[1] Abida Khanam
[2]Mohd Faizan Farooqui

"Ensuring Security in Electronic Health Records: Implementing and Validating a Blockchain and IPFS Framework"

Journal of Electrical Systems

Abstract: - The rapid advancement of information technology has completely transformed the healthcare sector, demanding creative solutions to tackle a wide range of challenges. Electronic Health Records (EHR) are essential in contemporary healthcare systems, enabling the storage, retrieval, and sharing of data about patients among healthcare providers. Ensuring the confidentiality and safety of EHR data is a major challenge because of the sensitive nature of health-related information and the growing number of cyber threats. Our paper introduces a new framework for enhancing the security of Electronic Health Records by leveraging the use of blockchain technology and the Inter Planetary File System (IPFS). The framework utilizes the immutability and decentralized nature of blockchain to guarantee data integrity and audibility, while IPFS offers a distributed and resistant tamp storing solution for data stored off-chain. Explaining the structure of our proposed framework, which involves combining blockchain and IPFS components, and examining how it tackles important security and privacy issues in EHR systems. Furthermore, a demonstration of the framework's implementation is provided, along with an assessment of its performance, scalability, and security aspects. The study illustrates the potential and success of utilizing blockchain and IPFS to secure Electronic Health Records, leading to improved data security and compatibility in healthcare systems.

Keywords: Electronic Health Records, Blockchain, InterPlanetary File System (IPFS), Security, Privacy, Data Integrity, Decentralization, Healthcare Systems.

1. Introduction

In recent years, the volume of digital data has been growing rapidly, doubling annually and significantly impacting our daily lives. It is evident that data is the key driver of the future economy. Big companies need increasing amounts of data as the use of machine learning algorithms improves[1]. The social media industry is currently experiencing criticism for the sale of user data. In the future, major corporations and large companies might be willing to pay for access to our data, given its inherent value. Ensuring a private and secure access control designs is crucial in the healthcare sector. In the era of big data, vast amounts of health information are stored and accessed over the Internet. Cloud networking is becoming more and more essential in this process[2].

Despite being user-friendly and dependable, traditional EHR (electronic health record) systems pose various privacy and security concerns. Health records are filled with sensitive information regarding patients and their diagnoses, making it one of the most critical data collection methods. HR data is now more vulnerable to breaches because of the internet and digital healthcare system advancements. It is important to consider the safety and confidentiality of EHR data when evaluating a decentralised and trust-based approach.

Nevertheless, obstacles remain, such as storing and processing information, and security. The framework we have developed tackles these challenges by combining blockchain technology for health record security and IPFS for decentralised storage[3].

However, blockchain is viewed as a trustless system; it does assume certain factors such as device security and the intentions of the miners. Eliminating these trust elements can be categorised under zero trust architecture. There have been few studies exploring the combination between blockchain technology and zero trust principles. A model was proposed in reference that utilises blockchain technology to enable the implementation of the zero trust framework. This framework primarily emphasised implementing a zero trust architecture, utilising blockchain to guarantee access management, user authentication, and transaction security. In a separate study, Samaniego and Deters introduced a model called Amatista, which integrates zero trust in blockchain to serve as a middleware for IoT devices[4]. This model utilised the zero trust structured mining process, where block and validation of transactions occur at distinct trust levels.

Digitising patients data as well as streamlining clinical workflows has revolutionised the healthcare industry with the widespread implementation of EHR (electronic health records). Nevertheless, conventional EHR systems are frequently centralised and susceptible to data breaches, unauthorised access, and tampering. Securing and safeguarding sensitive health data is crucial for upholding patient trust and meeting regulatory standards.

[1,2] Computer Application, Integral University, Lucknow, India.
[1]abidakhan@iul.ac.in, [2]ffarooqui@iul.ac.in

Blockchain technology has proven to be a valuable solution for improving the safety and integrity of EHR systems due to its decentralisation, immutability, and transparency. Storing EHR data on a distributed ledger can help prevent unauthorised modifications, create an auditable trail of unauthorized access and changes, and facilitate safe transmission of patient information between healthcare providers. Moreover, the Interplanetary File System (IPFS) provides a decentralized and content-addressable storing solution that complements blockchain features. It offers effective and tamper-resistant storing for off-chain data linked to EHRs.

Integration of Elliptic Curve Cryptography (ECC) in the suggested framework for Electronic Health Records (EHR) improves the security and privacy of patient data stored on IPFS, while also utilizing blockchain technology for the accuracy of data and auditability. This thorough method guarantees the protection of sensitive healthcare information from unauthorized access, tampering, and data security breaches[5].

