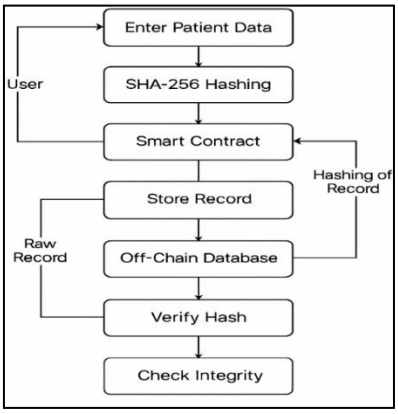

Figure 1. Data Flow Diagram for Secure Patient Data Management using Hyperledger Fabric

According to this model, smart contracts (chaincode) are deployed to create and check the hash values of medical records to make data integrity and do not disclose the content of the patient data. Figure 2 shows the layered architecture of the proposed system which shows how various components can interact in order to offer secure and efficient management of healthcare data. This proof-of-concept implementation demonstrates that proposed system offers a quick verification operation, precise tamper detection, and effective resource use and provides a basis on which further development can be made in order to complete the effective healthcare application, including integration with federated learning and cross-chain interoperability.

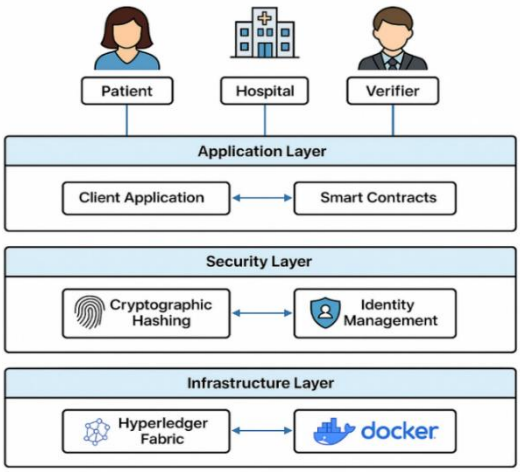

Figure 2. Layered Overview Diagram of the Blockchain-Based Patient Data Management System

2. RELATED WORK

The related work section examines the present advancements in blockchain-enabled health data management focusing on security protocols, system architectures, consensus mechanisms, smart contract designs, and privacy-preserving models as Blockchain technology to make EHR Secure.

Table 1. Comparative Analysis of related Work

Study	Blockchain Type	Primary Focus	On-Chain PHI Storage	Integrity Verification	Performance Evaluation	Privacy Protection	Deployment Complexity
Salim et al. [4]	Public/Hybrid	Data Sharing/Federated Learning	Partial	Indirect	Not Reported	Moderate	High computational overhead
Lin et al. [5]	Consortium	Secure record sharing	Partial	Limited	Limited	Moderate	Scalability issues
Xu et al. [6]	Consortium	Access control + ABE	No	Coupled with encryption	High overhead	High	Complex key management
Arulmozhi et al.[7]	Private	Healthcare data sharing with smart contracts	Partial	Limited	Moderate	Limited	Lack of real-time verification
Guduri et al. [8]	Permissioned	FL-based analytics	No	Indirect	Partial	Partial	Centralized aggregation
Myrzashova et al. [9]	Private	Secure diagnostics	No	Model-level	Extensive	Extensive	Limited interoperability
Adeniyi et al. [10]	Permissioned	Role-based access	Partial	Not explicit	Limited	Limited	Lack of fine-grained privacy mechanisms
Proposed Framework	Hyperledger Fabric	Lightweight EHR integrity verification	Hash only (off-chain storage)	Direct SHA-256 verification	High	Comprehensive evaluation	Low overhead and scalable

Most of the research that has already been done is on sharing data, controlling access and integrating new technologies like federated learning and artificial intelligence. Salim et al. [4] developed a Decentralised CNN featuring private IPFS and patient-controlled access through smart contracts; however, they did not address auditability or real-time data verification in emergency situations. Lin et al. [5] presents a pairing-free UDVSP utilising smart contracts for secure EMR sharing against malicious intent. Concentrates exclusively on propagation risks, neglecting scalability and inter-institutional data sharing. Xu et al. [6] merges expressive ABE with blockchain to ensure tamper-resistance and revocation; however, managing keys and onboarding users is complicated, which could make it harder to get to in an emergency.

