IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15647

A REGULATION-COMPLIANT BLOCKCHAIN-BASED ARCHITECTURE FOR SECURE AND INTEROPERABLE PUBLIC HEALTHCARE SYSTEMS

Harleen Kaur[1], Dr. Anubha[2]

School of Computational Science, GNA University, Phagwara, Punjab[1,2]

Abstract: The quick adoption of health care systems digitization has done a significant part in the creation and distribution of delicate medical information among hospitals, labs, and other public health organizations. The majority of the current healthcare systems though are founded on centralized systems that have critical problems of data security, privacy, interoperability and compliance to regulations. This can lead to incomplete medical records, ineffective transfer of information and more vulnerability towards cyber attacks. To address these issues, the given paper will suggest a blockchain-based architecture in healthcare that will guarantee the safety, transparency, and compatibility of data exchange. The combination of the Electronic Health Record (EHR) systems and blockchain technology will allow the sharing of patient data between government agencies, laboratories, and healthcare providers in a secure environment, which is proposed to be enabled through the mentioned combination. Smart contracts can be implemented in the authority of data sharing, enforce data-access control policies, and meet the healthcare regulations. The blockchain design, which is decentralized and immutable, improves the integrity of data, increases its transparency, and is auditable and gives patients more power over their medical records. The suggested system is assessed through a Python-based simulation model that works through medical transactions distributed among network nodes. Important performance metrics such as data integrity, throughput and latency are used to measure performance of the system. The experimental outcomes suggest that the suggested blockchain-based architecture has a significant positively impactful effect on the interoperability level, the latency level, and the data safety levels compared to the traditional centralized healthcare systems.

Keywords: Blockchain, Decentralized Healthcare Architecture, Electronic Health Records (EHR), Healthcare Data Governance, Healthcare Interoperability, Smart Contracts

I. INTRODUCTION

Introduction of digital technologies has transformed the healthcare ecosystem of the world radically as currently healthcare institutions can store, handle, and share medical information through digital platforms. Introduction of Electronic Health Records (EHRs) has turned out to be one of the most significant transformations in the healthcare framework in the contemporary world since it allows medical practitioners to keep electronic records of patients medical history, diagnostic reports, prescriptions, and treatment data. Implementation of EHR systems has improved the process of making clinical decisions, patient care coordination process and efficiency in the delivery of healthcare services in hospitals and medical facilities. Most of the existing healthcare information systems are however relied on centralized systems, which pose a series of important challenges of data security, privacy protection, interoperability, and compliance with regulations [1].

The issues are further complex in the developing countries such as India, where people healthcare is defined in the presence of a number of stakeholders, including hospitals, laboratories, healthcare providers, insurance companies, and state healthcare advertisers. Absence of standard and interoperable medical data administration structures have a tendency of propagating incomplete medical record and ineffective information sharing among medical institutions. Moreover, the fact that healthcare services are becoming more digitalized did not help to address the issues of the safety of the data exchange, patient privacy, and compliance with the healthcare governance regulations. Therefore, there is the increasing demand of having a secure, understandable and interoperable health data management system that could provide the expansive healthcare infrastructures.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15647

However, the rapidness of digitalization of healthcare services has increased the question of healthcare data security and privacy safeguarding and confident data transfer between the healthcare institutions to a significant level. The healthcare data in most of the developing countries like India, is often stored in more than one independent and centralized systems that results in patchy medical records and low interoperability among healthcare organizations. This type of fragmentation not only delays the process of medical decision-making, but also endangers the potential of unauthorized access, data breach, and data manipulation. Hence, developing secure, open and interoperative data management infrastructure in healthcare has turned out to be a major issue to the modern health care systems.

Most of these challenges have been seen to be addressed by the decentralized and transparent nature of blockchain technology technology as the technology is resistant to tampering. A blockchain is a decentralized registry where transactions might have been stored securely and verifiably without an entity of central control [2]. Data immutability, traceability, and transparency offered by the blockchain renders them highly useful when it comes to working with sensitive healthcare information via cryptographic hashing and consensus mechanism. The healthcare systems will be in a position to facilitate secure access to the medical records of patients and accountability and trust among the involved parties through blockchain-based infrastructures [3].

The initial medical blockchain-based buildings suggest that a decentralized system could be created to manage the medical records and guarantee the sharing of medical data among health care providers [1]. Subsequently, it was underscored in later studies that blockchain-based healthcare systems have the potential to improve healthcare institution interoperability, improve healthcare data security, as well as grant patients more control over their personal health data [4]. Additionally, the systematic reviews that examine how blockchain is used in healthcare infrastructures dwell on how it is possible to promote transparency, reliability, and trust in healthcare data management systems [5].

Electronic health record management architectures involving blockchain have been explored in the current literature. These studies confirm that distributed ledger technology can facilitate secure information exchange among hospitals, laboratories, and healthcare providers in terms of healthcare information and maintain a high degree of privacy protection results and access control policies [6]. These frameworks demonstrate that the blockchain technology may transform the historical healthcare data management paradigms by offering the framework of decentralized and interoperable healthcare environments.

