Check for updates

Original Research Article

Design of Patient-centric Hyperledger-based Blockchain Framework for Indian Healthcare Services

Journal of Pharmacology and Pharmacotherapeutics
17(3) 374–387, 2026
© The Author(s) 2025
Article reuse guidelines:
in.sagepub.com/journals-permissions-india
DOI: 10.1177/0976500X251336871
journals.sagepub.com/home/pha
Sage

Namdev M. Sawant[1] and Joanne Gomes[1]

Abstract

Background: The Indian healthcare system faces significant challenges, such as data fragmentation, lack of interoperability, and concerns about data security. The increasing digitization of healthcare requires a robust infrastructure to address issues like counterfeit drugs, medical data breaches, and inefficient supply chain management. Processed healthcare data play an important role in improving the quality of healthcare services and supporting effective decision-making. Advancements in the information technology (IT) sector have facilitated the management and maintenance of electronic health records (EHRs), making it essential for IT infrastructure to ensure confidentiality and access control due to the sensitive nature of healthcare data.
Objectives: Blockchain technology provides a decentralized and tamper-proof solution, ensuring secure, interoperable, and transparent management of EHR across healthcare providers. The proposed research work addresses the issues related to confidentiality and access control of EHR by proposing the Hyperledger blockchain-based healthcare framework, which connects multiple public health centers for secure data sharing.
Materials and Methods: The role-based access control mechanism helps the participants maintain data privacy in the system. Compared to existing Indian healthcare frameworks, the proposed blockchain framework supports additional features such as authentication, access control, and privacy.
Results: The framework satisfies the patient-centric need for EHR in the Indian healthcare context by guaranteeing the safe storage and private access to patient healthcare data in the blockchain environment. As the volume of data and the number of users in a blockchain network grow, latency and throughput become critical concerns that must be addressed.
Conclusion: The performance analysis of the proposed blockchain framework achieved a latency of 0.57 s and a throughput of 170 transactions per second (TPS) for 10 MB block size and 1,000 transactions, which shows outperforming results reported in previous studies.

Keywords

Healthcare, electronic health record, Hyperledger blockchain, patient-centric, role-based access

Received 05 December 2024; **revised** 20 March 2025; **accepted** 26 March 2025

Introduction

One of the largest industry sectors in the world is healthcare. Every year, more than 2,000 exabyte of related data are generated.[1] Processed healthcare data plays an important role in improving the quality and decision-making process of healthcare services. Healthcare data is categorized into three distinct types based on the entity who manages it: personal health record (PHR), electronic medical record (EMR), and electronic health record (EHR). EHR offers several advantages over PHR, including lower long-term costs, improved storage accessibility, enhanced security, better diagnostic support, easier access and exchange of data, and greater readability and accuracy due to standardized documentation.[2,3] Advancements in the information technology (IT) sector have facilitated the management and maintenance of EHRs, making it essential for IT infrastructure to ensure confidentiality, authentication, access control, non-repudiation, interoperability, transparency, accountability, and privacy due

[1]Department of Computer Engineering, St. Francis Institute of Technology, Borivali, Mumbai, Maharashtra, India

Corresponding author:
Namdev M. Sawant, Department of Computer Engineering, St. Francis Institute of Technology, Borivali, Mumbai, Maharashtra 400103, India.
E-mail: namdev.sawant@sknscoe.ac.in

Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (http://www.creativecommons.org/licenses/by-nc/4.0/) which permits non-Commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (https://us.sagepub.com/en-us/nam/open-access-at-sage).

to the sensitive nature of healthcare data.[4] Over the past decade, the healthcare industry has been suffering from exposure or impermissible disclosure of healthcare data. Figure 1 shows the number of data breaches in the United States involving more than 500 records between 2013 and 2023, based on the provided data.[5]

In India, the effective implementation of EHR is critical for improving healthcare outcomes, yet issues like data privacy, duplication, and accessibility persist. Blockchain can address these challenges by enabling secure data sharing, ensuring data integrity, and creating a unified system for managing patient health records. Figure 2 shows sample examples of data breaches in India.[6] It is challenging for healthcare organizations to secure EHR from breaches as well as criminal activity. The healthcare system implemented using either client-server or cloud-based, suffer from privacy and security flaws.[7]

Among these security challenges is the secure exchange of EHRs between patients and clinicians in mobile cloud environments. Unauthorized parties may gain harmful access to EHRs without the patients' consent, compromising data security, privacy, and integrity in cloud-based e-health systems.[8] Furthermore, traditional cloud-centric healthcare systems face several inherent issues, including significant latency, single points of failure, lack of transparency, and inadequate control over personal data. During epidemics, the healthcare industry struggles to provide essential medical treatment to a large patient population due to a shortage of medical professionals.[9]

Blockchain is a decentralized distributed ledger technology with open source, immutability, transparency, anonymity, and distributed consensus features.[10,11] It is categorized into private/consortium and public blockchain. Public blockchain allows anyone to join the network, take part in the consensus process, and read the data from a chain of blocks. Whereas, in a private blockchain, a user has to obtain permission to join the network and participate in the consensus mechanism.[12] Governance, accountability, modular architecture, smart contract (SC), performance, and scalability are the advantages of private blockchain over public blockchain. Sawant and Gomes[13] conducted an analysis of various blockchain-based EHR systems. The reviewed articles were compared based on security parameters and performance parameters. Authors Yue et al.[14] studied the applications of blockchain technology in the healthcare sector, highlighting its potential to enhance user privacy, data security, authentication, and data sharing. Fragmented patient data leads to interoperability and scalability challenges. These challenges were addressed by providing a unified view of patient data without evaluating security and privacy aspects.[15,16]

The sharing of medical data among custodians in a trustless environment is facilitated through the Ethereum platform, which includes discussions on data security and auditing mechanisms. Additionally, another solution for secure and scalable medical data sharing is presented by utilizing the InterPlanetary File System (IPFS) for off-chain storage of substantial datasets.[17] This method promotes healthcare information exchange via off-chain storage combined with on-chain verification to ensure privacy and authenticity.[18] Implementing access control within these systems can be complex. A blockchain-based service framework has been proposed in[19] for managing personal medical data,

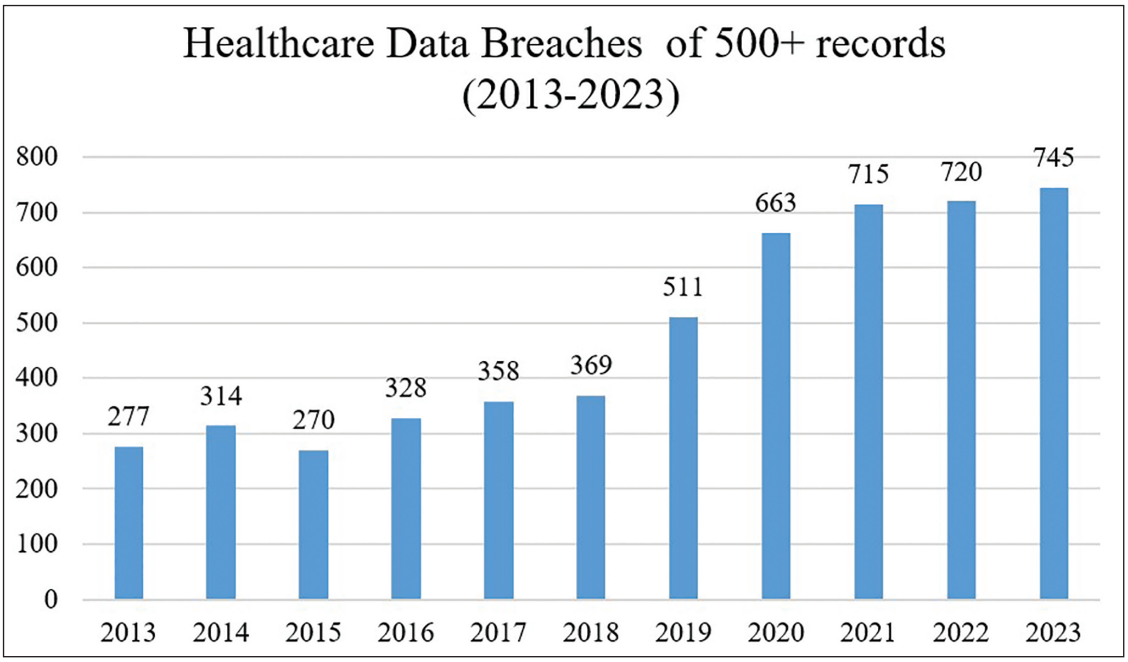


Figure 1. Frequency of Healthcare Data Breaches.[6]