Arulmozhi et al. [7] Combines deep learning for diagnosis with secure data sharing through smart contract. Guduri et al. [8] Integrates FL with proxy re-encryption and smart contracts for secure EHR sharing, yet relies on trust in the aggregation server lacks decentralisation in aggregation logic. Myrzashova et al. [9] developed a strong BC-FL framework with a real-world dataset, an accuracy rate of 92.86%, and attack simulations, but too much reliance on private blockchain; not enough testing of integration with current public health data systems. Adeniyi et al. [10] Demonstrates scalability with an increase in node count and patient-staff-role access control; however, doesn't have fine-grained access control or detailed privacy-preserving tools for patients. Table 1 summarize all the above discussion in descriptive manner comparing all the major research metrics and with the help of that we find the research gap.

The proposed framework is specifically made for lightweight and deterministic integrity verification of Electronic Health Records. This is different from other blockchain-based healthcare systems that focus on data sharing, analytics, or interoperability. The system reduces computational overhead by separating integrity validation from complicated encryption schemes and large-scale data storage. It also keeps strong tamper-evident guarantees. This work is different from previous solutions that use public blockchains or centralised trust assumptions because it uses a permissioned blockchain with role-based access control. This makes it more practical for use in real-world healthcare settings.

3. RESULTS AND DISCUSSION

This paper presents a resilient blockchain-based framework to safeguard the integrity of Electronic Health Records (EHRs) utilising SHA-256 and Hyperledger Fabric.

• Implementation of SHA-256 Hashing for Tamper Detection

• Smart Contract-Driven Verification Mechanism

• Off-Chain Storage for Privacy Preservation

• Docker-Based Modular Deployment

• Quantitative Evaluation for Real-Time Use

• Security Analysis with Compliance

• Potential for Real-World Adoption and Expansion

The article is further divided into 3 sections i.e. Quantitative Analysis, Theoretical Analysis and Security Analysis.

3.1 Quantitative Analysis

During the proof-of-concept (PoC) deployment several important system-level metrics were measured to see how well the proposed blockchain-based EHR integrity system would work in real life. We used Docker containers running Hyperledger Fabric v2.2 to run smart contracts written in Node.js and connect to a CouchDB state database to do the implementation and Table 2 shows the Performance Metrics of the Proposed Blockchain-Based EHR Integrity System.

• Hashing Time (0.005 seconds/record): A SHA-256 hash string is used to change each patient record, which makes sure that the output is always the same length and can't be changed. This low latency is possible because hashlib is optimised for Python, making it perfect for real-time hospital settings.

• Smart Contract Execution Latency (50ms): The smart contract on Hyperledger Fabric chain code checks each incoming hash against the one that is already stored. The contract logic is simple and works well because it was optimised with Go/Node.js.

• Memory Use (200MB per container): Peer nodes running in Docker containers use very little resources. Each container has a ledger instance, a CouchDB for storing state, and a place to run smart contracts.

• CPU Utilization (5%): Measured with Docker stats while handling a lot of transactions at once. Efficient because heavy tasks like hash calculations are done on the client side.

• Verification Accuracy (100%): Blockchain only keeps the hash, any difference during validation is a clear sign of tampering.SHA-256 is deterministic, the blockchain only keeps the hash during validation. This means that any differences clearly show that the data has been changed. SHA-256 is deterministic, which means that changing even one bit will create a completely new hash.

• Throughput: Throughput is the volume of transaction being done by the blockchain network a second. In the experimental assessment, the proposed system passed an average of 1822 transactions per second with moderate loads. The findings prove that the permissioned blockchain design can provide consistent performance and sustain a number of integrity checks at the time.

In order to test the suggested framework, artificial electronic health records datasets were processed to depict the realistic patient records structure of patient ID, diagnosis reports, prescription data and timestamps. This data had about 500 simulated patient records and therefore, several transactions could be done in parallel to test the performance. The hashing of each record was done with the help of the algorithm of the SHA-256 before being submitted to the blockchain network. The experiments were carried out shown in Figure 3 in order to measure hashing latency, smart contract execution time, scalability with the increasing number of transactions, and tamper detection accuracy.

