Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 47 (2026), No. 7, pp. 2695–2712
DOI : 10.47974/JIOS-2325

BS-EHR : Blockchain-based secure electronic health record sharing

Md Ahteshamul Haque †
Khaleel Ahmad *
Sobiya Arsheen §
Department of Computer Science and Information Technology
Maulana Azad National Urdu University
Hyderabad 500032
Telangana
India

Laura Emilia Maria Ricci ‡
Fabrizio Baiardi @
Department of Computer Science
University of Pisa
Pisa 56127
Italy

Abstract

Blockchain is a disruptive technology currently finding its position in several domains of day-to-day life, like finance and administration. In healthcare, it can improve quality of life by addressing resource allocation and by protecting information. This is important because Electronic Health Records (EHRs) contain sensitive and private information of patients, but nowadays even EHR systems can be infected with malware or viruses that compromise patient information. Blockchain technology offers a viable solution for addressing these issues by providing a secure, tamperproof, decentralized platform for EHR management. Furthermore, this technology provides a decentralized platform that eliminates the need for intermediaries or third parties to manage and access the data. This means that patients have complete control over their medical records and can share them securely and transparently with healthcare providers without the need for a central authority to validate the data. This paper describes a secure Electronic Health Record system using the Hyperledger Fabric platform of permissioned blockchain. Our system ensures that patients' personal

---

† *E-mail:* `haquemanuu@gmail.com`
* *E-mail:* `khaleelahmad@manuu.edu.in (Corresponding Author)`
§ *E-mail:* `sosheen95@gmail.com`
‡ *E-mail:* `laura.ricci@unipi.it`
@ *E-mail:* `f.baiardi@unipi.it`

health information remains secure and private, and healthcare providers need to comply with regulatory requirements for protecting health data. Additionally, the proposed system provides secure access to EHRs to the participating entities by using advanced cryptographic techniques (ECC) that prevent unauthorized parties from accessing or modifying the data. The proposed system aims to decrease transaction time, improve throughput, and reduce latency.

Subject Classification: *68M25.*

Keywords: *Blockchain, Hyperledger fabric, Hyperledger caliper, Data sharing, Electronic health record, Security, Privacy.*

1. Introduction

Healthcare is essential in everyone's life, and the records for the same are maintained manually. As these records are increasing rapidly, there is a need to plan their maintenance in digital formats. Electronic records reduce errors related to handwriting, lost or misplaced documents, incomplete or missing information related to prescriptions, and other documentation errors. The records can be stored and used as a reference to diagnose the patient and review their complete history, including the drugs and treatment prescribed. Overall, EHR offers significant benefits over paper-based medical records, which include improved accuracy, efficiency, patient care, and cost savings [1]. One of the biggest security challenges for Electronic Health Records (EHRs) is unauthorized access to patient information through hacking, cyberattacks, phishing scams, and data breaches. EHR systems can be infected with malware or viruses that can compromise patient information. Data integrity is also a challenge in electronic health records. Any error in patient data can result in incorrect diagnosis, treatment decisions, or medication orders [2].

Blockchain technology enables transparent information sharing inside an organization network. It also offers several benefits due to decentralized networks, immutability, increased security, better privacy, improved interoperability, and faster access to medical data at reduced costs [3]. Data is organized in blocks that are connected in a chain and stored in a database; each block contains records of a patient's medical data, including treatment, medication, and diagnoses.

Blockchain technology plays an important role in providing secure data access to EHRs [4], and it improves the efficiency of healthcare providers by allowing them to quickly access patients' information from a single location. This saves time, reduces redundancy, and results in more accurate decisions [5] to provide patients with more effective care. It can also improve communication and coordination of healthcare providers, resulting in better service.

An electronic health record is stored in blocks after being encrypted. Healthcare providers can access patient data on the blockchain, but only with the patient's permission and after receiving the proper decryption keys. Patients can control who can access their data, and they can remove access at any time. Blockchain technology [6] has brought revolutionary changes to the healthcare industry by facilitating smooth interoperability among diverse healthcare providers.

Blockchain technology effectively addresses significant challenges in the sharing of EHRs, which contain sensitive patient data. It tackles issues related to data security, privacy, interoperability, and data ownership.

The goal of our research is to implement an EHR system that exploits the unique features of a blockchain, such as security, access control, and privacy of data, to achieve secure data sharing. This research work confirms the potential benefits of the blockchain for EHR data sharing, making this technology worth exploring and investing in for the future of healthcare. The throughput, latency, and success rate of the proposed solution have been measured while increasing the execution duration of transactions. It is found that longer transactions result in increased throughput, decreased latency, and significantly improved success rate of the transactions.