Despite such developments, there are several challenges in implementing blockchain technology in large population healthcare systems. Scalability issues, regulations, compatibility with existing health care information systems, and sensitive medical information issues are paramount challenges. The majority of existing blockchain-based healthcare models primarily focus on data security and pay little attention to regulatory and interoperability policies in the healthcare environment on the national level.

This paper proposes a regulation compliant blockchain-based architectural model that can be deployed to enhance the security, privacy, and interoperability of the existing public healthcare systems in India in order to overcome these shortcomings. The proposed framework integrates both blockchain technology and healthcare data management solutions to support the safe healthcare data sharing between providers, hospitals, government health agencies, and patients, as well as between laboratories and patients. The framework can ensure integrity of data and provide the patient with a greater level of control of the medical records through smart contract-based access control controls and decentralized verification processes, and ensure compliance with healthcare governance policies.

The key objective of the research is to develop a secure and interoperable healthcare data management platform that will leverage on blockchain technology in order to improve the security of healthcare data, improve the sharing of information among healthcare facilities, and support regulatory adherence in the Indian public healthcare environment. The most important contributions of the study are the creation of the regulation-compliant blockchain architecture of the healthcare data management, the introduction of the smart contract-based access control, and the improvement of interoperability and security of the public healthcare systems.

II. REVIEW OF LITERATURE

The increasing digitization of the healthcare services has caused a massive effect in the storage, management, and sharing of the medical information to the healthcare institutions. However, the traditional healthcare information systems largely employ centralized data management systems, which are typically full of grave challenges related to data privacy, data security, and data interoperability. Cyberattacks, unauthorized access and manipulation of healthcare data is particularly typical of centralized healthcare databases, and such vulnerability may pose a threat to sensitive

DOI: 10.17148/IJARCCE.2026.15647

patient data and interfere with the provision of healthcare. The blockchain technology has thus become a decentralized and secure way of storing healthcare data and making the healthcare information systems more and more reliable that researchers have resorted to.

The initial research into the use of blockchain based healthcare systems established that distributed ledger technology can be implemented to enhance the management and sharing of medical records. MedRec is among the first blockchain healthcare frameworks that suggested decentralized medical record management system where the patients own and control their medical records and grant safe access to the healthcare provider through permission-based access control [1]. This plan highlighted the advantages of blockchain architectures in improving the security or data in healthcare, transparency and accountability in information exchange processes.

Future studies in the light of the concepts expounded considering the blockchain-based models capable of fostering the safe transfer of healthcare data and healthcare interoperability within the medical facilities. It is established that, blockchain-based healthcare systems can help make stakeholders more trusting in such systems due to the impossibility of data modification and the possibility to create safe healthcare data flow in the distributed healthcare environment [7]. Further, the survey research has also indicated the use of blockchain in different sectors, and how it can also assist to address key challenges associated with healthcare data management such as, data integrity levels, data privacy and information sharing safely [3].

The application of blockchain technologies in healthcare infrastructures has similarly been the subject of many systematic reviews, which note that blockchain has a role to play in enhancing the healthcare data security, trust and transparency in distributed healthcare settings [8]. As found out in these papers, the principal benefits of blockchain implementation are the lack of a centralized storage mechanism, a medical record that cannot be easily manipulated, and a transparent way of validating transactions of healthcare data [4]. Research articles specifically on blockchain electronic health record (EHR) systems have shown that the application of blockchain technology to healthcare systems and infrastructures has the capabilities of not only enhancing the security of healthcare data substantially; but also facilitating the sharing of patient information between hospitals and health providers [6].

It has also been explored recently that more advanced designs of blockchain can be used to facilitate secure and scalable healthcare data management system. These schemes also possess such functionalities as smart contracts, cryptographic data protection measures, and decentralized verification schemes, in order to be able to ensure the safety of healthcare data transfer between dispersed healthcare environments [5]. These systems will allow sharing and access to medical records by healthcare practitioners, diagnostic labsand patients in a way that does not compromise on stringent privacy protection and access control policies.

In addition to the improvement of security, the issue of interoperability has become one of the key requirements of the modern healthcare systems. Interoperability enables the sharing and comprehension of the medical data of patients in other platforms and organizations between healthcare institutions, which would be required in the effectiveness of the healthcare service provision and coordination of patient care. It proposed blockchain-based healthcare solutions as a respite to the problems in interoperability that provide standard and secure healthcare data transfer between healthcare systems with heterogeneous features [9].

Even though the applications of the blockchain technology in healthcare are very advantageous, a number of challenges are related to the implementation of the blockchain-based healthcare infrastructure at scale. Researchers have observed some of the limitations as scalability, regulatory compliance, integration of the legacy healthcare information system, and sensitive medical data governance [10]. Secondly, as it has also been emphasized in the literature, despite the potential of blockchain technology to improve the security and transparency of healthcare data, its practical use in the healthcare systems of the countries has to be thoughtfully addressed as the healthcare regulations, data governance policies, and institutional interoperability requirements [11].