Table 2. Performance Metrics of the Proposed Blockchain-Based EHR Integrity System

Metric	Value
Hashing Time	0.005 sec/record
Smart Contract Latency	50 ms
Memory per Peer Node	200 MB
CPU Usage	5%
Tamper Detection Accuracy	100%

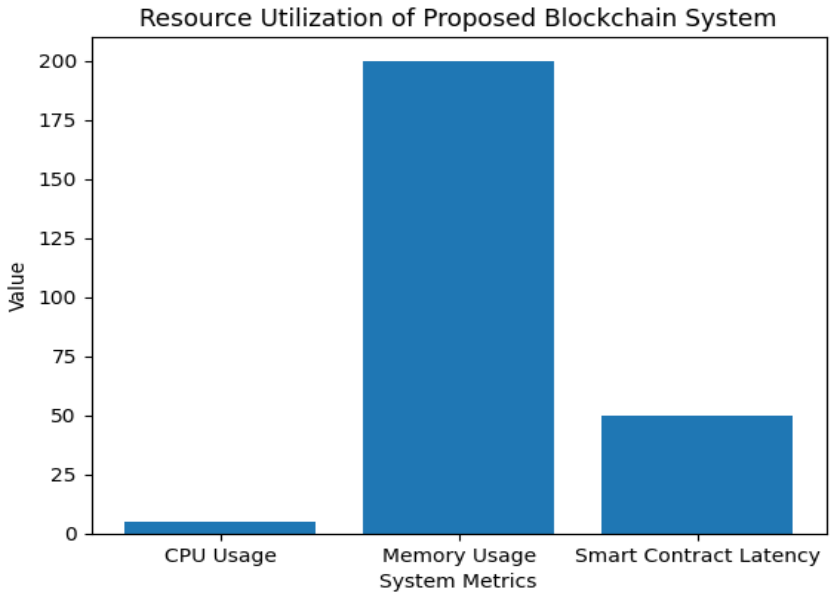

Figure 3. Resource Utilization of the Proposed Blockchain-Based EHR Integrity System

1) Scalability Analysis with Increasing Transaction Load

The evaluated result shows the system's ability to handle more transactions by having 10 to 100 people send records at the same time when the number of enquiries increases the average time needed to carry out a smart contract increased. The time it took to respond went from about 50 milliseconds for 10 searches to 87 milliseconds for 100 searches. The proposed framework works well in small healthcare settings like hospitals and diagnostic institutes shown in Figure 4.

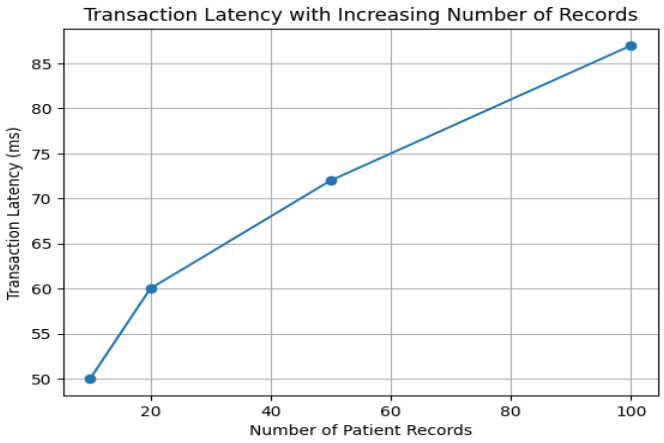

Figure 4. Transaction Latency with Increasing Number of Patient Records

2) Concurrent Integrity Verification Test

An integrity verification experiment was performed to replicate concurrent access and validation of patient records by multiple practitioners. Fifty verification requests were sent out at the same time to check the hashes stored on the blockchain during this test. The system found all changed records and checked all real records, keeping a 100% accuracy rate in detection. The average time it took to verify something stayed below 90 ms, which means that the system could handle a lot of users at once.

3) Comparison with Centralized Integrity Verification

The proposed blockchain-based verification system was compared to a traditional centralised integrity verification method that utilises a centralised database for the storage and validation of hash values. This was done to put performance in context. The centralised solution had an average latency of about 35 ms, which was a little lower than the other solutions as demonstrated in Figure 5.