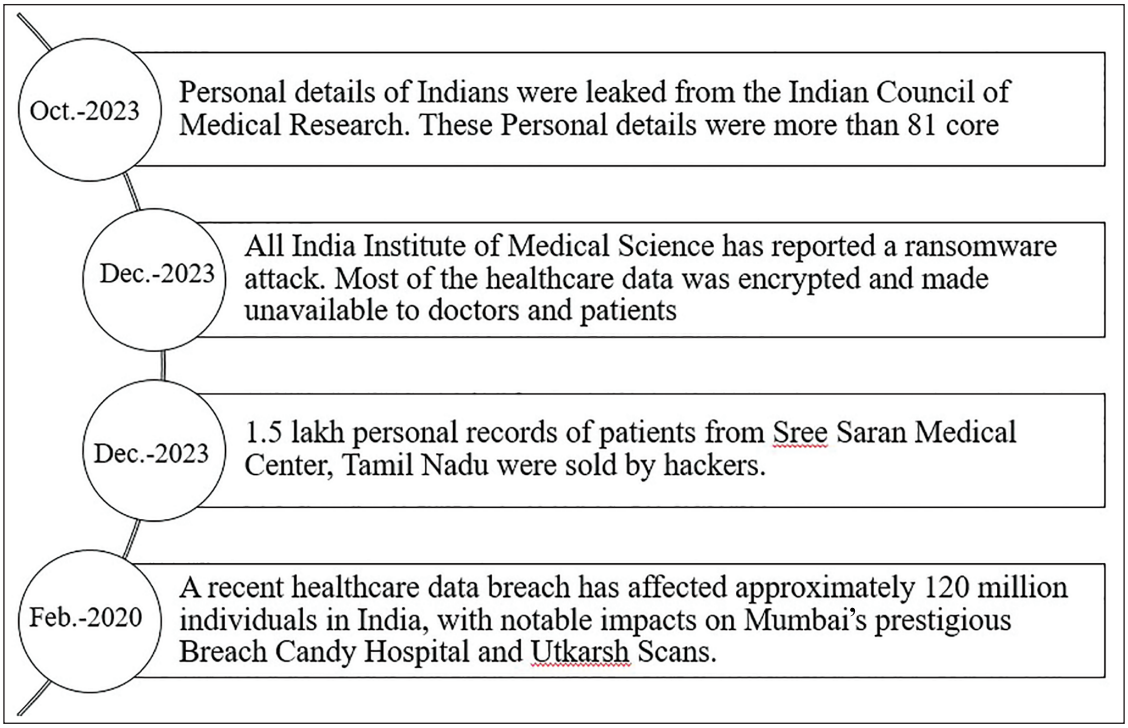


Figure 2. Notable Examples of Healthcare Data Breach.

granting patients complete control over their information; however, this proposal lacks practical implementation. To safeguard patient privacy among multiple authorities, an attribute-based signature scheme is suggested.[20] Although this approach results in a linear increase in performance costs with the number of authorities and patient attributes, it effectively mitigates collision attacks. Moreover, decentralized blockchain technology can assist in locating missing EMRs from distributed nodes. The implementation of SCs aims to automate actions concerning EMRs but may encounter limitations in emergency situations.[21] A further decentralized attribute-based signature scheme has been introduced for healthcare systems using blockchain, promoting secure data sharing, streamlined access to EHR, and ensuring non-repudiation.[22] Nonetheless, in this system, the data owner has no control overwrite operations. A Hyperledger-based blockchain solution is proposed for efficient access and retrieval of EMR data, featuring an access control protocol designed to obscure signature information.[23] This system may experience performance degradation as the volume of data ordering increases.

The work introduced a new blockchain-based architecture for an access model, coupled with an authorization scheme that empowers users with granular control of the system.[24,25] All users share a common encryption key, which could potentially lead to non-repudiation issues. Furthermore, smart mobile devices can facilitate remote management of blockchain-based systems for personal health data sharing and collaboration, creating a user-centric application for data sharing among various healthcare professionals.[26] The author designed the EHR sharing framework for a mobile cloud environment.[27] The prototype model was implemented through the Ethereum blockchain to address security and privacy challenges. Another consortium blockchain-based EHR sharing platform proposed to avoid a centralized cloud platform for data sharing.[28] The scheme focuses on conditional proxy re-encryption and searchable encryption for data security, privacy, and access control. A decentralized blockchain-based patient-centric scheme for healthcare data management was introduced, which addresses the challenges faced by traditional EHR systems such as security, data loss, and inefficient clinical data retrieval.[29] Cross blockchain-based platform proposed to achieve data privacy while sharing data between multiple blockchain-based platforms.[30]

The Indian healthcare system has been studied to some extent in the literature. A detailed study of the Indian healthcare system, along with various frameworks, is presented.[31,32] India, comprising 28 states and 8 union territories, operates a multi-layered healthcare system with both public and private hospitals. The Ministry of Health and Family Welfare (MoHFW) manages national health programs for communicable and non-communicable diseases, along with healthcare facilities and medical education. The public system is structured by population, starting with sub-centers (SCs) for communities of 5,000 (3,000 in hilly areas), followed by primary health centers (PHCs) for 20,000–30,000 people, and community health centers (CHC) for 80,000–120,000. District hospitals serve as final referral centers to ensure quality

care.[33,34] In India, the lack of mandatory standardization complicates achieving interoperability in the healthcare system. An application programming interface (API) enabled system can facilitate smooth data exchange among stakeholders, with PHR querying all nodes for updates and stored on the source node to prevent single points of failure. The Systematized Nomenclature of Medical-Clinical Terms (SNOMED-CT) and Health Level 7 (HL-7) standards are adopted for nomenclature standardization and data exchange, respectively.[35,36] The adoption of blockchain technology in India's healthcare ecosystem is minimal, yet it has significant potential for enhancing health information exchange.[37] Effective collaboration among healthcare stakeholders is crucial for ensuring a reliable digital future for patients and optimizing the hospitalization process, which includes modules for data management, cloud storage, access permissions, and security layers.[38,39] The author proposed an EHR framework utilizing standardized medical terminology and coding. The system comprises various components, including Administrative, Nursing, Laboratory, Radiology, Clinical Documentation, and Pharmacy functions, with basic operations for reading and writing data. Data entered via a web application are converted to a standard format and stored in collections, while the STRIDE and DREAD models are employed to identify threats and assess associated risks.[40]

In this research work, the Hyperledger blockchain-based healthcare framework has been proposed for Indian healthcare, which connects multiple public health centers, where a role-based access control mechanism is used to help the participant maintain data privacy in the system. After a comprehensive study of the existing healthcare systems and frameworks in India, the research gaps and challenges in the said area were identified. The key contributions of this work are (a) the design of a Hyperledger-based framework tailored for the Indian healthcare system to enhance data security, privacy, and interoperability with a patient-centric approach; (b) the development and software implementation of SC and a user-friendly graphical user interface for both doctors and patients, facilitating seamless interactions; and (c) the performance evaluation of the proposed blockchain framework using the reliable-replicated and fault-tolerant (RAFT) consensus algorithm, demonstrating its effectiveness and efficiency in the healthcare context.

It was observed that as the volume of data and the number of users in a blockchain network grow, latency and throughput become critical concerns that must be addressed. The performance analysis of the proposed blockchain framework was carried out with varying numbers of blocks and varying numbers of transactions per block to estimate latency and throughput. With a block size of 100 transactions per block and with a total of 10 blocks, a latency of 0.57 s and a throughput of 170 transactions per second (TPS) was achieved, outperforming the results reported in previous studies.

The rest of the research article is enumerated: Section two discusses the related work. Section third presents the proposed Hyperledger blockchain framework along with a working use case diagram. Section four shows the software implementation of the proposed framework. Section five reveals the performance evaluation of the said framework, and Section six summarizes the article.