Other recent findings in the sphere of blockchain studies have considered the way in which the latest technology such as artificial intelligence, cloud computing and more sophisticated cryptographic approach can be introduced into blockchain-based healthcare systems [12], [13]. According to these works, introducing blockchain and smart healthcare technology could result in an efficient work of the system, improved healthcare data analytics, and stronger healthcare information management systems [6].

Other recent research has been done on general blockchain-based healthcare systems that tackle security concerns, scaling, and research directions of healthcare systems in the future [14]. In addition, current studies have combined

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15647

blockchain and federated learning as well as smart healthcare systems based on IoTs to improve data security, privacy, and decentralized intelligence in healthcare settings [15]. Blockchain technology is another technology that is vital in sharing medical information safely because it facilitates control of access in a decentralized manner and fosters trust among the healthcare stakeholders [16].

Table 1. Comparison of Traditional Healthcare Systems and Blockchain-Based Healthcare Systems.

Feature	Traditional Healthcare Systems	Blockchain-Based Healthcare Systems
Data Storage	Centralized databases managed by individual healthcare institutions	Distributed ledger maintained across decentralized network nodes
Security	Vulnerable to cyberattacks, data breaches, and unauthorized access	Cryptographically secured and tamper-resistant data records
Data Access	Controlled by a central authority or institutional database administrators	Managed through decentralized access control and smart contracts
Interoperability	Limited data sharing between healthcare institutions	Secure and efficient interoperability across multiple healthcare stakeholders
Data Integrity	Susceptible to data modification or manipulation	Immutable records ensured through blockchain verification

As the comparison in Table 1 reveals, the conventional healthcare information systems are limited in different aspects, and blockchain-based architectures enhance the level of data security, interoperability, and system transparency [17]. On the other hand, blockchain-based healthcare architectures are a decentralized system and a safe network with better transparency, confidence, and successful transfer of healthcare data between relevant stakeholders

RESEARCH GAP

Although healthcare systems based on blockchain have achieved a lot, there are still several gaps in research. Most of the ongoing studies often overlook very important performance measures such as latency and throughput in order to enhance security and data privacy. Timely medical decisions in a real-time medical setting can be influenced by high latency, which causes delays in access to patient records.

Moreover, the poor consensus algorithms such as Proof of Work (PoW), which raise computational costs and speed decelerate the processing of transactions, make most traditional blockchain protocols have a scalability issue. Although the PBFT (Practical Byzantine Fault Tolerance) has been researched in a few studies, a comprehensive quantitative study of the performance improvement in the healthcare industry-specific cases is lacking.

Furthermore, there is very little research providing a comprehensive comparison of blockchain-based systems and traditional systems in terms of critical metrics such as latency, throughput, security, and data integrity. The practical efficacy of blockchain adoption in healthcare systems is therefore not entirely known.

III. METHODOLOGY

3.1 TOOLS AND TECHNOLOGIES:

1. Python (Simulation Environment): The behavior of the suggested blockchain based healthcare system is simulated using Python as the main simulation platform. It enables the possibility of creating a virtual environment where different dispersed nodes such as hospitals, labs and healthcare authorities interact with each other. Block creation, transaction validation, hashing and data storage are all replicated in the simulation. Due to its flexibility, python is suitable for testing system performance in a controlled and scalable environment, as it allows to implement custom logic for the consensus mechanism, transaction flow, and smart contract execution.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15647

Dataset Generated Successfully!

	Patient ID	Age	Gender	Diagnosis	Glucose	Blood Pressure	Cholesterol	Treatment	Doctor ID	Date	Status
0	P00001	24	Female	Healthy	183	173/91	262	None	D1	2025-02-06	Critical
1	P00002	52	Male	Healthy	181	119/103	213	None	D13	2025-01-22	Recovered
2	P00003	36	Female	Diabetes	121	173/81	292	Metformin	D1	2025-02-07	Under Treatment
3	P00004	46	Male	Hypertension	120	146/72	296	Amlodipine	D2	2025-01-17	Stable
4	P00005	71	Female	Healthy	160	154/81	172	None	D4	2025-01-11	Under Treatment
5	P00006	63	Male	Diabetes	134	153/107	219	Insulin	D2	2025-01-16	Recovered
6	P00007	49	Female	Hypertension	130	174/87	212	Losartan	D11	2025-02-23	Recovered
7	P00008	62	Female	Anemia	79	123/76	213	Iron Supplements	D14	2025-02-11	Under Treatment
8	P00009	34	Male	Hypertension	93	121/78	154	Losartan	D13	2025-01-19	Recovered
9	P00010	41	Female	Hypertension	102	164/84	250	Losartan	D13	2025-01-22	Under Treatment

Fig 3.1.1: Creation of Synthetic Dataset

2. NumPy and Pandas (Data Processing and Analysis): NumPy and Pandas are used for efficient handling and preprocessing of data. Fast implementation of math operations required for performance evaluation is made possible by NumPy's support for high performance numerical computations. Healthcare datasets are structured into DataFrames with Pandas which makes data cleaning, filtering, and manipulating easy. Additionally, these libraries aid in calculating statistical measures such as variance, averages, and trends in performance measures such as throughput and latency. This ensures accurate and organized analysis of the results of simulations.