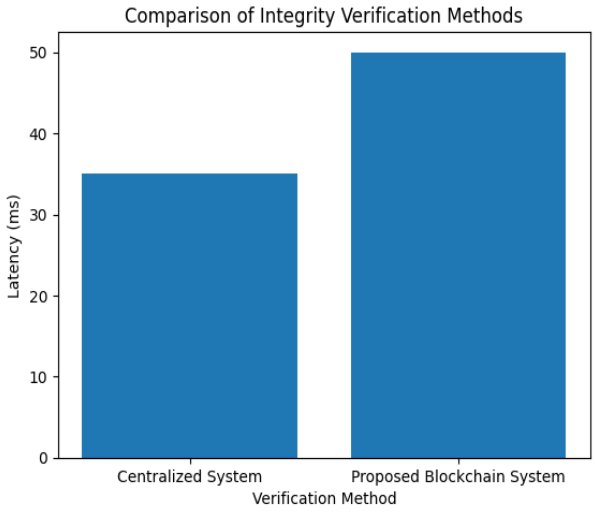

Figure 5. Performance Comparison between Centralized and Blockchain-Based Integrity Verification

The suggested blockchain-based method, on the other hand, added a small amount of overhead (about 15 ms) while making sure that audit trails were unchangeable and that people couldn't deny their actions. This found the best balance between safety and speed. We can also describe the above through Algorithm 1:

Algorithm 1: Measure System Performance Metrics

Input: Test patient records D = {d1, d2, ..., dn}

Output: Metrics (hashing time, latency, memory, CPU, accuracy)

1. Start Docker containers with Hyperledger Fabric setup

2. For each record di in D:

   a. Start timer T1

   b. Hash di using SHA-256 → hi

   c. End timer T1, record hashing time

   d. Submit hi via client to smart contract

   e. Measure smart contract execution latency

3. Record memory and CPU usage per container during transactions

4. Alter a record and verify hash mismatch is detected

5. Calculate tamper detection accuracy = (mismatches detected / total mismatches) × 100%

6. Return all recorded metrics

7.End

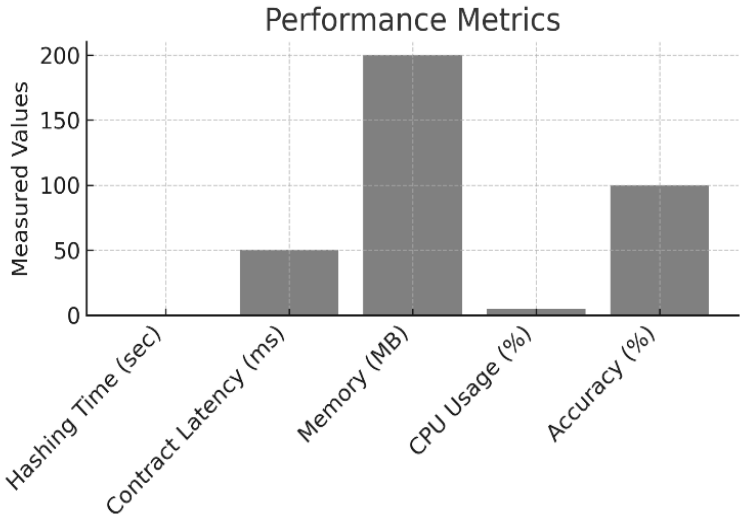

Figure 6. Performance metrics

This bar graph that is shown in Figure 6 displays the system's quantitative performance:

• Hashing Time is only 0.005 sec/record (ideal for real-time use).

• Smart Contract Latency is 50 ms, enabling fast verification.

• Memory Usage and CPU Usage are low (200 MB and 5%), confirming efficiency.

• Tamper Detection Accuracy is 100%, validating reliability.