The paper is organized as follows: Section 2 reviews the relevant literature to find the research gap in the context of Blockchain-based EHR. Section 3 investigates the transaction flow of Hyperledger Fabric, while Section 4 presents a proposed approach. Section 5 presents the performance measurement, and Section 6 concludes the paper.

2. Literature Review

This review aims to synthesize current research on EHR data sharing in the context of Hyperledger Fabric, a widely used permissioned blockchain platform, revealing the complexities, challenges, and repercussions connected with data-sharing mechanisms inside this platform.

Nguyen et al. [7] investigated the use of blockchain technology in healthcare, specifically for managing access to and exchange of EHRs between hospitals and clinics. In this work, the authors employ the Ethereum blockchain, Amazon Cloud Front, and IPFS to showcase practical data-sharing scenarios in a mobile app. Potential applications are discussed, with a focus on the safe transfer of EHRs and the control of who has access to what information.

Shamshad et al. [8] proposed a blockchain-based protocol to address the challenges faced by the telecare medicine information system (TMIS) in accurately diagnosing and treating new patients remotely. They investigated data security, access control, secure search, and privacy preservation by public-key encrypting all EHRs with a searchable keyword, but the evaluation of the scalability and efficiency of the protocol was missing.

Arsheen and Ahmad [9] reviewed the blockchain technology's current development in the healthcare industry and examines how these cutting-edge solutions aid in accelerating treatment protocols and also mitigate the COVID-19 pandemic's effects.

Gan et al. [10] proposed a blockchain-based access control strategy for handling personal health information. To prove the usefulness and viability of the suggested strategy, a case study is carried out using Ethereum.

Hussien [11] proposed a decentralized personal health record (PHR) system using blockchain technology to solve privacy concerns in healthcare applications. It established an enforced cryptographic permission and access control scheme for encrypted medical data that has been offloaded to the IPFS. The proposed scheme may not be suitable for all healthcare applications, as some may require more complex access control policies or distinct encryption mechanisms.

Nguyen et al. [12] proposed an effective approach for healthcare data sharing and offloading to improve services and reduce device resource burden. They used methods that included efficient data offloading, new data sharing integrated with blockchain, and trustworthy access control mechanisms.

Abdelgalil and Mejri [13] presented a framework called HealthBlock that employs blockchain technology to facilitate the collaborative sharing of EHRs while ensuring their integrity, interoperability, and availability. IPFS stores and shares patients' EHRs in decentralized off-chain storage, ensuring their immutability. Hyperledger Indy provides patients with complete control over their EHRs, while Hyperledger Fabric stores patient-access control policies and delegations.

Ahmad et al. [14] proposed the Vaccine Intelligent Network, which includes vaccines covered by the Universal Immunization Programmed, and is based on blockchain technology for pregnant women. In order to create the Electronic Immunization Record for pregnant women who have received vaccinations, the proposed system is built on the Hyperledger Fabric platform.

Reegu et al. [15] proposed a blockchain-based EHR system that is interoperable. The suggested framework can provide the healthcare industry with safer ways to exchange health information and enhance the characteristics of immutability, security, integrity, and confidentiality in centralized storage.

Yuan et al. [16] proposed a healthcare data sharing and protection system based on blockchain technology that ensures efficient access and lessens the workload of patients by storing encrypted data on a cloud server. They have implemented a better proxy re-encryption strategy to protect against potential Man-in-the-Middle (MITM) attacks and maintain the privacy of PMHR data while lowering computational cost.

Jayakumar et al. [17] suggested a blockchain-based method that guarantees safe storage, effective medical record transmission, and decentralization of patient data into a single record owned by the patient.

Arsheen and Ahmad [18] proposed a blockchain-based vaccine supply chain and immunization framework. In their research, the authors focused on the security concerns in the blockchain and discussed how it helps to mitigate the common security and privacy threats of networking.