Related Work

The healthcare information exchange system leverages Hyperledger Fabric (HLF) to enhance data security and interoperability, addressing critical challenges in current healthcare systems. Building on prior work with Ethereum, this system uses HLF's permissioned access, private channels, and encryption to improve security beyond traditional databases.[41] The architecture tackles interoperability issues, offering a unified platform for seamless data exchange and overcoming information silos. The research provides a foundational framework for stakeholders considering blockchain integration, outlining a scalable, flexible approach that aligns blockchain's theoretical potential with practical healthcare needs, thus contributing valuable insights for future implementations. One of the articles investigated the use of HLF for managing EHR at Frere Hospital in South Africa's Eastern Cape, focusing on how blockchain can improve security, transparency, and interoperability in healthcare systems.[42] By employing a mixed-methods approach, the study captures practical insights into current record management challenges and evaluates blockchain's potential to transform healthcare practices. The results highlight blockchain's ability to foster trust, enhance efficiency, and strengthen data security in healthcare, offering meaningful implications for institutions seeking advanced solutions to persistent EHR management issues. Another research article introduces a HLF-based blockchain solution designed to strengthen the privacy and security of EHRs within eHealth systems.[43] Utilizing SCs and blockchain technology, the study implements advanced access control mechanisms that ensure secure client identification, authentication, and authorization. The proposed architecture, along with chain code (CC) implementation, offers an efficient EHR management framework. HLF's consensus mechanism enhances scalability while maintaining patient anonymity. Performance evaluations through experimental and computational tests highlight the system's capability to protect EHRs from data breaches, demonstrating blockchain's effectiveness in healthcare data security.

Ndzimakhwe et al. explore the application of HLF in the healthcare sector, focusing on tailored solutions to support the adoption of EMRs.[44] With a user-centric approach, the study evaluates blockchain methods that enhance simplicity and practicality for healthcare use. Results suggest that HLF, as an open-source platform, provides a flexible framework for secure EMR storage via a customizable test network. The study also identifies implementation challenges, emphasizing HLF's capability to offer a secure, distributed environment.

By leveraging grants and revoking access controls, HLF empowers patients to manage their medical information and enables authorized doctors to view records, facilitated through CC. Another research proposes an HLF-based solution using SCs to establish transparent trust, ensure general data protection regulation (GDPR) compliance by storing only hash values, and enable secure patient authentication with cryptographic techniques.[45] The solution's usability is demonstrated through a user interface and live deployment. The research article examines the integration of blockchain and machine learning (ML) to enhance the healthcare insurance sector in developing countries, addressing issues like fraudulent claims and data mismanagement.[46] The proposed model utilizes a private blockchain for secure transaction processing and payment settlements, while ML techniques, such as support vector machines and random forest regression, differentiate between fraudulent and legitimate medical records. This integrated framework aims to create a patient-centric environment with improved data transparency, ultimately offering a more secure and efficient ecosystem than traditional methods. Khatri et al. introduced a blockchain-based framework to improve healthcare management during the COVID-19 pandemic by addressing existing system shortcomings.[47] The solution offers virtual assistance from medical professionals and enhances the accuracy of patient data, aiding government decision-making. Utilizing JavaScript-based SCs within an HLF prototype strengthens EHR management while ensuring patient privacy and security. Benchmarking with the Hyperledger Caliper tool confirms the architecture's effectiveness in advancing healthcare administration and fostering patient-centered care. HLF addresses the healthcare requirements of high-level security and enterprise-level trust requirements, providing a robust environment for managing patient medical records. The study leverages HLF and SCs to design a system that overcomes these limitations, enhancing patient interaction and data management.[48] Díaz introduces HLF, a modular and extensible platform for permissioned blockchains across diverse industries.[49] Unlike other blockchain systems, it incorporates flexible membership models compatible with industry-standard identity management, addressing issues such as non-determinism and performance vulnerabilities. Benchmarking results demonstrate Fabric's scalability and efficiency, achieving over 3,500 TPS with sub-second latency.

Hyperledger Blockchain Fundamentals

Hyperledger is an open-source blockchain platform that provides a modular framework designed to support the development of private, permissioned blockchain solutions tailored to enterprise needs. HLF is one of the Hyperledger projects, that is a highly flexible and secure distributed ledger framework. It is designed for use in environments requiring controlled access and scalability. It supports pluggable consensus protocols, enabling organizations to customize the network's trust model according to their specific use cases. Peer nodes, Orderer, Ledger, SCs, also called CCs, membership service provider (MSP), certificate authority (CA), channels, client application, and endorsement policies are components of the HLF framework. These components of HLF are shown in Figure 3.[49] Peer, Orderer, and Client are the three different nodes in HLF. The nodes communicating with the blockchain ledger and approving transactions by executing CC are known as peers. Peer nodes come in distinct varieties: Endorser Committer and Anchor. Endorsing Peers execute SCs and propose transactions; Committing Peers validate and commit transactions to the ledger; and Anchor Peers enable communication between organizations in the network. It is necessary to set up these peers with the required cryptographic components, such as certificates. The Orderer node, providing an ordering service, is responsible for transaction ordering and maintaining consensus across the network, where consensus is the process by which blockchain network participants agree on the validity and order of transactions to maintain a single, consistent ledger. The ledger in blockchain serves as a tamper-proof record of all transactions, ensuring transparency, accountability, and trust within the network. SC defines and executes business logic on the blockchain, running on peer nodes to process and validate transactions, whereas MSP manages identities and access control in the network using digital certificates, ensuring only authenticated participants can interact with the blockchain.

The endorsing peer receives invocation requests from a client application, it then validates the transaction by utilizing a valid certificate from CA and, if successful, simulates CC. The client gathers the feedback received from endorsing peers and resends it to the ordering service. The ordering service decides the order of each transaction by executing a consensus algorithm to maintain the consistency of transactions in the network. The ordering service distributes newly produced blocks to peers as soon as a transaction is made on the network. The ledger is then updated and validated by peers that receive these blocks. Because there is no requirement for a centralized effort to grow the infrastructure or the network, this architectural solution is naturally very scalable. Participants have access to several Hyperledger Blockchain networks. Each network has discrete transactions, which are made possible by a structure known as a channel. Peers establish connections with channels that are capable of receiving all transactions, broadcast on those channels. The business logic of the application written in CC is a self-executing program. To write governance rules for any type of business application SCs play an important role. The ordering service is a collection of multiple nodes. These nodes communicate with each other to reach a consensus on an order of transactions. It gives the benefit in terms of immutability, integrity, and scalability of transactions. Practical Byzantine Fault Tolerance, Solo, and Kafka RAFT are some of the HLF blockchain algorithms.

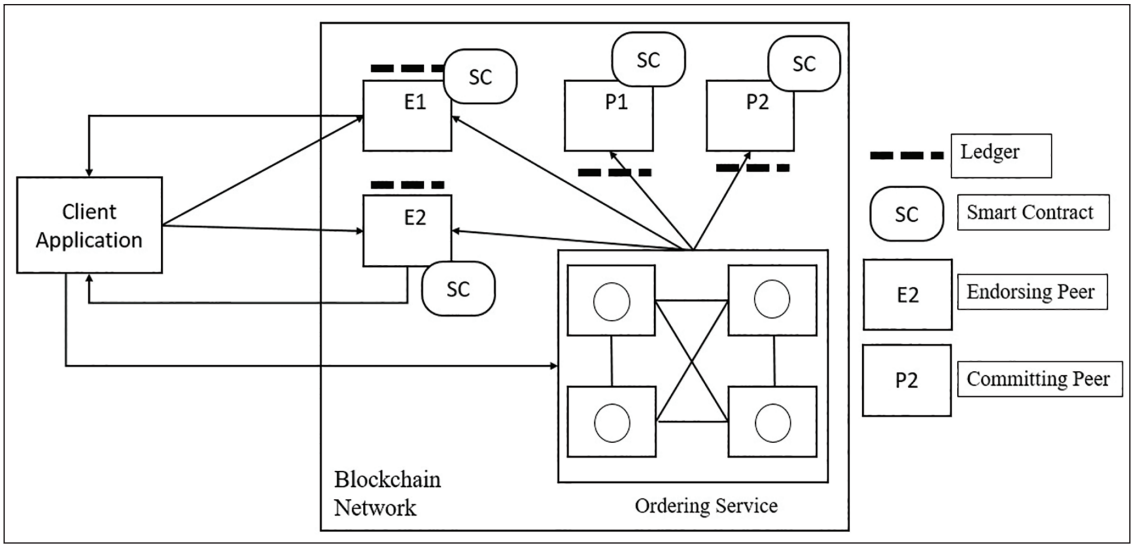


Figure 3. Hyperledger Framework Components.