Despite being user-friendly and dependable, traditional EHR systems (electronic records) come with various privacy and security concerns. Health records are repositories of highly confidential patient information and diagnoses, making them one of the most sensitive forms of data collection. With the evolution of the internet and digital healthcare systems, HR data has become more vulnerable to breaches . It is crucial to consider the safety and confidentiality of HR data when evaluating a decentralized and trust-based approach.

Nevertheless, there are still obstacles to overcome, such as storing and processing data, as well as security. Our framework aims to tackle these challenges by combining blockchain technology for medical record security and IPFS for decentralized storage[6].

However, blockchain is viewed as a trustless system, although it does rely on factors such as device security and the intentions of the miners. Eliminating these trust elements can be categorized under zero trust architecture. There have been few studies exploring the combination of blockchain and zero-trust principles. A model was proposed in reference that utilizes blockchain to enable the implementation of the zero-trust framework. This framework primarily emphasizes implementing zero trust architecture, utilizing blockchain to guarantee access management, user authentication, and transaction security. In a separate study, Samaniego and Deters introduced a model called Amatista, which integrates zero trust in blockchain to serve as a middleware program for IoT devices. This model utilized the zero trust structured mining process, where block and transaction verification occur at distinct trust levels[7].

1.1 Functional and Non-Functional Requirements of EHR

To guarantee the efficiency, usability, and compliance of electronic health record (EHR) systems, it is crucial to specify both functional and non-functional needs[8]. The functional and non-functional requirements which are relevant to EHRs are broken down as follows:

Functional Requirements:

- Data Capture: Patient health data, such as demographics, medical histories, prescription histories, allergies, test results, and treatment plans, should be able to be captured by the EHR system.
- Patient Management: Processes for patient registration, admission, discharge, and transfer should be supported by the system. It should also make it possible to keep track of referrals, appointments, and patient interactions.
- Clinical Documentation: The development and administration of clinical documentation, such as progress notes, diagnosis reports, plans for treatment, and summary of discharge, ought to be made easier by the EHR system.
- Order Entry and Management: Electronic order entry and management for prescription drugs, lab tests, imaging studies, treatments, and referrals should be available to healthcare practitioners[9].
- Decision Support: To help healthcare providers make well-informed decisions about patient care, the system should include support for clinical decision features including alerts, warnings, and clinical guidelines.
- Interoperability: To ensure the smooth sharing of health data with different systems and organizations, the EHR system should embrace standards for interoperability such as HL7 FHIR (Fast Healthcare Interoperability Resources).
- Privacy and Security: To preserve the confidentiality, availability, and integrity of patient health information, the system should abide by privacy and security regulations such those outlined in HIPAA (Health Insurance Portability and Accountability Act).

Non-Functional Requirements:

- Performance: In order to support the demands of numerous users at once, the EHR system needs to be scalable and responsive. It should guarantee prompt access to patient information with less latency and downtime.
- Usability: Healthcare professionals should find it simple to navigate, enter data, and obtain information from the system with its intuitive workflow and user interface.
- Reliability: The EHR system must be dependable and always open to allow for constant access to patient medical records. It should be equipped with reliable disaster recovery and backup systems.
- Compliance: The system ought to adhere to industry norms and legal mandates that oversee electronic health records (EHRs), including Meaningful Use standards, HITECH (Health Information Technology for Economic and Clinical Health Act), and HIPAA.
- Data Integrity: Patient health information should be accurate, consistent, and comprehensive according to the system's procedures, which should include version control, audit trails, and data validation.
- Interoperability: To promote data interchange and interoperability, the EHR system should interact with medical equipment, other healthcare IT systems, and external data sources with ease.
- Security: Strong authorization, control of access, encryption, and auditing should all be implemented by the system to guard against cyberattacks, illegal access, and data breaches[10].

1.2. Traditional Electronic Health Record Systems

For the past few years, there have been boundaries in the level of care that health practitioners can provide due to the lack of complete and accurate health records data[11]. This paper overlooks non-electronic options and solely focuses on current Electronic Health Records (EHR). The EHR refers to a comprehensive digital record that includes a patient's physical examination, medical history, investigations, and treatment details. Each hospital has its own unique Record Management Software[12]. Some people opt for a company that provides cloud services, others prefer storing data within in their databases, and some choose to store data in a format that meets insurance agencies' requirements. The data usually stays on a server owned or leased by the hospital.