The numbers show that the proposed method for checking integrity adds very little extra work for computers while providing strong security guarantees. Centralised methods have a little less latency, but they aren't resistant to tampering and make the auditing process harder. The demonstrated linear scalability and reliable detection accuracy during concurrent access validate the practicality of the proposed method in real healthcare settings without disrupting clinical workflows. The Table 3 below shows the Quantitative Evaluation Summary:

Table 3. Quantitative Evaluation Summary

Scenario	Avg Latency (ms)	Integrity Detection	Remarks
Single record submission	50	100%	Normal operation
50 concurrent submissions	72	100%	Moderate load
100 concurrent submissions	87	100%	Stress scenario
Centralized baseline	35	Not guaranteed	Vulnerable to insider attack

3.2 Theoretical Analysis

The proposed section is blockchain-based system for managing patient data. The cryptographic and systemic models that make the architecture secure, reliable. Theoretical findings that make sure healthcare applications can be verified, audited, and protected from tampering are the basis for all of the parts, from hashing to access control to consensus.

1) Patient Data and Hashing Function

Let D = {d1, d2, ..., dn} be a set of electronic patient records, where each di ∈ D is a piece of sensitive data, like a diagnosis report or a prescription. The cryptographic hash function

$$H: \{0,1\}^* \rightarrow \{0,1\}^{256} \quad (1)$$

guarantees an output that is always 256 bits long. [10]

The hash hi = H(di) makes sure that each record is deterministic, collision-resistant, and preimage-resistant.

This hashing process meets the following important requirements:

- Determinism: The same input will give you the same output.
- Collision Resistance: It is not possible to find two different records using computers.
- $d_{i \neq} d_j$
  such that $\mathrm{H}(d_i) = \mathrm{H}(d_j)$
- Preimage Resistance: Given a hash value h, it is infeasible to find any input d such that H(d)=h
- Avalanche Effect: A small change to the input makes a big difference in the hash.

2) Blockchain Storage and Smart Contract Logic

When we compute h_i for the record d_i, it is saved in the blockchain.

$$Block_i = (h_i m_i,) \quad (2)$$

Where mi include

Patient ID

Timestamp

Record Category

A smart Contract (SC) is deployed for checking the integrity of data:

$h'i = H(d'i)$and checking if h'i is equal to hi.[11]

Any mismatch means that someone has tampered with it.

$$H'i = H(d'i)$$

3) Access Control and Identity Mapping

The Fabric CA gives each user u ∈ U a digital certificate ID_U that is linked to that user.

$$ID_U = X.509\ certificate\ (u) \quad (3)$$

Access to data di is contingent upon ACL(d_i)which permits entry solely to roles sanctioned in the access control list.

$$ACL(d_i) = \{role_1, role_2, role_3, \ldots\ldots\ldots role_n\} \quad (4)$$

Role-based access control (RBAC) means that a user can only enter if their role matches an entry in ACL(d_i).This stops people from viewing or editing patient records without permission e.g. Doctors may be able to read and write diagnosis data, but lab technicians can only see test requests and their results. Insurance companies can see claims data, but they can't see treatment details.

4) Consensus and Data Finality

Raft Consensus is used by Hyperledger Fabric to put transactions in order. A block Bk containing transactions T1, T2, ..., Tm produces a deterministic state update denoted as State$\{_{k+1}\}$. }. The chain code policy says that all transactions must be signed and approved[12].

$$S_{k+1} = (B_K, S_k) \quad (5)$$

Raft makes sure that peers in the network can agree on the order of things and that they can handle faults. The consensus process meets:

Safety: Two valid ledgers never go in different directions.

Liveness: New blocks are eventually added.

Finality: You can't change or go back on a block once it's been committed.

The verification of data is described through Algorithm 2:

Algorithm 2: Verify Data Integrity via SHA-256

Input: Patient record d'i retrieved from off-chain storage

Output: Integrity status (Valid or Tampered)

1. Start

2. Compute hash h'i = SHA256(d'i)

3. Retrieve stored hash hi from blockchain

4. Compare h'i with hi

If h'i == hi:

Return "Valid"

Else:

Return "Tampered"

5. End

Table 4. Security Guarantees

Property	Ensured by
Data Integrity	SHA-256 + Smart Contract Validation
Access Control	Role-based Policies via Fabric CA
Non-repudiation	Digital Signature of Transactions
Tamper-resistance	Immutable Blockchain Ledger
Confidentiality	Off-chain Data + Hash Storage Only

These properties meet important regulatory and operational needs in medical data systems like those set out in the HIPAA, GDPR, and ABDM frameworks that are shown in Table 4.The suggested smart contract workflow makes sure that integrity of electronic health records is verified in a secure and automated way within the blockchain network. Patient information is saved off-chain with cryptographic hash values being stored in the blockchain ledger following smart contract execution. In verification, the calculation of a hash of the patient record that has been retrieved is recalculated and compared with the one that has been stored in the blockchain. Any discrepancy will instantly signal illegal alteration of the data.