3. Hyperledger Fabric Transaction Flow

Hyperledger Fabric, an enterprise-grade blockchain framework [19], offers a flexible and modular architecture designed for developing robust applications. Notably, Hyperledger Fabric excels in enabling secure and transparent data sharing among multiple participants. It achieves this through a shared ledger, a replicated database storing the current state of the network. Transactions are validated and endorsed by peer nodes before being added to the shared ledger, guaranteeing data integrity and accuracy [20]. Chaincode is a self-executing agreement with encoded terms, further enhancing efficiency by automating processes like billing and insurance claims, thereby reducing administrative burdens and minimizing errors. It operates to enable the execution of business logic, automate processes, and maintain the integrity of transactions, and it may also be referred to as "smart contracts" in the Hyperledger Fabric, which is a private and permissioned blockchain network where participants must be known and granted access [21]. The decentralized nature of blockchain ensures a secure and transparent exchange of information

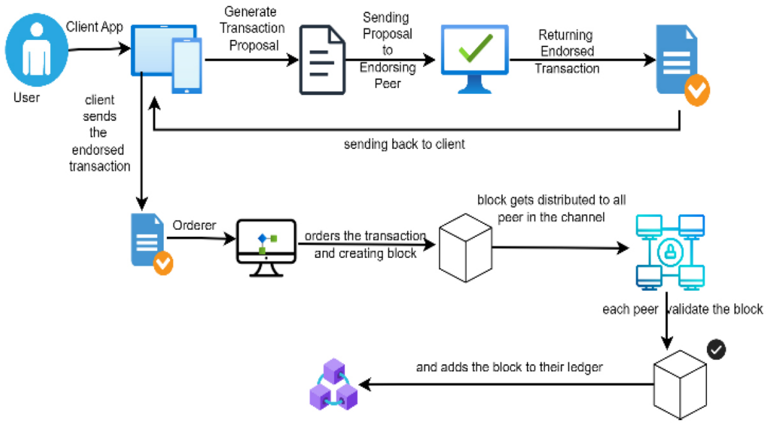

Figure 1

Transaction Flow in Hyperledger Fabric

without the need for intermediaries or third-party validators. Consequently, data can be shared directly between parties, streamlining the process.

Figure 1 depicts the detailed steps of transaction flow in Hyperledger Fabric, where the user initiates the transaction proposal through a client application [22], and it executes the following steps:

Patient Interface: This is a web application to access and manage EHR, control data-sharing preferences, and communicate with healthcare providers.

Doctor Interface: Healthcare professionals access the EHR system through a separate user interface designed for doctors. They can update medical information and communicate with patients.

Distributed Ledger: It securely stores the patient's medical history, diagnoses, treatments, test results, and other relevant data while maintaining data integrity and privacy.

Transaction Proposal: The necessary details for the transaction, such as the channel name, chaincode name, chaincode version, and the function to be invoked. These parameters determine the specific action to perform on the ledger. Additionally, gather any required function arguments from the client application.

Consent Management: A consent management module handles patient consent for data sharing. It enables patients to specify their preferences for sharing a specific portion of their EHR data.

Channel: Secure communication channels that use encryption protocols are established between the patient interface and the doctor interface. File encryption system on the peer can be used to encrypt ledger data at rest, while TLS is used to encrypt data in transit. Fabric uses TLS 1.3 to protect and authenticate nodes at the network level. TLS certificates issued by ECDSA and RSA are both accepted.

4. Proposed Approach

Blockchain technology provides a secure store for EHRs. Figure 2 shows the architecture of the EHR system using Hyperledger Fabric.

The fundamental system components are briefly described here:

1. **Identity and Authentication**: The architecture incorporates an identity verification and authentication mechanism to validate the patient's identity using Public Key Infrastructure (PKI) and authorize access to the EHR system.
2. **Submit Transaction Proposal to Endorsing Nodes:** Before starting the network, each node has already decided on the endorsement policy. It formulates the transaction proposal by combining the defined parameters and required client certificates, such as the CA and orderer certificates. Then, it sends the transaction proposal to the endorsing nodes in the network that endorse the transaction proposal by applying their digital signature.

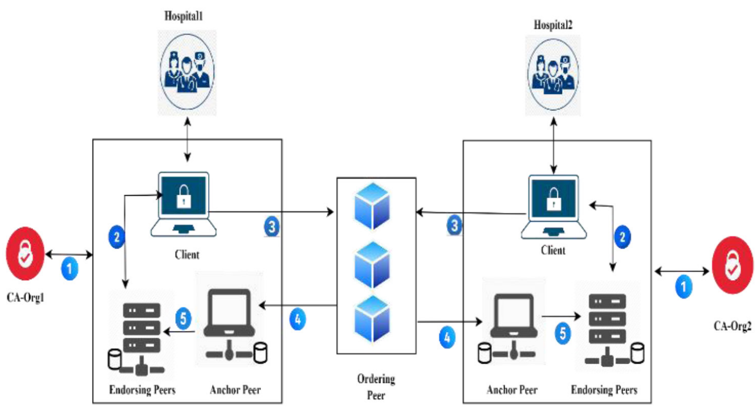

Figure 2

Architecture of EHR System

3. **Submit to Ordering Service:** Collect the endorsed transaction proposals, which include the necessary signatures from the endorsing nodes. These endorsed proposals form the complete transaction. Once the transaction gets verified at each of the endorser nodes, it is submitted to the ordering service.
4. **Validate and commit the block:** The participating peers receive the block from the ordering service. They validate the transaction by checking the endorsements and ensuring it meets the defined endorsement policies. If the transaction is valid, the peers update their local copy of the ledger to reflect the changes introduced by the transaction.
5. **Dissemination of block:** Once the transaction is successfully committed by a sufficient number of peers, it is considered confirmed. The changes made by the transaction are now permanent and reflect the updated state of the blockchain.