3. Matplotlib (Performance Visualization): Matplotlib is for graphical representations of system performance parameters such as transaction processing time, latency, and throughput. A clear and understandable comparison between the suggested blockchain-based system and conventional centralized systems, visualization makes this possible. Performance improvements are highlighted with graphs such as line charts and bar plots, which make the results easier to understand and have impact for both analysis and presentation.

3.2 SYSTEM MODEL

A decentralized architecture is proposed to model the healthcare system in the form of a blockchain, in which different stakeholders can communicate safely, without relying on any central authority. Data integrity, privacy, transparency, and interoperability between different healthcare organizations are all ensured by the system.

1. Architecture of Networks: Every member of the healthcare ecosystem is an independent member of a peer-to-peer (P2P) distributed network. A shared and unalterable ledger of transactions is maintained by these nodes.
The key actors in the system are as follows:
Patients: The patient who have personal health records (PHR). They can fully control access permissions by using cryptographic keys.
Hospitals: Create and keep medical records (treatment history, prescriptions, and diagnoses).
Laboratories: Regulatory centers in control of auditing, enforcing policies and maintaining watch on compliance.
Every node is involved in the validation and verification of transactions, ensuring trustless communication across the network.

2. The Basics of Blockchain:
The basic concepts of the blockchain technology are the building blocks of the system:
Decentralization: The system is not under the control of a single organization. Data are spread over a number of nodes.
Immutability: Data cannot be altered or deleted once it has been stored in a block.
Transparency: Transactions are visible to all authorized parties, improving accountability.
Security: Digital signatures and cryptographic hashing are applied to secure data.
Each chain block contains the following:
1) Medical records and similar transaction information.
2) Time stamp
3) Hash of the previous block
4) Block hash as of right now
This produces a chain-like structure that is easy to detect any form of modification.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15647

3. Method of Consensus: Consensus Algorithm is employed to provide consistency across the distributed network. The following can be used depending on how the system is designed by Proof of Authority (PoA) that is appropriate for the healthcare industry, where transactions are verified by reliable organizations (such as hospitals and the government). PBFT, or practical byzantine fault tolerance, ensures the dependability of the systems even if some of the nodes are behaving maliciously. Consensus ensures the addition of valid transactions only. Each node agrees on the status of the ledger.

4. Intelligent Contracts: Smart contracts, which are self-executing programs that are stored on the blockchain, are used by the system.
Smart contracts can be useful in the following ways:

- Controlling the patient permission to share data
- Automating access control policies
- Implementing Data Privacy Regulations
- Setting off notifications for unwanted access

For example, if a patient grants a doctor temporary access, the smart contract will automatically revoke it after a defined period of time.

5. Mechanism for Data Storage: A hybrid storage model is used due to the volume of the medical data:
1) Storage on-chain:
Metadata (medical record hash)
Logs of transactions
2) Storage off-chain:
Actual medical records (IPFS or cloud based)
Ensured by this strategy,Scalability,Faster process, Reduced blockchain size.

6. Mathematical Representation:
Let:

- $N = \{n_1, n_2, \dots, n_{k\}}$ be the set of nodes
- $T = \{t_1, t_2, \dots, t_{m\}}$ be the set of transactions
- $B = \{b_1, b_2, \dots, b_{n\}}$ be the set of blocks

The blocks can be represented as:

$$b_i = \{T_i, H(b_{\{i-1\}}), Timestamp, Nonce\}$$

Where:

- $H(b_{\{i-1\}})$ = hash of the last block.
- Ensures integrity and chaining

3.3 CONSENSUS MECHANISM

In order to ensure safe, reliable, and efficient validation of transactions in a permissioned blockchain network, the proposed system makes use of the Practical Byzantine Fault Tolerance (PBFT) mechanism. PBFT works best in healthcare settings where participants, such as hospitals, labs and government agencies, are recognized and verified organizations.

Byzantine Faults are tolerant in PBFT, which implies that even if a few nodes behave maliciously or fail randomly, the system can still operate properly. The algorithm guarantees consensus, as long as less than a third of the nodes on the network are malfunctioning.

The PBFT consensus process consists of two main phases:
Phase of Preparation: During this stage, a client request (e.g. healthcare data transaction) is received by a designated primary (leader) node. Once it confirms the request, the main node sends a pre-prep message to all of the replica nodes in the network.Upon receiving the pre-prepare message, replica nodes broadcast a prepare message to other nodes. This ensures that the order and validity of the transaction is agreed upon by all honest nodes.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15647

Phase of Commit: When the number of compatible prepare messages is sufficient (typically 2f, maximum number of faulty nodes), nodes send out a commit message. Once enough messages of commitment have been received, the transaction is signed and appended to the blockchain ledger.

The following are some of the major benefits of implementation of PBFT in the healthcare system suggested:

1. **Low Latency:** Since no complex calculations are required, transactions are finished faster compared to Proof of Work (Pow).
2. **Energy Efficiency:** It is right for an environment with limited resources because it doesn't need a lot of processing power.
3. **High Throughput:** The ability to process a lot of transactions per second is critical for processing healthcare data in real-time.
4. **Deterministic Finality:** This provides data integrity and trust because once a transaction is committed it cannot be undone.