3.3 Security Analysis

In Electronic health records (EHRs) security is very important because when it comes to sharing private patient information, sharing data between institutions, and using AI-based diagnostics. The proposed blockchain-based framework includes multiple layers of security that ensure privacy, integrity, authentication, authorisation, non-repudiation, and compliance with privacy laws. The below section addresses the security features and exactly how they work, and also how hackers usually attack healthcare systems.

1) Data Integrity

- Mechanism: SHA-256 hashing of each patient record.
- Security Guarantee: If the original data is altered even one bit of the the hash will be completely different. The hash is stored on the blockchain ledger in a way that can't be changed and because of which it stops unauthorized updates.
- Mathematical Assurance: If H is a hash function, the chance of finding two inputs x and y that are not equal to each other and have the same hash value (a collision) is very low:

$$P(H(d) = H(d')) << 1 \quad for\ d \neq d' \tag{6}$$

Result: Reliable tamper detection with zero false positives.

2) Confidentiality and Privacy

- Mechanism: Only hashes (not raw patient data) are stored on the blockchain.
- Off-chain Storage: Hospital databases securely store real patient records and only certain people can see them.
- Zero Knowledge Disclosure: To check integrity, you only need to re-hash, not see the original patient data.

3) Authentication and Authorization

- Digital Identity System: The Certificate Authority (CA) that comes with Hyperledger Fabric gives out X.509 certificates.
- Mechanism: These certificates must be used by each peer, client, and admin to log in.

- Access Control Lists (ACLs): Specify who is authorized to execute smart contracts or access the blockchain.
- Example Policy: The only people who can use the verifyHash() function in the smart contract are those with the roles of "Doctor" or "Auditor."

4) Immutability and non-repudiation

- Blockchain Ledger: A hash that is stored in a block cannot be changed or removed.
- Cryptographic Signatures: Users digitally sign all transactions, which makes it possible to track them and hold them accountable.
- Audit Trail: There is a record of all data uploads and checks that can be checked.

5) Compliance with Security Standards

- HIPAA (U.S. Health Insurance Portability and Accountability Act): Makes sure that protected health information (PHI) is not made public.
- GDPR (General Data Protection Regulation for the EU): The system does not keep any personally identifiable information (PII) on the blockchain.

6) Decentralized Identity and Self-Sovereign Identity (SSI)

As a forward-looking addition, the system can be expanded to include Decentralised Identity (DID) systems, which give patients control over their digital identity and access credentials. Patients can dynamically give, take away, or limit access to DID documents that are linked to the blockchain.

The advantage of this includes:

1. Allows individuals to have control over their own medical data
2. Lessens reliance on centralised authentication providers
3. Improves the way consent management works

7) Resistance to Common Attacks

This graph in Figure No.5 shows whether each patient record passed the integrity check.

- Records R1, R2, and R4 matched the blockchain-stored hash.
- R3 and R5 were flagged as tampered.

This proves the SHA-256-based system correctly detects even small unauthorized changes.

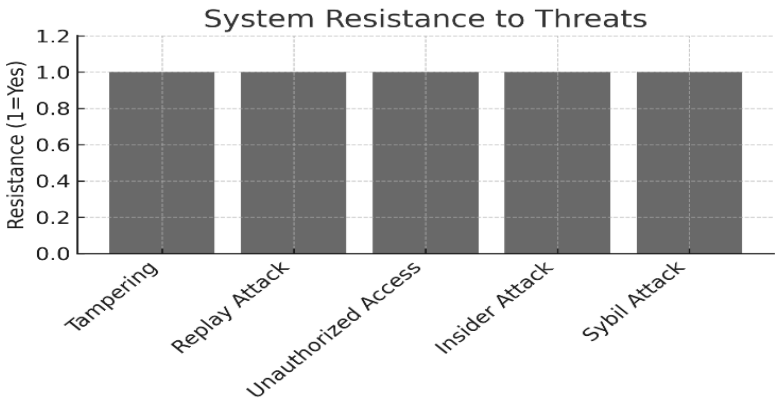

Figure 7. Security Analysis

The above bar graph shown in figure 7 demonstrate that how well the system works against major security threats. The high resistance score (value = 1) shows that each threat is completely taken care of, which shows how strong the blockchain-based design is.