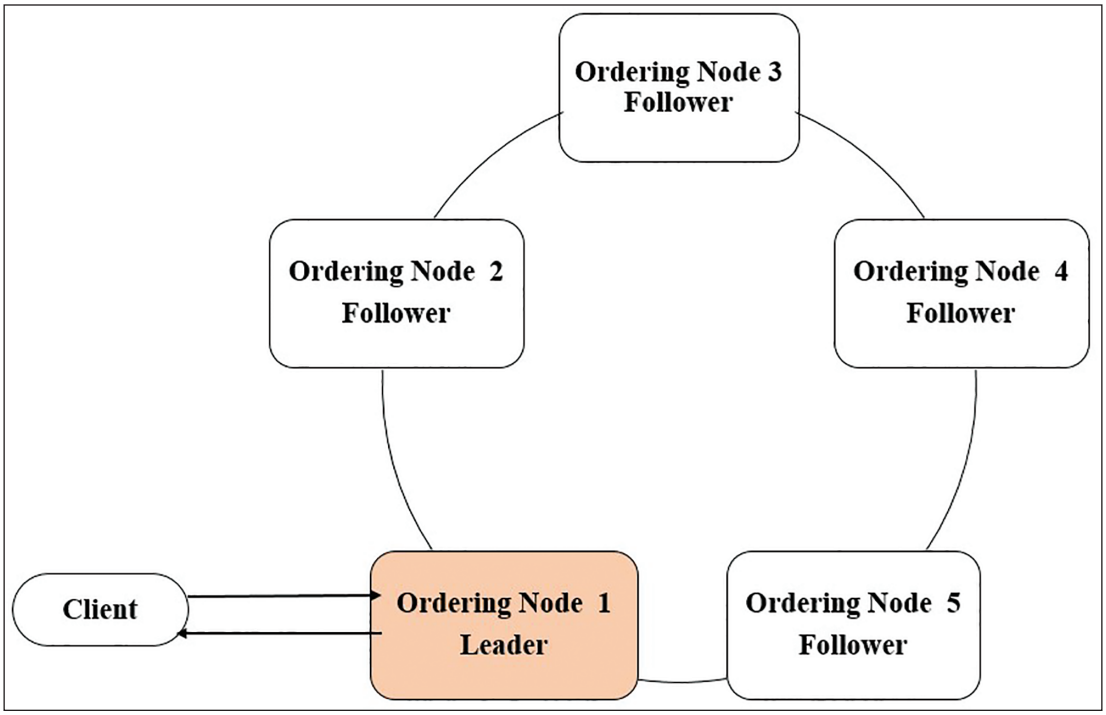


Figure 4. Working Model of Reliable-replicated and Fault-tolerant (RAFT) Consensus.

RAFT is used as the default consensus mechanism in HLF because it is a crash-tolerant, leader-based protocol that offers simplicity, high performance, and scalability, making it well-suited for enterprise blockchain applications.

In this research work, the proposed Hyperledger blockchain-based framework uses the RAFT consensus algorithm. RAFT is a distributed consensus algorithm that follows the leader and follower model, as shown in Figure 4. It is used to ensure consistency of transaction ordering across the nodes. A leader is responsible for transaction proposal and block creation. Once the transaction is received from a client, the leader creates a block and broadcasts the block to the follower. The majority of followers conform to the block; then it is committed. For N nodes algorithm can tolerate (N-1)/2 failures in the system. Fault tolerance, reliability, and scalability are the advantage over Solo and Kafka.[50]

Methodology

Hyperledger blockchain is suitable for healthcare systems to maintain EHR and enable secure data sharing because it offers a permissioned network with strict access controls, ensuring that only authorized parties can access sensitive patient data. Its immutable ledger guarantees data integrity, while its support for privacy through channels and private data collections allows selective sharing of information among stakeholders like doctors, hospitals, and insurers. Additionally, the scalability and interoperability of Hyperledger enable seamless integration with existing healthcare systems, promoting efficient and trustworthy data exchange.

Figure 5 illustrates the architecture of the proposed framework built on the Hyperledger blockchain, designed to address the challenges and limitations of current healthcare systems. As explained in the literature survey, PHCs are an integral part of the Indian healthcare system. In this framework, multiple PHCs relate to each other through the blockchain network for patient data sharing. Role-based access control mechanism has been implemented in this framework, which helps the participants such as doctors, patients, insurers, and others, to maintain privacy during healthcare data exchange in the system. The proposed framework is implemented through a permissioned blockchain called HLF due to its inherent features that support business applications.

In the proposed blockchain network, initially, healthcare providers go through off-chain identity verification by a trusted third party (TTP). In the Indian context, this TTP could be the municipal health department, state medical council, or MoHFW. TTP gives the credentials to use the blockchain network. In the proposed implementation, a network administrator (NA) has been assigned as the TTP. Roles and permissions are given by the NA to healthcare providers. Patients register in the system through a registration form provided by the NA. NA can add and remove doctors and patients. The registered patient visits any registered doctor for treatment. A patient-centric system is implemented through a consent-based mechanism in which the doctor takes permission from the patient to see the previous patient's history. Patients achieve privacy through the grant and revoke functionality implemented in the patient's login.

The proposed system is implemented, assuming two participants, a doctor and a patient. Figure 6 shows a sequence diagram of patient and doctor interaction with the system. The doctor asks for consent for the EHR from the patient to see the patient's previous history, if any. If the request is not granted, the doctor cannot see the patient's EHR. On acceptance request, the doctor sees the previous history and depending on the treatment if required, creates an EHR. This is referred to as the transaction proposal and is submitted to the endorsing peer. The endorsing peer digitally signs the proposal and resends it to the doctor. The doctor sends it to the ordering service to order the transaction. This transaction proposal is then ordered sequentially in a block by ordering service. Finally, this block containing ordered transaction proposals is sent to the committing peers where it will be stored in the form of a block.

Implementation of the Proposed Framework

The proposed blockchain system is implemented using libraries provided by HLF with version 2.2.

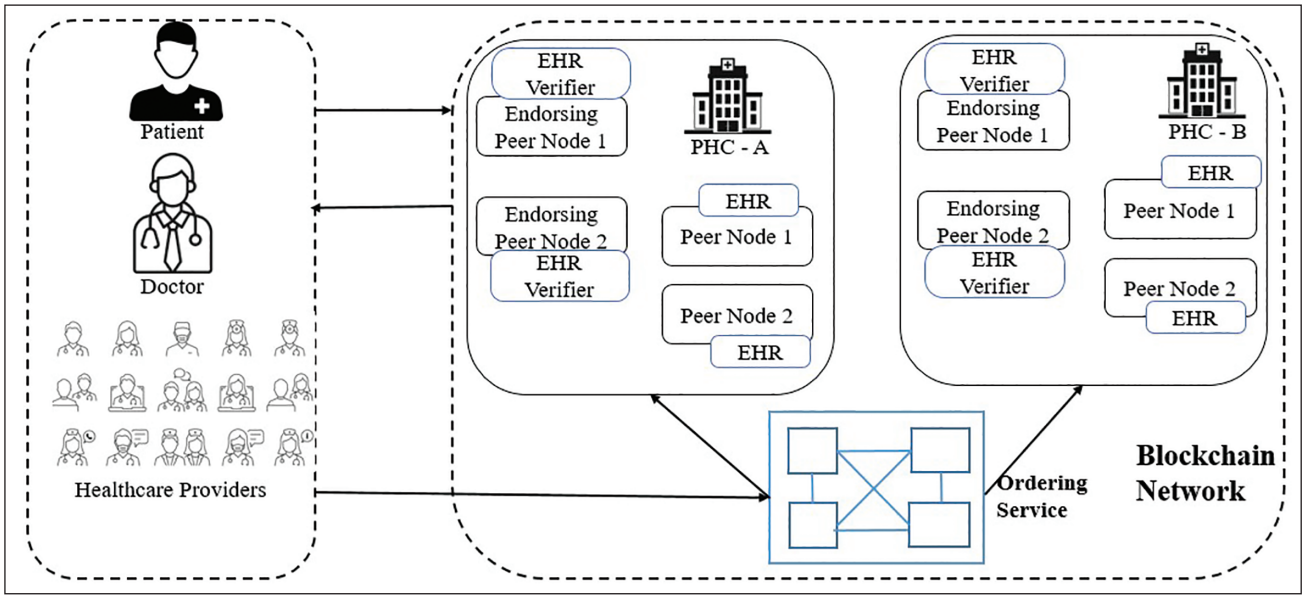


Figure 5. The Proposed Architecture of Hyperledger Fabric Framework.