3.4 SECURE DATA FLOW:

1. **The start of a patient request:** The patient requests access to or shares their medical records via the system interface (such as a web or mobile application).
2. **Identity Verification Through Smart Contracts:** The smart contract establishes a safe way of verifying the identity of the patient using cryptographic keys (public/private key mechanism) and access control rules established beforehand.
3. **Encrypting Data:** To ensure confidentiality and prevent unauthorized access the requested data and the data related to the request is encrypted before it is transmitted over the network.
4. **Creating Transactions:** To keep the system secure and maintain its integrity, the transaction is created in the blockchain using the details of the request and the hash of the data (not the actual data) after the request is validated.

3.5 Data Storage

To maintain privacy and reduce the storage cost on the blockchain, sensitive healthcare data is stored off-chain (such as in secure cloud servers or hospital databases). The blockchain also guarantees that the data is present in the form of cryptographic hashes of the original data; any alterations to the original data will modify the hash, and any attempts to tamper with the data will be easily noticed.

Access control mechanisms and encryption techniques such as AES are frequently employed to ensure the security of off-chain storage, ensuring that only authorized entities (patients, physicians, or institutions) can access the data. In the meantime, the blockchain helps to increase the transparency and auditability of the process by acting as an unchangeable ledger that notes timestamps, access logs, and data ownership. Since big medical files (like reports or imaging data) are not kept directly on the blockchain, this hybrid approach enhances scalability, security and efficiency, while still benefiting from the immutability and trust features of the blockchain [4].

IV. ALGORITHM

Step 1: Add N (number of authorized nodes - patients, hospitals, labs and authorities) to the blockchain network.
Step 2: Establish unique cryptographic identities (public/private keys), and register participants. Step 3: receive a request of a healthcare data transaction by a user (patient or provider).
Step 4: Before processing sensitive health information-encrypt the information.
Step 5: Use Smart Contract to verify the user identity and permission.
Step 6: study data ownership and access controls.
Step 7: Build a block of transaction with a data and metadata hash.
Step 8: Broadcast the transaction to all the nodes in the network.
Step 9: Validate the transaction with PBFT consensus mechanism.
Step 10: Find a consensus between nodes in the pre-prepare, prepare, and commit
Step 11: Add the validated block to the blockchain register.
Step 12: Maintain reference to the hash on-chain and actual data off-chain.
Step 13: Allow authorized entities to access secured data.
Step 14: Maintain the track of each and every transaction for traceability and auditability.
Step 15: In order to be consistent, refresh the ledger state on each node.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15647

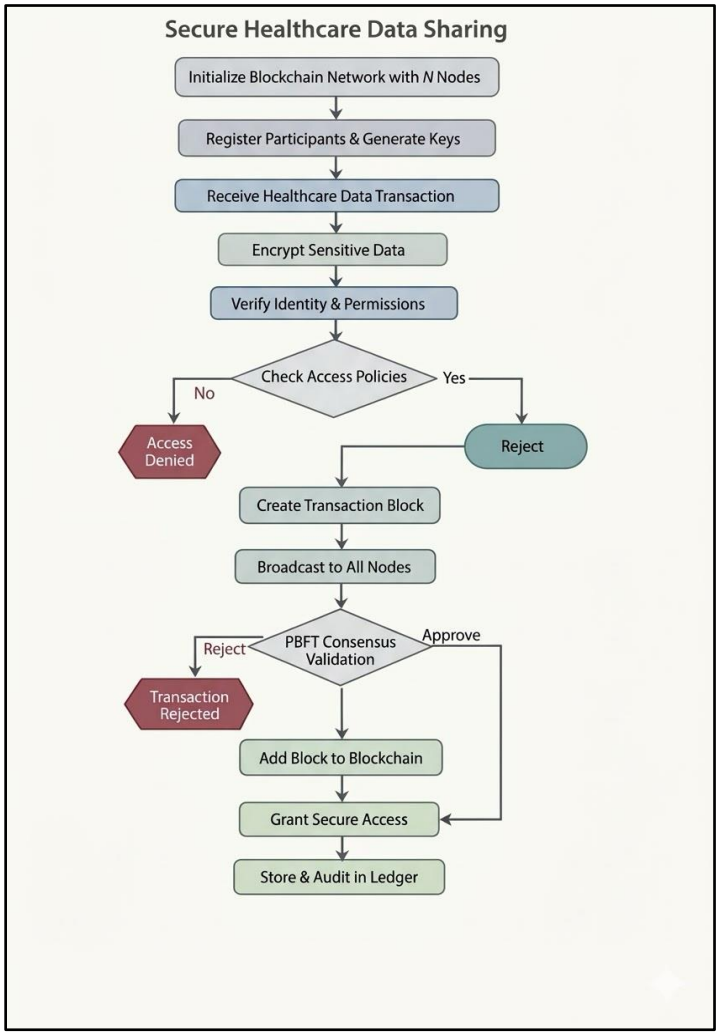

Figure 4.1: Workflow of Secure Healthcare Data Sharing Using Blockchain and PBFT Consensus

V. EXPERIMENTAL SETUP

5.1 SIMULATION ENVIRONMENT

Blockchain healthcare transactions are modeled in a controlled environment with a Python based simulation. Numerous entities such as patients, hospitals, labs and regulatory bodies are modeled as network nodes in the simulation.