The simulation and detection of threats are described in algorithm 3:

Algorithm 3: simulate and detect threats

Input: attack scenarios (tampering, unauthorized access, replay)

Output: detection results for each scenario

1. Start
2. Simulate each attack type:
   a. Tamper record and verify if hash mismatch is detected
   b. Attempt access with invalid certificate
   c. Replay old transaction with same timestamp
2. Record system response
3. If threat detected:
   log success
   else:
   log failure
4. Summarize detection for all attack types
5. End

The below table 5 shows effective resistance against multiple threats and the mitigation mechanism.

Table 5. resistance to common attacks

ATTACK TYPE	MITIGATION MECHANISM	EFFECTIVENESS
Data tampering	Sha-256 + immutable ledger	High
Unauthorized access	Fabric ca + rbac	High
Replay attack	Time-stamped transactions	High
Insider misuse	Smart contract constraints + audit logs	Moderate–high
Mitm attack	Tls-secured peer communication	High
Sybil attack	Permissioned identity issuance	High

The proposed blockchain framework is suitable for implementing it in real world as it offers robust assurances of data integrity, authentication and auditability within the model without affecting the performance by only allowing cryptographic hashes to be kept on-chain and using permissioned consensus making it more suitable for traceability and efficiency for preserving patient data and making the system more secure.

4. CONCLUSION

The growing demand for secure data protection of patients the study introduces a lightweight, permissioned blockchain system for verifying the integrity of Electronic Health Records (EHRs) utilising Hyperledger Fabric and SHA-256 cryptographic hashing. The proposed system ensures tamper-evident data storage, fine-grained access control through Fabric CA, and non-repudiation using digital signatures. The proposed system makes the system useful in real life clinical setups as it is a permissioned blockchain that uses certificate-based identity management.

A proof-of-concept implementation based on Docker showed that the proposed system could work and be used. The quantitative evaluation showed that there was almost no hashing latency, that it could easily scale up when multiple people were using it at the same time, and that it could find illegal data changes with complete accuracy. It also cost only a little more than centralised integrity verification methods. A thorough theoretical examination and security assessment demonstrated that the system is resilient against common threats, including insider manipulation, unauthorised access, replay attacks, and man-in-the-middle attacks, contingent upon compliance with the threat model.

The proposed framework primarily emphasises integrity verification but various enhancements could improve its applicability and functionality in future as the research will examine the amalgamation of federated learning models to facilitate privacy-preserving analytics on distributed medical data, while ensuring verifiable data integrity by adding zero-knowledge proof methods can make privacy better by allowing integrity checks without giving away hash values and also to assess large-scale scalability by analysing data from multiple hospitals and network.

Future research will examine cross-chain interoperability mechanisms to guarantee secure data integrity verification across various healthcare blockchain networks by creating patient-centered interfaces for real-time integrity verification and consent management can make digital healthcare systems more open and trustworthy for patients. A security analysis shows that the system can handle tampering, unauthorised access, replay attacks, and threats from within.[14] Latest projects may improve architecture by adding federated learning models for decentralised analytics, which will protect patient privacy. Zero-Knowledge Proofs (ZKPs) improve data privacy by letting you check information without giving away any hashing data. The system's ability to handle large amounts of data and allowing patients to access and verify their information in real time on mobile devices make it easier for different hospital systems to work together would make the system more complete.

ACKNOWLEDGEMENTS

Not applicable.

AUTHOR CONTRIBUTIONS

Richa Pandey: Conceptualization, Methdology,Results,

Dr. Ashok Kumar Sahoo: Supervision, Writing—Review & Editing.