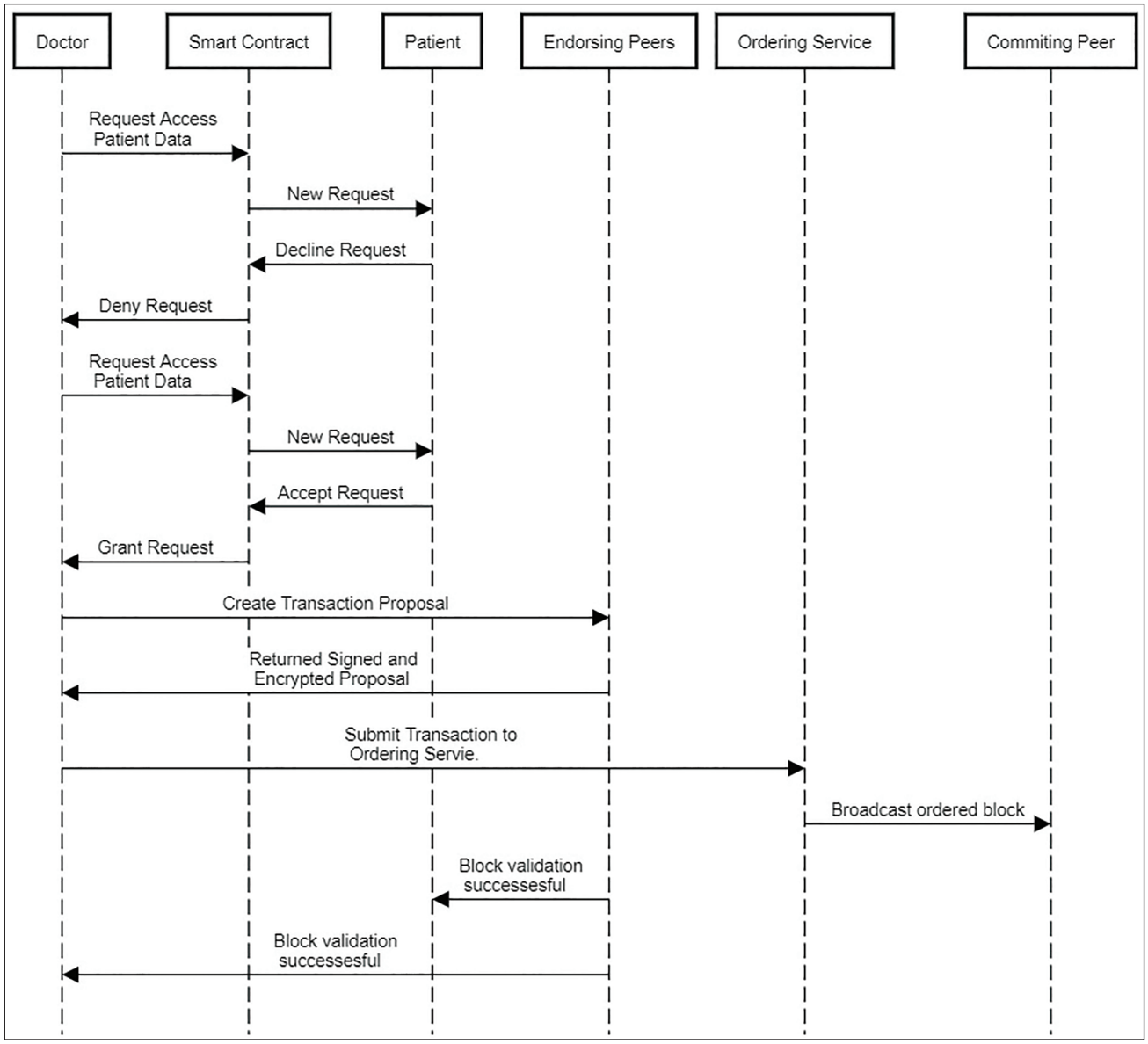


Figure 6. Sequence Diagram for the Proposed Method.

In the first step, the network participants have been defined and configured, including the details about the hospitals and their respective peer groups. Next, the CC is applied to the selected peers to activate the SC. Establishing the channel requires determining the ordering service for consensus, approving peers, and setting policies. Finally, the configuration is completed to establish a robust HLF network with operational channels, peers, hospitals, and deployed CC. All components are properly synchronized and communicate seamlessly with one another for optimal functionality.

The system users are assigned roles based on their organizational responsibilities. Once users authenticate themselves, the system grants access privileges according to their assigned roles. This approach enhances security by restricting access to specific blockchain network components to authorized users only. It provides a tailored and secure experience while complying with the standards of distributed ledger technology for enterprise-grade applications.

In the creation and updating of the stakeholders stage, if the patient has already seen a doctor, the primary care provider sends a transaction proposal to obtain any prior patient metadata from the hospital ledger. If the patient's information is found in the ledger, it is sent back to the doctor; if not, the physician will evaluate the patient and send the revised data to the ledger, treating them as a new patient.

When a patient sees their primary care physician, the doctor suggests medication, their records are updated and added to the ledger, and the patient and other fabric network stakeholders will get the same information.

The ledger contains the hash values of certain of the transactions that will be stored in the decentralized storage and need additional space. It is essential to emphasize that certain transactions, like patient registration details, will be kept in a provisional database until the transactions are finished, and patients will no longer require consultation with the doctor until the same circumstance happens again. Patients have the option to accept or reject an access request from an investigator seeking their medical records for research purposes. The patient or the relevant health authority has the authority to approve or disapprove of access to EHRs. This helps to achieve the privacy of patient healthcare data.

Health data is stored here in encrypted form within the ledger, utilizing a decentralized, role-based access system. With the inherent capabilities, the proposed framework promotes interoperability among healthcare systems by utilizing permissioned networks and standardized SC. Its consensus and role-based access control methods guard against unwanted changes, and its immutability feature limits access to categories of health data. The framework additionally protects sensitive health data by utilizing privacy-preserving strategies, including private channels and private transactions. Scalability is facilitated by its endorsement policies and modular design, which enable integration of outside-of-the-chain storage options for massive datasets and horizontal scaling. By giving participants defined responsibilities, the HLF improves healthcare efficiency by minimizing pointless data searches and transactions. By automating data access and validation procedures, SC lowers the need for human involvement and increases the system's performance. Because it is decentralized and data storage is less redundant, it improves data updates and retrieval. Strong security features built into the framework, such as cryptographic methods, guarantee data confidentiality and integrity.

Results

This section presents the performance analysis of the proposed blockchain framework. The performance of the said system is evaluated using the RAFT consensus algorithm. The assessment of the performance indicators is monitored and reviewed. The instrument is used to analyze the system performance parameters such as throughput, latency, and central processing unit (CPU) utilization.

Latency and throughput are crucial factors in the performance of a proposed blockchain network for the Indian healthcare system. Latency refers to the time it takes for a transaction to be processed and confirmed within the given network. In healthcare, low latency is essential for real-time access to patient data, enabling quick decision-making by medical professionals. Throughput, on the other hand, measures the number of transactions the blockchain can handle within a given time frame. High throughput is crucial for ensuring that the proposed healthcare system can scale effectively as the volume of transactions (e.g., patient records, prescriptions, and test results) increases. Together, low latency and high throughput ensure that the proposed blockchain network remains efficient, responsive, and capable of supporting the growing data demands of the Indian healthcare sector while maintaining the security and integrity of sensitive health information.