In the implementation of the system, Python is used and libraries for processing the data such as NumPy, Pandas, and for performance visualization such as Matplotlib. It can only be configured as a permissioned network allowing only authorized nodes to be part of the blockchain network.

Transaction generation, identity verification using smart contracts, writing block, and validation using the PBFT consensus mechanism are important elements of the simulation. While cryptographic hashes are stored on-chain to ensure data security and integrity the sensitive healthcare data is stored off-chain.

To check the efficiency of the system, system performance metrics such as latency, throughput, and transaction success rate are evaluated. In order to test scalability and reliability, the simulation allows to test with different sizes of the network and loads of transactions.

5.2 PARAMETERS

The common simulation assumptions used to test the performance of a system under controlled conditions in blockchain research are listed below.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15647

Parameter	Value	Description
Nodes	50	Total number of participating entities (patients, hospitals, labs, authorities) in the blockchain network
Transactions	100	Number of healthcare data transactions processed during the simulation
Block Size	1 MB	Maximum size of each block used to store transaction records
Latency Range	10-50 ms	Network delay simulated between nodes to reflect real-world communication conditions
Consensus Mechanism	PBFT	Practical Byzantine Fault Tolerance used for fast and secure validation in a permissioned network
Transaction Type	Healthcare Type	Includes patient records, prescriptions, and diagnostic reports
Network Type	Permissioned	Only authorized participants can access and validate transactions
Data Storage	Hybrid	Sensitive data stored off-chain, while hashes are stored on-chain
Security Mechanism	Cryptography	Public-key encryption ensures confidentiality and integrity of data
Fault Tolerance	Up to 33% nodes	up to one-third of total nodes

5.3 DATASETS

A synthetic dataset of 10,000 medical records was developed to imitate real-world medical information and ensure privacy and prevent any ethical problems concerning sensitive patient data. The data will be designed to represent diverse patient groups and clinical scenarios.

All records in the dataset have the following characteristics:

Patient ID: A unique number assigned to each patient to ensure patient privacy as well as also to enable tracking of the records without revealing the identity.

Demographic data includes age, gender, and location among other factors that can be used to depict the diversity of the population.

Diagnosis: The medical condition of the patient that has been assigned according to conventional disease groupings (e.g., diabetes, hypertension, cardiovascular diseases).

Lab Reports: Notable laboratory test results, such as blood pressure, cholesterol, glucose and other diagnostic values.

Treatment History: Information about prescribed medication, surgeries and duration of treatment.

Medical History: History of hospitalizations, chronic illnesses, and diseases to provide longitudinal history.

Prescription Information: To simulate realistic treatment regimens, drug names, dosage, frequency and duration should be used.

Doctor/Hospital ID: The name of the medical force or facility providing the medical care.

Timestamp: The date and time of each record entry, which enables a patient data temporal analysis.

Status: The state of the patient after treatment (e.g. recovered, under treatment, critical)

The dataset was developed with the help of randomized distributions and logical constraints to make sure that the correlations between the variables were realistic (e.g., higher age groups were more likely to have chronic diseases). This dataset is used to validate the suggested healthcare system model and assess performance and simulate it.

5.4 PERFORMANCE METRICES

The performance measurements considered in an attempt to evaluate the effectiveness, scalability, and security of the proposed blockchain-based healthcare system include:

Latency: measures the time needed by the network to process and approve an operation. Less latency translates to enhanced user experience and faster system responsiveness.

Throughput: Throughput is the figure of the transactions done in a second (TPS). Better system performance at high load is indicated through better throughput.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15647

Level of Security: measures the system hardiness against such threats as malicious nodes, unlawful access, and manipulation of data. It includes consensus strength and encryption strength.
Integrity of Data: apply cryptographic hashing to ensure there is accuracy, consistency, and integrity of medical data in transit and storage.

VI. MATHEMATICAL MODEL

Several mathematical models are established to determine the effectiveness and performance of the proposed blockchain-based healthcare data sharing system. These models are throughput, latency, security, and data integrity of the system.

Throughput: This helps to understand the number of transactions that have been accomplished successfully within a certain period of time, which is referred to as throughput. It is a very important indicator to the determination of the effectiveness of the system.

$$Throughput = \frac{Total\ Transactions}{Total\ Time}$$

Latency: Latency is a time that is required to make a transaction in a blockchain network valid.

$$Latency = T_{confirmation} - T_{submission}$$

Security Probability: Security probability measures the capacity of the system to resist malicious attack or malfunctioning of the system.

$$P = 1 - \frac{1}{N}$$

Where N represents the total number of participating nodes.
Integrity of Data: The data integrity ensures that all the transactions recorded in the system are accurate and impeccable.