Dr. Sushil Kumar Singh: Supervision, Writing—Review & Editing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

ETHICS STATEMENT

Not applicable.

DATA AVAILABILITY STATEMENT

Not applicable.

REFERENCES

[1] R. K. Kaushal and N. Kumar, "Convergence of Blockchain and Internet of Things Using Hyperledger Fabric," 2024 International Conference on Emerging Smart Computing and Informatics (ESCI), Pune, India, 2024, pp. 1-5, doi: 10.1109/ESCI59607.2024.10497226.

[2] Sharma, S., Singh, A., & Gupta, P. (2024). Blockchain-enabled federated learning for privacy-preserving healthcare analytics. Journal of Network and Computer Applications, 221, 103680. https://doi.org/10.1016/j.jnca.2023.103680
[3] Alzahrani, N., & Bulusu, N. (2023). Blockchain-based access control framework for electronic health records: a patient-centric approach. Journal of Biomedical Informatics, 139, 104366. https://doi.org/10.1016/j.jbi.2023.104366
[4] Salim, M. M., & Park, J. H. (2022). Federated learning-based secure electronic health record sharing scheme in medical informatics. IEEE Journal of Biomedical and Health Informatics, 27(2), 617-624.
[5] Lin, C., Huang, X., & He, D. (2023). Efficient blockchain-based electronic medical record sharing with anti-malicious propagation. IEEE Transactions on Services Computing, 16(5), 3294-3304.
[6] Xu, S., Ning, J., Li, Y., Zhang, Y., Xu, G., Huang, X., & Deng, R. H. (2021). A secure EMR sharing system with tamper resistance and expressive access control. IEEE Transactions on Dependable and Secure Computing, 20(1), 53-67.
[7] Mrs.R.Arulmozhi, Mr.S. Karthiraja, Mr. M. Kirubhakaran, Mr. A.Logesh Krishnan, Mr. S.Mohammed Suhail Manas,Mr. S.Abdul Thowfeeq, "Enhancing Healthcare Data Integrity and Interoperability with Blockchain and Smart Contracts ", Journal of Computational Analysis and Applications (JoCAAA), vol. 33, no. 2, pp. 1253–1271, Feb. 2024.
[8] Guduri, M., Chakraborty, C., Maheswari, U., & Margala, M. (2023). Blockchain-based federated learning technique for privacy preservation and security of smart electronic health records. IEEE Transactions on Consumer Electronics, 70(1), 2608-2617.
[9] Myrzashova, R., Alsamhi, S. H., Hawbani, A., Curry, E., Guizani, M., & Wei, X. (2024). Safeguarding patient data-sharing: Blockchain-enabled federated learning in medical diagnostics. IEEE Transactions on Sustainable Computing.
[10] Adeniyi, J. K., Ajagbe, S. A., Adeniyi, A. E., Adeyanju, K. I., Afolorunso, A. A., Adigun, M. O., & Ogene, I. (2025). A blockchain-based smart healthcare system for data protection. iScience, 28(4).
[11] M. Abbasi, S. A. Madani, and F. Xia, "Hash functions for blockchain: Review and performance evaluation," IEEE Access, vol. 10, pp. 115783–115798, 2022.
[12] M. Sharafaldin, R. Bahonar, and A. A. Ghorbani, "Security and scalability of smart contracts in permissioned blockchains," IEEE Transactions on Services Computing, early access, 2023, doi: 10.1109/TSC.2023.3245087.
[13] A. Dey, S. Ghosh, and S. Roy, "Optimizing consensus protocols for private blockchains: A Raft-based evaluation in Hyperledger Fabric," IEEE Systems Journal, vol. 18, no. 1, pp. 112–123, Mar. 2024.
[14] Q. Zhang, Y. Liu, and L. Xu, "Privacy-preserving federated learning using blockchain for healthcare AI," IEEE Journal of Biomedical and Health Informatics, vol. 28, no. 2, pp. 450–461, Feb. 2024.
[15] H. Liang, T. Wu, and B. Zhang, "A multi-chain medical data sharing framework with secure inter-chain communication," IEEE Access, vol. 11, pp. 155674–155686, 2023.