The latency and throughput are defined as given as below

$$\mathrm{TL} = \left(\mathrm{CT} \times \mathrm{NT}\right) - \mathrm{ST} \tag{1}$$

$$\mathrm{TT} = \frac{\mathrm{TCT}}{\mathrm{TTS}} - \left(\mathrm{NCN}\right) \tag{2}$$

where TL denotes transaction latency, CT denotes confirmation time, NT denotes the network time, ST denotes the start time, TT denotes the transaction throughput, TCT denotes total cycle time, and TTS denotes the transaction turnaround time.

The performance of the proposed framework was evaluated by varying the block size and the number of transactions per block. Tables 1 and 2 demonstrate the impact of transactions per block and the number of blocks on throughput.

Figures 7 and 8 show that increasing the block size and the number of transactions per block improves both latency and throughput up to a certain point; exceeding the block size may decrease performance. Figure 9 shows that the execution of the number of TPS increases by keeping the maximum block size per block constant. That is, variable block size affects the system performance. Looking at the underlined hardware capability and keeping the block size constant will give the best performance.

Tables 1 and 2 provide analysis of system performance parameters; they focus on the impact of block size on throughput and latency. Table 1 shows results for varying numbers of transactions per block and block size. The number of blocks to be simulated kept constant. It is observed that the optimal performance in terms of both throughput and latency is achieved at a block size of 50–60 MB. This suggests that increasing the block size improves system efficiency up to a certain point, after which performance begins to degrade slightly. Table 3 shows simulated results by keeping the maximum transactions per block and block size constant. It is observed that as the number of blocks increases, the throughput increases and latency decreases consistently. For 800 blocks, the system gives a throughput of 41,237 TPS.

Discussion

The proposed framework has been compared with existing blockchain frameworks presented in the literature. Table 3 shows a comparison of the proposed framework with existing state-of-the-art frameworks presented in the literature. Performance parameters such as CPU utilization, throughput,

Table 1. Effect of Transaction Per Block on Throughput.

Number of Nodes	Maximum Transaction Per Block	Block Size (MB)	Total Blocks to Simulate	Latency (Second)	Throughput (Tx per Second)
5	10	10	10	0.00032	869
5	20	20	10	0.00021	1,550
5	30	30	10	0.00017	2,173
5	40	40	10	0.00015	2,580
5	50	50	10	0.00014	3,012
5	60	60	10	0.00014	3,092
5	100	100	10	0.00018	2,906

Table 2. Effect of Number of Blocks Over Throughput.

Number of Nodes	Maximum Transaction Per Block	Block Size (MB)	Total Blocks to Simulate	Latency (Second)	Throughput (Tx per Second)
5	100	100	20	0.00010	869
5	100	100	30	0.00010	1,550
5	100	100	40	0.00009	2,173
5	100	100	50	0.00008	2,580
5	100	100	100	0.00005	3,012
5	100	100	200	0.00003	3,092
5	100	100	400	0.00002	2,906
5	100	100	800	0.00002	41,237

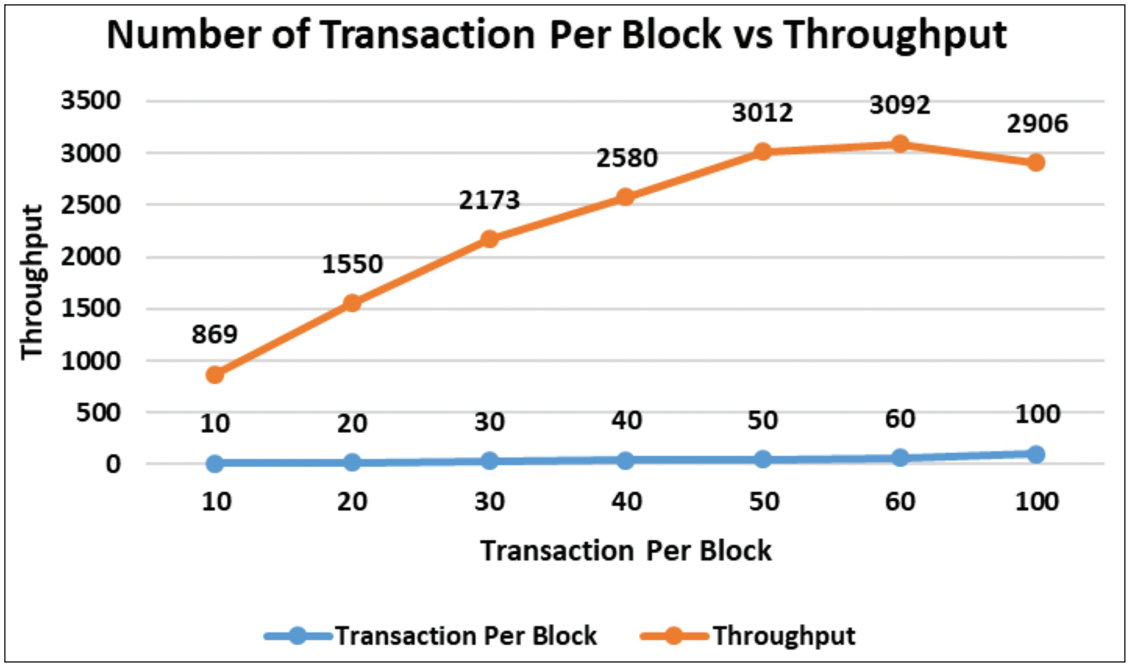


Figure 7. Impact of Transactions/Block on Throughput.

and latency were calculated by considering a block size of 10 and 20 MB with a total of 2,000 transactions.[45] The transaction sending rate is 200 TPS. Similarly, the experiment was carried out considering 1,000 transactions with a sending rate of 200 TPS.[47] They used the concept of single channel and dual channel. Dual channel can be used to connect one organization to another organization. The outcome shown in Table 4 is for a single channel. The size of the block and organization count

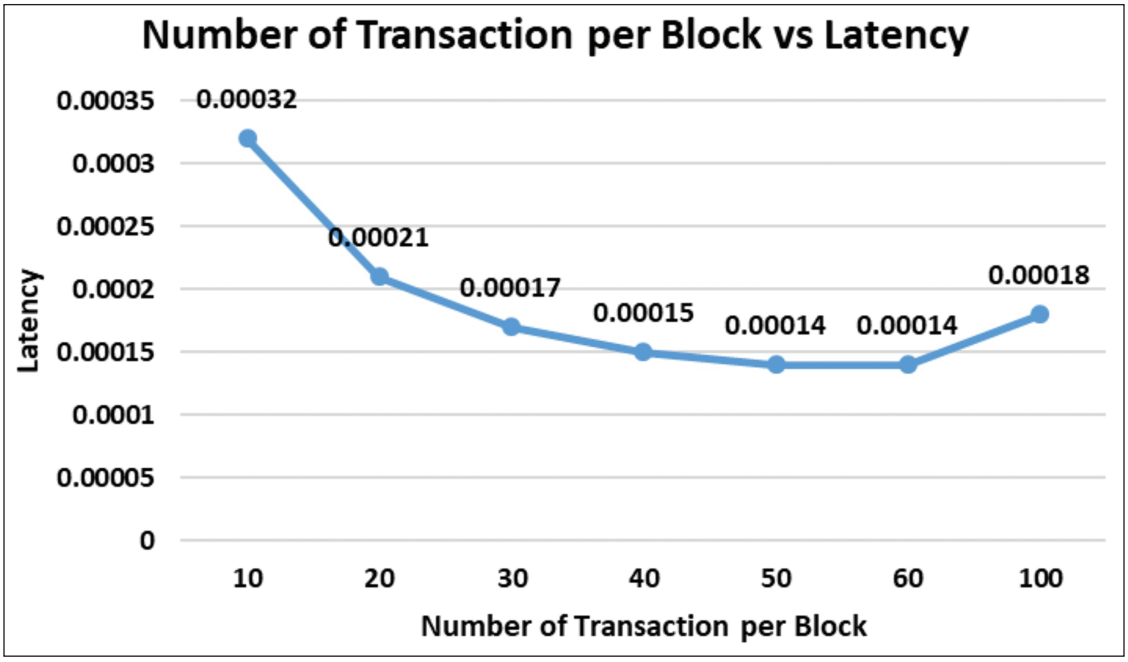


Figure 8. Impact of Transactions/Block on Latency.