Data Exchange APIs: Application Programming Interface (APIs) facilitate the exchange of data between the patient interface and the doctor's interface. These APIs simplify the secure transfer of specific data. The implementation of this architecture offers a secure and efficient EHR data sharing between a patient and a doctor, with patient privacy as a prime focus. The architecture ensures patient complete authority over their health records while enabling effective collaboration and communication between patients and healthcare providers. Access Control List can also be used to add additional layers of security. Figure 3, shows the Finite State Automata for the access control with its transition steps.

Finite State Automata for EHR Access Control:

States:

1. *LedgerInitialized (s0) [Initial State]*
2. *AccessRetrieved (s1) [Final State]*
3. AccessRevoked (s2) [Final State]
4. AccessGranted (s3)

Transitions:

- Initial → LedgerInitialized: asyncinitLedger(ctx)
- LedgerInitialized →AccessGranted:

asyncgrantAccess(ctx, patientId, providerId,accessLevel)

- LedgerInitialized→AccessRevoked: asyncrevokeAccess(ctx, patientId, providerId)
- AccessGranted →AccessRetrieved:

  asyncgetAccess(ctx, patientId, providerId)
- AccessRevoked → AccessRetrieved: asyncgetAccess(ctx, patientId, providerId)

Inputs:

a,b,c identifies a new transaction, an active transaction and an invalid transaction respectively.

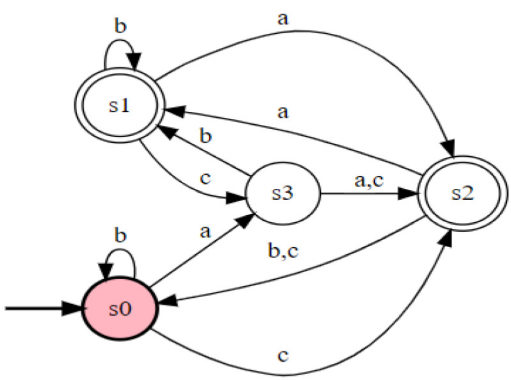

Figure 3

Finite State Automata for Access Control

- The LedgerInitialized (s0) is the start state; it initializes the access control rules. The system manages the access rights of the users by transferring to one of the two states, "AccessRevoked" and "AccessGranted". Based on the transaction parameters, it may traverse to "AccessRetrieve". If the system validates the user's ID then it may grant access to the patient's data and transfer to the AccessGranted state. If the user already possesses access rights to data, the system may proceed to the "AccessRevoked" state to withdraw the access rights from the patient's data.
- The AccessGranted (s3) state receives the patient ID, provider ID, and access level, it may transition either to AccessRevoked (s2) to revoke the access from the user or to AccessRetrieved (s1) to find the

access rights of the user, and then the user is granted the access right to the patient's data.

- The AccessRevoked (s2) state receives the patient ID and provider ID. It will revoke the access from the user. It may transition to either AccessRetrieved (s1) to find the access right of a user or to LedgerInitialized (s0), the initial state.
- The AccessRetrieved (s1) state receives the patient ID and provider ID to get the access control rule for the current patient and provider. It may transition back to either AccessRevoked (s2) to revoke the access if access is already granted to the user or to AccessGranted (s3) if access is not granted.

A. **Participants and Organizations**

In Hyperledger Fabric, an organization represents a unique entity or participant within a blockchain network. It could be a hospital, a department, or any identifiable entity involved in the network. Organizations play a critical role in the permissioned blockchain infrastructure provided by Hyperledger Fabric.

Table 1

Participants and Organizations

Sr. No	Participants	Organizations
1	Patients	Org1 (Hospital 1)
2	Doctors	Org2 (Hospital 2)
3	Nurses	

An organization in Hyperledger Fabric typically consists of multiple network participants or nodes, each having its own cryptographic identities and X.509 certificates. The organization is identified by a unique identifier known as the 'MSP ID' (Membership Service Provider ID), which is used to authenticate and differentiate members of the organization within the network. As shown in Table 1, in the described prototype, there are two organizations Org1 and Org2, with two peers in each organization for three participant entities in the network, i.e. Patients, Doctors, and Nurses.