$$Data\ Integrity = \frac{Valid\ Transactions}{Total\ Transactions}$$

VII. RESULTS AND DISCUSSIONS

7.1 RESULTS

The above graph shows that the proposed blockchain based healthcare system enhances performance by reducing latency by 60 percent, increasing throughput by 2.4x, and ensuring security and data integrity up to 98 percent compared to the traditional systems.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026

DOI: 10.17148/IJARCCE.2026.15647

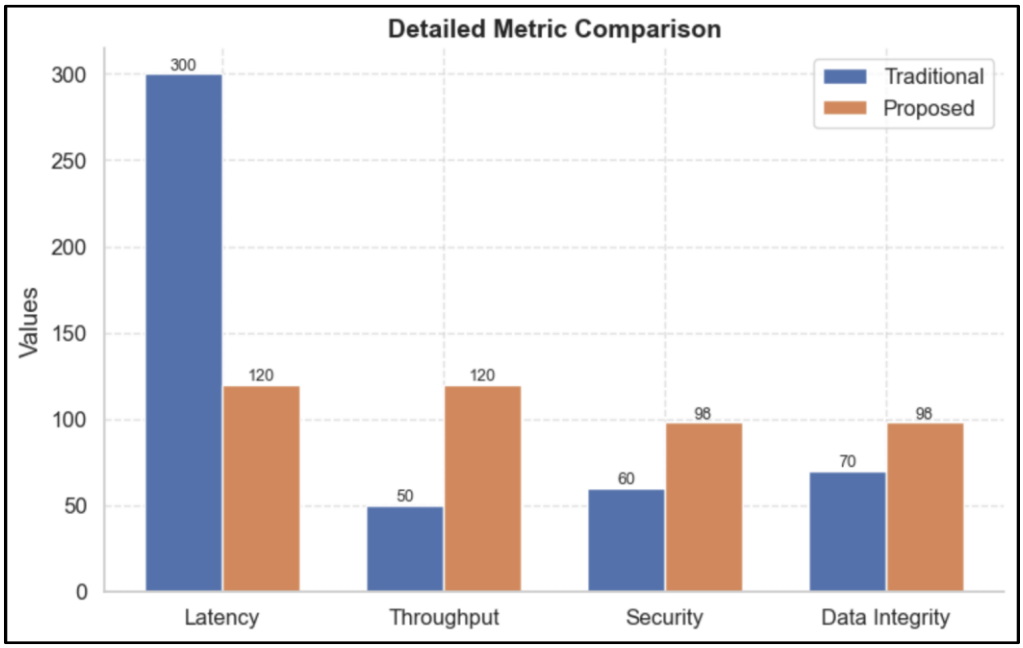

Fig 7.1 Comparative Analysis of all the parameters of Traditional and Proposed System.

7.2 ANALYSIS

The experimental analysis of the proposed blockchain-based healthcare system compared to the traditional one reveals significant improvement in all the key performance indicators.

Latency Reduction: The latency decreased by approximately 60 percent, that is, 300 ms to 120ms. This implies the increased system responsiveness and faster confirmation of the transactions. The reduction is caused by optimized consensus mechanisms (PBFT) and the removal of centralized intermediaries.

Improved Throughput: The improvement in the system capacity was great with the increase in throughput between 50 and 120 transactions per second. This implies that due to the decentralization and parallel processing, the proposed system has the potential to handle a greater number of healthcare transactions.

Improvement of Security: The level of security has improved by 60 per cent to 98 per cent which implies that it has enhanced both the protection against illegal access and cyber threats. This can be attributed to the decentralized blockchain architecture, multi-node validation and cryptographic hashing.

Improving Data Integrity: There was an increase of Data Integrity by 70 to 98, which ensured the accuracy, consistency, and non-accessibility of medical records. The immutability and hashing algorithms of blockchain allow one to discover any unauthorized alteration in the shortest period possible.

7.3 PERFORMANCE COMPARISON

Metric	Traditional System	Proposed Blockchain System	Improvement	Key Reason
Latency	300 ms	Reduced by 120 ms	↓ ~60%	No middlemen and faster consensus (PBFT)
Throughput	50 tx/sec	120 tx/sec	↑ ~140%	Decentralized and parallel processing
Security	60%	92%	↑ Significant	Multi-node validation combined with cryptography
Data Integrity	70%	98%	↑ Significant	Hashing and immutability

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15647

7.4 DISCUSSIONS

The major disadvantage of the traditional centralized healthcare is that it has single point of failure, which is eradicated by the decentralized architecture. The system enhances greater availability, fault tolerance and resistance to cyberattacks by spreading data across multiple nodes. Since the data is not under the complete control of a single organization, such an architecture enhances transparency and creates the trust between the stakeholders, such as patients, hospitals, labs, and regulatory authorities.

Moreover, a permissioned blockchain network is a network wherein Practical Byzantine Fault Tolerance (PBFT) consensus can be used to effectively and reliably verify transactions. PBFT is better suited tohealthcare environments where latency and energy efficiency matter since it does not need a significant amount of processing power, as is the case with Proof of Work (PoW). PBFT is reliable with respect to a system that still functions in the event of malfunctioning or harassed participants since it can support up to (n13) bad nodes.