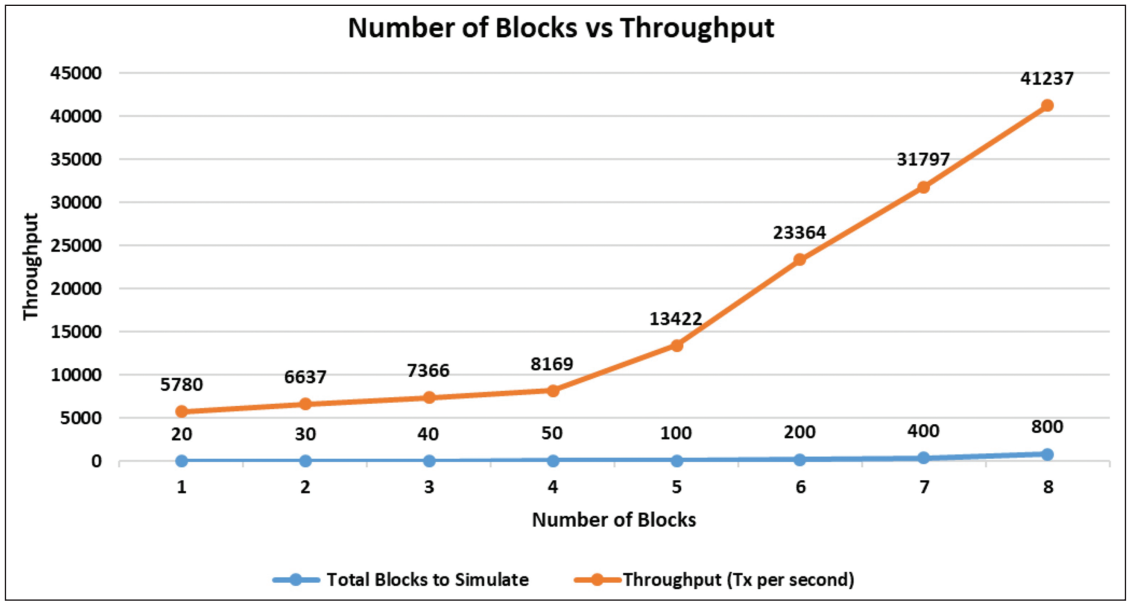


Figure 9. Impact of No. of Blocks on Throughput.

Table 3. Comparison of Proposed Framework with Existing Framework.

Parameter	[45]	[47]	[48]	Proposed Framework
Latency	0.62	0.52	0.56	0.57
Throughput	160	167	72	170

Table 4. Comparison with Existing Indian Framework.

Parameter	Framework-1 [33]	Framework-2 [35]	Framework-3 [37]	Proposed Framework
Blockchain based	Yes	Yes	No	Yes
Data storage	Cloud	Federated	Cloud	Decentralized
Authentication	Yes	No	Yes	Yes
Access control	Yes	No	Yes	Yes
Privacy preservation	Yes	Yes	No	Yes
Patient centric	No	No	No	Yes
Performance analysis	No	No	No	Yes

are not considered. The result shown for the article [48] also considered 1,000 transactions and a sending rate of 75 TPS. The author considered the write operation, that is, appending blocks to the ledger. The experiment does not consider block size, number of organizations, and channels.

In the proposed framework, execution was carried out with a 10 MB block size, 200 TPS, for 1,000 transactions. These results are taken for appending EHR, that is, write operation. From the results presented earlier, it is prominent that parameters such as block size, number of channels, rate of transaction, number of organizations, and consensus algorithm affect the system performance.

The proposed framework demonstrates improved throughput (170 TPS) compared to existing frameworks with a latency of 0.57 s.[45,47,48] It is observed that specific parameters, such as block size, transaction rate, and organizational structure, highlight their impact on system performance. This shows that optimizing these parameters enhances blockchain efficiency for managing EHR data.

Comparison of Proposed Framework with Existing Indian Framework

The proposed framework stands out as a comprehensive and patient-centric solution compared to the other frameworks shown in Table 4.

Unlike Framework-1 and Framework-3, which rely on cloud-based storage solutions, the proposed framework leverages decentralized data storage, ensuring enhanced security, autonomy, and reliability of patient data. This decentralized approach aligns well with modern advancements in blockchain technology, providing a robust mechanism for safeguarding sensitive healthcare information. Additionally, the proposed framework incorporates authentication and access control mechanisms, like Framework-1 and Framework-3, ensuring that only authorized individuals have access to the system, thereby enhancing both security and patient trust. Moreover, the privacy preservation capabilities of the proposed framework make it superior to Framework-3, ensuring that patient information is kept confidential and protected from unauthorized disclosure. One of the unique features of the proposed framework is its patient-centric design, which is absent from the other existing frameworks. This focus on patient-centricity ensures that the system prioritizes the patient's needs and preferences, fostering greater engagement and transparency between healthcare providers and patients.

Lastly, the proposed framework is the only one that includes a detailed performance analysis, a crucial factor for evaluating the system's efficiency and scalability in real-world healthcare environments. This further highlights its superiority over the existing frameworks that lack any performance evaluation measures.

Conclusion

Growing IT infrastructure for management of EHRs suffering from cyber-attacks. To enhance system security, the role-based access protocol is implemented through Java script in the proposed framework. Here the SC makes sure that data stored in the ledger may only be accessed and retrieved by authorized entities, such as physicians or clinical authorities. This method satisfies the needs of patient-centric EHR in the Indian healthcare setting by guaranteeing the safe storage and private access to healthcare data in the blockchain. The privacy of the patient is achieved through the grant and revoke mechanism. The proposed framework gives better performance compared to other frameworks by considering all affecting performance parameters. It was observed that increasing block size affects the latency and throughput increases as the number of transactions increases by keeping the appropriate block size (based on system specification). The proposed framework combines blockchain technology with decentralized storage, enhanced security features, and a focus on patient involvement, making it a more secure, efficient, and patient-friendly solution for healthcare data management.

Future research in the field can be explored by considering various consensus algorithms and their effects on the performance of the blockchain framework for the healthcare system. Currently, the proposed system considers only text data; image data also needs to be considered. Sharing data between blockchain-based systems and existing healthcare information systems may result in interoperability challenges, which also present opportunities for further research.

Abbreviations

API: Application programming interface; **CA:** Certificate authority; **CCs:** Chain codes; **CHC:** Community health centers; **CPU:** Central processing unit; **DREAD:** Damage, reproducibility, exploitability, affected users, discoverability; **EHR:** Electronic health record; **EMR:** Electronic medical record; **GDPR:** General data protection regulation; **HL-7:** Health Level 7; **HLF:** Hyperledger Fabric; **IoT:** Internet of things; **IPFS:** InterPlanetary File System; **IT:** Information technology; **ML:** Machine learning; **MoHFW:** Ministry of Health and Family Welfare; **MSP:** Membership service provider; **NA:** Network administrator; **PHC:** Primary health centers; **PHR:** Personal health record; **RAFT:** Reliable-replicated and fault-tolerant; **SC:** Sub-centers; **SCs:** Smart contracts; **SNOMED-CT:** Systematized Nomenclature of Medical-Clinical Terms; **STRIDE:** Spoofing, tampering, repudiation, information disclosure, denial of service, elevation of privilege; **TPS:** Transactions per second; **TTP:** Trusted third party.

Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical Approval and Informed Consent

Ethical approval was not sought for the present study.

Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

References

1. Banks MA. Sizing up big data. *Nat Med* 2020; 26(1): 5–6.
2. Zhang R and Liu L. Security models and requirements for healthcare application clouds. In: *Proceedings of* 3*rd international conference on cloud computing*. IEEE; 2010, pp 268–275.
3. Sahneya R and Sharmab M. Electronic health records: a general overview. *J Curr Med Res Pract* 2018; 8: 67–70.
4. Miyachi K and Mackey TK. hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf Process Manag* 2021; 58(3): 102535.
5. Abbasi N and Smith DA. Cybersecurity in healthcare: securing patient health information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. *J Knowl Learn Sci Technol* 2024; 3(3): 278–287.
6. Mehra P. Major data breaches that shook India in 2023. *TechCircle*;2023.https://www.techcircle.in/2023/12/26/major-data-breaches-that-shook-india-in-2023.
7. Sawant NM, Pottigar VV, and Mane NS. A survey on auditing techniques used for preserving privacy of data stored on cloud. In: *International conference on electrical, electronics, and optimization techniques (ICEEOT)*. 2016, pp. 1320–1323.
8. Nguyen DC, Pathirana PN, Ding M, et al. *Blockchain for secure EHRs sharing of mobile cloud based e-health systems*. Vol. 7. IEEE Access; 2019, pp. 66792–66806.
9. Egala BS, Pradhan AK, Badarla V, et al. Fortified-chain: a blockchain-based framework for security and privacy-assured internet of medical things with effective access control. *IEEE Internet Things J* 2021; 8(14): 11717–11731.
10. Casino F, Dasaklis TK, and Patsakisa C. A systematic literature review of blockchain-based applications: current status, classification and open issues. *J Telemat Inform* 2019; 36: 55–81.
11. Nakamoto S. *Bitcoin: a peer-to-peer electronic cash system*. 2008. https://bitcoin.org/bitcoin.pdf.
12. Khezr S, Moniruzzaman Md, Yassine A, et al. Blockchain technology in healthcare: a comprehensive review and directions for future research. *J Appl Sci* 2019; 9(9): 1–28.
13. Sawant N and Gomes J. Analysis of various blockchain-based solutions for electronic health record system. In: *International conference on advances in IoT and security with AI*. Singapore: Springer Nature; 2023, pp. 211–223.
14. Yue X, Wang H, Jin D, et al. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. *J Med Syst* 2016; 40: 218.
15. Roehrs A, da Costa CA, and da Rosa Righi R. OmniPHR: a distributed architecture model to integrate personal health records. *J Biomed Inform* 2017; 71: 70–81.
16. Xia Q, Sifah EB, Asamoah KO, et al. *MeDShare: trust-less medical data sharing among cloud service providers via blockchain*. Vol. 5. IEEE Access; 2017, pp. 14757–14767.
17. Rifi N, Rachkidi E, Agoulmine N, et al. Towards using blockchain technology for health data access management. In: 4*th International conference on advances in biomedical engineering (ICABME)*. IEEE; 2017, pp. 1–4.
18. Jiang S, Cao J, Wu H, et al. BlocHIE: a BLOCkchain-based platform for healthcare information exchange. In: *IEEE international conference on smart computing*, 2018, pp. 49–56.
19. Chen Y, Ding S, Xu Z, et al. Blockchain based medical records secure storage and medical service framework. *J Med Syst* 2018; 43(5): 1–5.
20. Guo R, Shi H, Zhao Q, et al. *Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems*. Vol. 6. IEEE Access; 2018, pp. 11676–11668.
21. Azaria A, Ekblaw A, Vieira T, et al. MedRec: using blockchain for medical data access and permission management. In: *Proceeding of* 2*nd international conference on open and big data*. IEEE; 2016, pp. 26–30.
22. Sun Y, Zhang R, Wang X, et al. A decentralizing attribute-based signature for healthcare blockchain. In: 27*th International conference on computer communication and networks (ICCCN)*. 2018, pp. 1–9.
23. Fan K, Wang S, Ren Y, et al. Medblock: efficient and secure medical data sharing via blockchain. *J Med Syst* 2018; 42(8): 136.
24. Zhang X and Poslad S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). In: *IEEE international conference on communications (ICC)*, 2018, pp. 1–6.
25. Liang X, Zhao J, Shetty S, et al. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In: *IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*. IEEE; 2017, pp. 1–5.
26. Dias JP, Reis L, Ferreira HS, et al. *Blockchain for access control in e-health scenarios*. arXiv preprint arXiv:1805.12267v1; 2018.
27. Nguyen DC, Pathirana PN, Ding M, et al. *Blockchain for securing EHR sharing on mobile cloud based e-health system*. Vol. 7. IEEE Access; 2019, pp. 66792–66806.

28. Wang Y, Zhang A, Zhang P, et al. *Cloud-assisted EHR sharing with security and privacy preservation via consortium blockchain*. *Vol*. 7. IEEE Access; 2019, pp 136704–136719.
29. Singh AP, Pradhan NR, Luhach AK, et al. A novel patient-centric architectural framework for blockchain-enabled healthcare applications. *IEEE Trans Ind Inform* 2021; 17(8): 5779–5789.
30. Cao S, Wang J, Du X, et al. CEPS: a cross-blockchain based electronic health records privacy-preserving scheme. In: *IEEE international conference on communications (ICC)*, 2020, pp. 1–6.
31. Sawant N and Gomes J. Exploring current framework in Indian healthcare system: research challenges and solution. In: *International conference on data analytics and insights (ICDAI-2024)*. 2024.
32. Zambare SA and Sawant NM. Performance analysis of patient centric EHR through Hyperledger Fabric. In: Gunjan VK, Zurada JM, Singh N, editors. In: *Modern approaches in machine learning and cognitive science: a walkthrough. Studies in computational intelligence*. Vol. 1117.
33. https://nhm.gov.in/index1.php?lang=1&level=2&sublinkid=1220&lid=190
34. Department of Health and Family Welfare Government of India. https://mohfw.gov.in/
35. Balsari S, Fortenko A, Blaya JA, et al. Reimagining health data exchange: an application programming interface–enabled roadmap for India. *J Med Internet Res* 2018; 20(7): e10725.
36. Mulani AO, Jadhav MM, and Seth M. Painless machine learning approach to estimate blood glucose level with non-invasive devices. In: *Artificial intelligence, internet of things (IoT) and smart materials for energy applications*. CRC Press; 2022, pp. 83–100.
37. Balsari S, Fortenko A, Blaya JA, et al. Reimagining health data exchange: an application programming interface–enabled roadmap for India. *J Med Internet Res* 2018; 20(7): e10725.
38. Maske Y, Jagadale AB, Mulani AO, et al. Development of BIOBOT system to assist COVID patient and caretakers. *Eur J Mol Clin Med* 2023; 10(01): 2023.
39. Pai MMM, Ganiga R, Pai RM, et al. Standard electronic health record (EHR) framework for Indian healthcare system. *J Health Serv Outcomes Res Methodol* 2021; 21(2) 339–362.
40. Kashid MM, Karande KJ, and Mulani AO. IoT-based environmental parameter monitoring using machine learning approach. In: *Proceedings of the international conference on cognitive and intelligent computing: ICCIC* 2021. Vol. 1. 2022, pp. 43–51.
41. Agbeyangi A, Oki O, and Mgidi A. Blockchain in healthcare: implementing Hyperledger Fabric for electronic health records at Frere Provincial Hospital. arXiv preprint arXiv:2407.15876; 2024.
42. Patil Y, Jain S, and Kale S. Leveraging Hyperledger Fabric for secure healthcare systems. *Int J Comput Digit Syst* 2024; 16(1): 189–200.
43. Sujihelen L. An efficient chain code for access control in hyper ledger fabric healthcare system. *e-Prime-Adv Electr Eng Electron Energy* 2023; 5: 100204.
44. Ndzimakhwe M, Telukdarie A, Munien I, et al. A framework for user-focused electronic health record system leveraging Hyperledger Fabric. *Information* 2023; 14(1): 51.
45. Nedaković A, Hasselgren A, Kralevska K, et al. Hyperledger Fabric platform for healthcare trust relations—proof-of-concept. *Blockchain: Res Appl* 2023; 4(4): 100156.
46. Jena SK, Kumar B, Mohanty B, et al. An advanced blockchain-based Hyperledger Fabric solution for tracing fraudulent claims in the healthcare industry. *Decis Anal J* 2024; 10: 100411.
47. Khatri S, al-Sulbi K, Attaallah A, et al. Enhancing healthcare management during COVID-19: a patient-centric architectural framework enabled by hyperledger fabric blockchain. *Information* 2023; 14(8): 425.
48. Saranya R and Murugan A. A hyperledger fabric-based system framework for healthcare data management. In *2023 7th International Conference on Computing Methodologies and Communication* (ICCMC). IEEE; 2023, pp. 552–556.
49. Díaz Á and Kaschel H. Scalable electronic health record management system using a dual-channel blockchain Hyperledger Fabric. *Systems* 2023; 11(7): 346.
50. Pahlajani S, Kshirsagar A, and Pachghare V. Survey on private blockchain consensus algorithms. In: 2019 *1st international conference on innovations in information and communication technology (ICIICT)*. IEEE; 2019, pp. 1–6.