B. **Sequence Diagram of Data Sharing Between Multiple Hospitals**

As shown in Figure 4, several healthcare providers share EHR data through a decentralized blockchain network. When a provider wants to access a patient's health record, at first, it requests access, the chaincode verifies, authenticates, and authorizes access to the requested record. The chaincode must be installed on the channel connected between the peers of the organization. The Smart Contract needs the data from the doctor, nurse, and patient to process. The processed information is submitted to CouchDB in JSON format. The system then encrypts and hashes the requested data and stores it on the blockchain. When another provider requests access to the same record, the chaincode verifies its authentication and, if successful, authorizes access, and the data is decrypted and shared securely. Protecting the privacy and integrity of the exchanged data is the job of the blockchain and the chaincode that runs on it. Only the data on the blockchain is accessible to healthcare practitioners and providers.

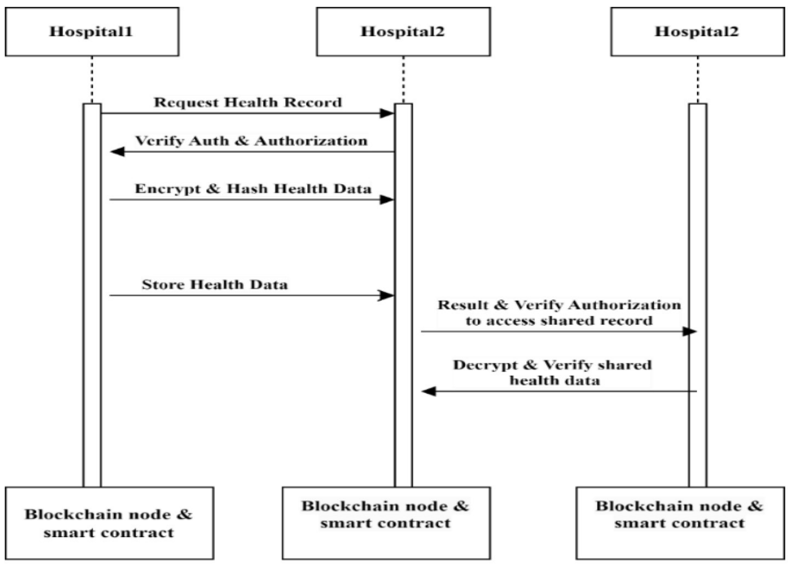

Figure 4

Sequence Diagram of Data Sharing between Multiple Hospitals

C. Practical Setup and Results

Table 2 shows the specifications of the system used in the experiments.

Table 2

Experimental environment

Configurations	Values
Hardware mode	MSI
RAM	16.0 GB
Processor	Intel(R) i7
Disk Capacity	1 TB SSD
OS Name	Ubuntu 22.04.2 LTS
OS Type	64-bit

The proposed framework uses the Docker compose tool to create, deploy, and run applications using a multi-container. In the Hyperledger Fabric network, Docker containers help to provide portability, uniformity, and isolation. The proposed network includes 13 services. Two further services are related to chaincode services, resulting in a total of 15 services in this module. Each service has a unique configuration that includes environment variables, assigned ports, volumes, and interdependencies. These options define variables like logging levels, network addresses, TLS configurations, CouchDB installations, and more. The configuration precisely defines environment variables, volumes, ports, and dependencies to guarantee the correct arrangement and efficient communication

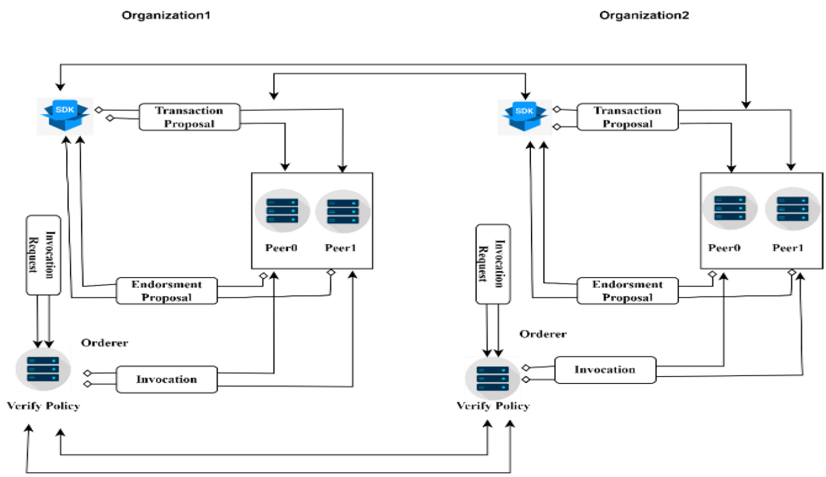

Figure 5

Architecture of the Proposed Network

between the components of the blockchain network. Figure 5, shows the overall architecture of the proposed system.