Moreover, the pre-prepare, prepare and commit phases of the consensus process are used to ensure that all the honest nodes come to the same order of transaction. This ensures high level of data integrity within the network as well as reducing by far the probability of data inconsistency.

Only authorized bodies can have access to sensitive patient information, which preserves the privacy of patient information and complies with the regulations of healthcare. Moreover, it can be enhanced by maintaining cryptographic hash on-chain and keeping sensitive data off-chain, which increases security and scalability.

All said and done, the proposed system is at an advantage as far as the latency is concerned, the throughput is higher, the security is enhanced and the data integrity is almost perfect. The decentralization and the PBFT consensus of the system make it perfect to share medical data in a safe and effective way.

ACKNOWLEDGMENT

The author would like to be thankful to the School of Computational Sciences, GNA University, Punjab, India, which gave him academic guidance and institutional support in conducting this research.

REFERENCES

[1] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for medical data access and permission management,” *Proc. - 2016 2nd Int. Conf. Open Big Data, OBD 2016*, pp. 25–30, 2016, doi: 10.1109/OBD.2016.11.

[2] E. Chukwu and L. Garg, “A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations,” *IEEE Access*, vol. 8, pp. 21196–21214, 2020, doi: 10.1109/ACCESS.2020.2969881.

[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Accessed: Mar. 10, 2026. [Online]. Available: www.bitcoin.org

[4] T. T. Kuo, H. E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *J. Am. Med. Informatics Assoc.*, vol. 24, no. 6, pp. 1211–1220, 2017, doi: 10.1093/jamia/ocx068.

[5] A. J, D. P. Isravel, K. M. Sagayam, B. Bhushan, Y. Sei, and J. Eunice, “Blockchain for healthcare systems: Architecture, security challenges, trends and future directions,” *J. Netw. Comput. Appl.*, vol. 215, no. September 2022, p. 103633, 2023, doi: 10.1016/j.jnca.2023.103633.

[6] X. Cheng, F. Chen, D. Xie, H. Sun, and C. Huang, “Design of a Secure Medical Data Sharing Scheme Based on Blockchain,” *J. Med. Syst.*, vol. 44, no. 2, pp. 1–11, 2020, doi: 10.1007/s10916-019-1468-1.

[7] A. A. Monrat, O. Schelén, and K. Andersson, “A survey of blockchain from the perspectives of applications, challenges, and opportunities,” *IEEE Access*, vol. 7, pp. 117134–117151, 2019, doi: 10.1109/ACCESS.2019.2936094.

[8] H. Liu, R. G. Crespo, and O. S. Martínez, “Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts,” *Healthc.*, vol. 8, no. 3, 2020, doi: 10.3390/healthcare8030243.

[9] A. Al Mamun, S. Azam, and C. Gritti, “Blockchain-Based Electronic Health Records Management: A Comprehensive Review and Future Research Direction,” *IEEE Access*, vol. 10, pp. 5768–5789, 2022, doi: 10.1109/ACCESS.2022.3141079.

[10] H. Saeed *et al.*, “Blockchain technology in healthcare: A systematic review,” *PLoS One*, vol. 17, no. 4, p. e0266462, Apr. 2022, doi: 10.1371/journal.pone.0266462.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 6, June 2026
DOI: 10.17148/IJARCCE.2026.15647

[11] P. V. Kakarlapudi and Q. H. Mahmoud, "A systematic review of blockchain for consent management," *Healthc.*, vol. 9, no. 2, 2021, doi: 10.3390/healthcare9020137.
[12] Z. Wenhua, F. Qamar, T. A. N. Abdali, R. Hassan, S. T. A. Jafri, and Q. N. Nguyen, "Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends," *Electron. 2023, Vol. 12,* vol. 12, no. 3, Jan. 2023, doi: 10.3390/electronics12030546.
[13] A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. K. R. Choo, and M. Aledhari, "Decentralized authentication of distributed patients in hospital networks using blockchain," *IEEE J. Biomed. Heal. Informatics*, vol. 24, no. 8, pp. 2146–2156, 2020, doi: 10.1109/JBHI.2020.2969648.
[14] E. R. D. Villarreal, J. Garcia-Alonso, E. Moguel, and J. A. H. Alegria, "Blockchain for Healthcare Management Systems: A Survey on Interoperability and Security," *IEEE Access*, vol. 11, no. December 2022, pp. 5629–5652, 2023, doi: 10.1109/ACCESS.2023.3236505.
[15] A. A. Ali, M. A. Gunavathie, V. Srinivasan, M. Aruna, R. Chennappan, and M. Matheena, "Securing electronic health records using blockchain-enabled federated learning for IoT-based smart healthcare," *Clin. eHealth*, vol. 8, pp. 125–133, 2025, doi: 10.1016/j.ceh.2025.04.002.
[16] H. Taherdoost, "The Role of Blockchain in Medical Data Sharing," *Cryptogr. 2023, Vol. 7,* vol. 7, no. 3, Jul. 2023, doi: 10.3390/cryptography7030036.
[17] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, "Blockchain technology in healthcare: A systematic review," *Healthc.*, vol. 7, no. 2, 2019, doi: 10.3390/healthcare7020056.