A channel that is named 'mychannel' is a private communication path between peers of the organization. In the blockchain network, it defines a mechanism to establish private spaces where confidential transactions can occur among a specific group of participants. The artifacts defined in the Docker container kick off the execution, generate cryptographic material for designated hosts, and run commands on each server to set up a channel, enable peer joining on the configured channel, install the chaincodes, and instantiate it.

5. Performance Evaluation

Several important performance metrics can be adopted to assess the performance of chaincodes. These metrics assist in analyzing the efficiency, throughput, latency, and overall performance of the system. Some commonly used performance metrics for evaluating Hyperledger Fabric chaincodes are:

This Hyperledger Fabric test network has 2 organizations, each with 1 endorsing peer for a total of 4 peer nodes. There are 3 orderer nodes. All nodes run on the x86_64 virtual machines using Ubuntu 22.4 with Hyperledger Fabric 2.2 version.

Figure 6, analyzes the throughput of five chaincodes for two Organizations, Org 1 and Org 2. It can be observed that throughput is

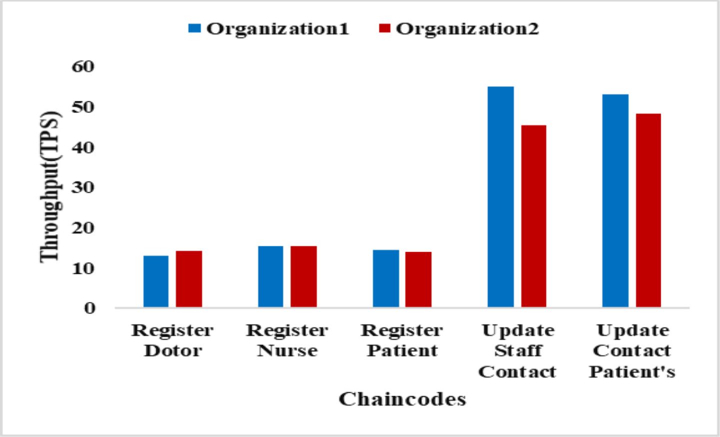

Figure 6

Throughput comparison between two organizations

approximately the same because of the slight difference between organizations.

Figure 7 shows the throughput of three chaincodes for different transaction durations (ranging 10-30) for one organization. This shows that the throughputs of almost all the chaincodes increase with the transaction durations.

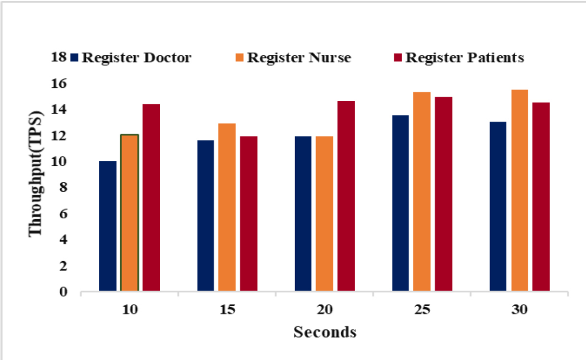

Figure 7

Throughput with different chaincodes

Figure 8 plots the Success rate of the three chaincodes for different transaction durations (ranging 10-30) for one organization. It can be observed that the success rate steadily rises alongside the duration of the transaction for registering multiple users at every invocation.

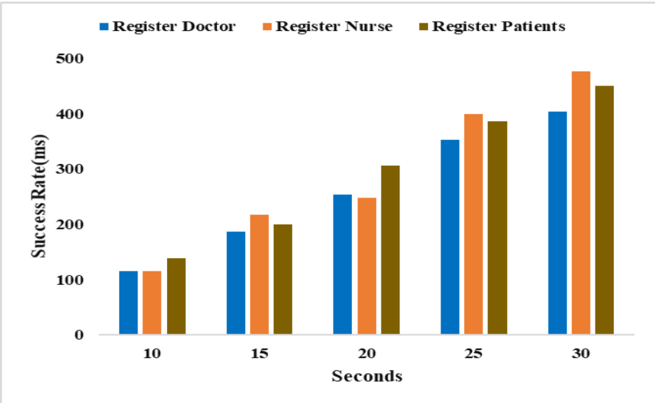

Figure 8

Success rate with different chaincodes.

Figure 9, plots the average latency of different chaincodes for different transaction durations. It shows that the average latency for Registered Doctors, Registered Nurses, and Registered Patients improves with the transaction duration (with avg. latency < 1). These three chaincodes register multiple users at every invocation, and they reach their best performance when the transaction duration is maximised. As it should be expected, the fixed cost of a transaction is compensated by the longest time of the transaction.

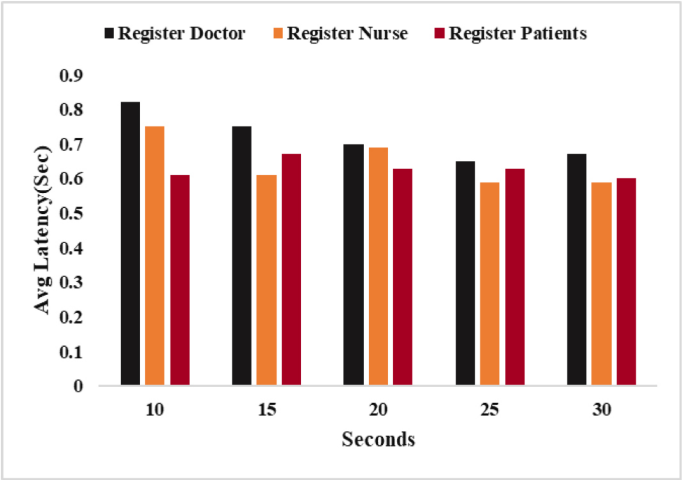

Figure 9

Success rate with different chaincodes

Overall, the experiments confirm the relationship between transaction duration and performance metrics such as throughput, average latency, and success rate. In general, longer transaction durations result in increased throughput, decreased average latency, and improved success rates for all the chaincodes.

6. Conclusion And Future Work

Blockchain technology ensures a secure, decentralized, and transparent exchange of information without the need for intermediaries or third-party validators. Consequently, data can be shared directly between parties, streamlining the process. However, many organizations are actively exploring the potential of blockchain in the healthcare domain. The adoption of blockchain in healthcare fosters efficient sharing of EHRs between healthcare providers and patients. This can improve the privacy, security, and interoperability of health records.

This work has presented a blockchain-based EHR system that enhances data security while increasing the complexity of unauthorized access to or updating of patient information while enhancing data security. Regardless of where a patient is receiving care, the proposed system simplifies for patients and healthcare professionals the access to healthcare data. Our research demonstrates the blockchain's potential advantages for exchanging EHR data. While increasing the framework's execution time, the throughput, latency, and success rate of chaincode transactions are measured and discovered that greater transaction time results in higher throughput, lower latency, and much higher transaction success rates. In a nutshell, the proposed framework achieved the security and reliability of the EHR. There are also some challenges associated with implementing blockchain-based EHR systems, such as technical complexity, regulatory compliance, and interoperability with existing healthcare IT systems. Future work concerns the integration of the proposed EHR system with medical laboratories and healthcare Insurance providers, which can be planned to make strategic improvements to the healthcare department. The main challenge for this work would be the full achievement of interoperability.

References

[1] 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.

[2] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Inform. J.,* vol. 22, no. 2, pp. 177–183 (2021), doi: 10.1016/j.eij.2020.07.003.

[3] Y. Sharma and B. Balamurugan, "Preserving the Privacy of Electronic Health Records Using Blockchain," *Procedia Comput. Sci.,* vol. 173, pp. 171–180 (2020), doi: 10.1016/j.procs.2020.06.021.

[4] R. Sangeetha, B. Harshini, A. Shanmugapriya, and T. K. P. Rajagopal, "Electronic Health Record System Using Blockchain," *Int. Res. J. Multidiscip. Technovation,* vol. 1, no. 2, pp. 57–61 (2019), doi: 10.34256/irjmt1927.

[5] A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," *IEEE Access*, vol. 7, pp. 147782–147795 (2019), doi: 10.1109/ACCESS.2019.2946373.

[6] V. Kamath, J. Sreenivas, and K. Yelpale, "Blockchain Solution to Healthcare Record System Using Hyperledger Fabric," *ResearchGate Preprint (2021)*, doi: 10.13140/RG.2.2.27957.60640.

[7] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Blockchain for Secure EHRs Sharing of Mobile Cloud Based E-Health Systems," *IEEE Access*, vol. 7, pp. 66792–66806 (2019), doi: 10.1109/ACCESS.2019.2917555.

[8] S. Shamshad, Minahil, K. Mahmood, S. Kumari, and C.-M. Chen, "A Secure Blockchain-Based E-Health Records Storage and Sharing Scheme," *J. Inf. Secur. Appl.*, vol. 55, Art. no. 102590 (2020), doi: 10.1016/j.jisa.2020.102590.

[9] S. Arsheen and K. Ahmad, "SLR: A Systematic Literature Review on Blockchain Applications in Healthcare," in *Proc. 2021 Int. Conf. Inf. Sci. Commun. Technol. (ICISCT)*, Tashkent, Uzbekistan, pp. 1–6 (2021), doi: 10.1109/ICISCT52966.2021.9670136.

[10] C. Gan, A. Saini, Q. Zhu, Y. Xiang, and Z. Zhang, "Blockchain-based access control scheme with incentive mechanism for eHealth systems: Patient as supervisor," *Multimed. Tools Appl.*, vol. 80, no. 20, pp. 30605–30621 (2021), doi: 10.1007/s11042-020-09322-6.

[11] H. M. Hussien, S. M. Yasin, N. I. Udzir, and M. I. H. Ninggal, "Blockchain-based access control scheme for secure shared personal health records over decentralised storage," *Sensors*, vol. 21, no. 7, Art. no. 2462 (2021), doi: 10.3390/s21072462.

[12] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "A cooperative architecture of data offloading and sharing for smart healthcare with blockchain," in *Proc. IEEE Int. Conf. Blockchain Cryptocurr. (ICBC)*, pp. 1–6 (2021), doi: 10.1109/ICBC51069.2021.9461063.

[13] L. Abdelgalil and M. Mejri, "HealthBlock: A Framework for a Collaborative Sharing of Electronic Health Records Based on Blockchain," *Future Internet*, vol. 15, no. 3, Art. no. 87 (2023), doi: 10.3390/fi15030087.

[14] K. Ahmad, L. E. M. Ricci, F. Baiardi, and S. Arsheen, "Hyperledger Fabric Enabled Vaccine Intelligent Network to Implement Immuniza-

tion Program," in *Proc. 12th IEEE Int. Conf. Commun. Syst. Netw. Technol. (CSNT)*, pp. 822–828 (2023), doi: 10.1109/CSNT57126.2023.10134692.

[15] F. A. Reegu, H. Abas, Y. Gulzar, Q. Xin, A. A. Alwan, A. Jabbari, R. G. Sonkamble, and R. A. Dziyauddin, "Blockchain-Based Framework for Interoperable Electronic Health Records for an Improved Healthcare System," *Sustainability*, vol. 15, no. 8, Art. no. 6337 (2023), doi: 10.3390/su15086337.

[16] W. X. Yuan, B. Yan, W. Li, L. Y. Hao, and H. M. Yang, "Blockchain-based medical health record access control scheme with efficient protection mechanism and patient control," *Multimed. Tools Appl.*, vol. 82, no. 11, pp. 16279–16300 (2023), doi: 10.1007/s11042-022-14023-3.

[17] S. Jayakumar, S. Ajith, N. R. Sriram, V. K. Reddy, and N. S. Ramaiah, "Block-chain based electronic health record system," *AIP Conf. Proc.*, vol. 2427, no. 1, Art. no. 020057 (2023), doi: 10.1063/5.0101344.

[18] S. Arsheen and K. Ahmad, "ImmuneChain: A blockchain-based secure and transparent vaccine supply chain," *SN Comput. Sci.*, vol. 6, no. 1, Art. no. 73 (2025), doi: 10.1007/s42979-024-03421-z.

[19] A. Adikane, N. Akole, A. Auti, S. Bhosale, and N. Mhetre, "Electronic Health Records Access System Using Hyperledger Fabric," *International Research Journal of Engineering and Technology (IRJET),* vol. 8, no. 5, pp. 4033–4036 (May 2021).

[20] Q. Wang and S. Qin, "A Hyperledger Fabric-based system framework for healthcare data management," *Appl. Sci.*, vol. 11, no. 24, Art. no. 11693 (2021), doi: 10.3390/app112411693.

[21] S. Arsheen and K. Ahmad, "Blockchain-Enabled Immunization System: A Novel Idea to Leverage Reliability and Traceability," in *Proc. 3rd Int. Conf. Emerg. Technol. (INCET)*, Belgaum, India, pp. 1–5 (2022), doi: 10.1109/INCET54531.2022.9824500.

[22] Hyperledger Foundation, "Hyperledger Foundation." [Online]. Available: https://www.hyperledger.org/. [Accessed: Oct. 5, 2025].

Received December, 2025