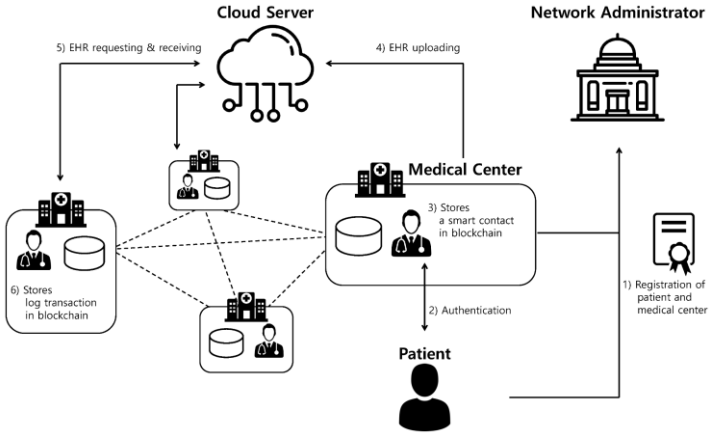


Fig.1. Existing EHR

1.3 Classification of Security Incidents in EHR

Classifying security incidents with a focus on electronic health records, or EHRs is essential to comprehending the various threats and vulnerabilities that may affect the availability, confidentiality, and integrity of patient health information[12]. The following categorization applies to security incidents in EHRs:

Unauthorized Access:

- Summary: Unapproved individuals are able to access patient health records without proper authorization.
- For instance: Healthcare staff inappropriately accessing patient records.
- External attackers are taking advantage of vulnerable authentication mechanisms to gain unauthorised access to EHR systems.

Data Breach: Description: The unfortunate occurrence of sensitive patient health information being disclosed to individuals or entities who are not authorised to access it.

- Instances: Hacking attacks aimed at EHR databases with the intention of pilfering patient records.
- Instances of unauthorised parties receiving leaked patient information by insiders.

Malware Infection:

- Description: EHR systems or devices are infiltrated by harmful software, which undermines their functionality and security.
- Instances: Ransomware attacks that encrypt EHR data and demand payment for decryption.
- Malicious software has been discovered that is designed to surreptitiously obtain login credentials for electronic health record (EHR) systems[13].

Phishing and Social Engineering:

- Explanation: Attackers employ cunning strategies to deceive individuals into revealing sensitive information or carrying out harmful actions.
- Instances: Phishing emails that mimic genuine organisations in order to deceive healthcare personnel into disclosing EHR login credentials[14].
- Social engineering attacks involve persuading employees to bypass security controls or disclose confidential information.

Insider Threats:

- Description: Individuals who are trusted within an organisation may misuse their access privileges, either intentionally or unintentionally, causing harm to the confidentiality, integrity, or availability of EHR data[15].
- Instances where employees improperly access patient records for their own benefit or out of personal curiosity.
- Careless actions resulting in unintentional removal or alteration of EHR data.

Denial of Service (DoS) Attacks:

- Attackers aim to disrupt the availability of EHR systems or services, hindering legitimate users from accessing patient information.
- Instances: EHR servers becoming unresponsive due to Distributed Denial of Service (DDoS) attacks flooding them with malicious traffic.
- Application-layer attacks can be a significant concern for EHR software, as they have the potential to overload server resources and negatively impact performance[16].

Concerning Data Integrity Compromise:

- Unauthorised modifications or alterations have been made to patient health records, which has compromised their accuracy and reliability.
- Instances of individuals without proper authorization altering patient records in order to hide medical mistakes or instances of malpractice[17].
- Manipulating EHR data to alter treatment plans or insurance claims.

Physical Security Breaches:

- Description: Unauthorised access or theft of physical devices that store EHR data, such as computers, laptops, or storage devices.
- Instances of laptops or mobile devices being stolen, which unfortunately may contain patient health information that is not encrypted.
- Preventing unauthorized individuals from gaining physical access to EHR server rooms or data centers is of utmost importance.

Through the classification of security incidents in EHRs, experts can delve into trends, pinpoint common attack vectors, and devise strategies to minimize risks and bolster the security of EHR systems[18]. This classification framework can provide valuable insights for the development of security policies, procedures, and technical controls to effectively safeguard patient health information.

1.4 Major Issues Arising from Existing Model

• The fragmentation of the patients' healthcare data. Patients transitioning between different healthcare providers often results in the misplacement of their previous medical records. The data has to be spread out among the different organizations. This leads to the fragmentation of the patient's medical information among different hospitals, medical apps, and other healthcare providers[19].

• Transferring medical records from one organization to another can be quite challenging. Patients may encounter difficulties accessing their health records, leading to the inconvenience of having to repeat tests at different organizations.

• Difficulty in accessing crucial information during emergencies.

• Data leaks from healthcare facilities that sell patient information to companies for their own gain.

• Hospital authorities are capable of manipulating data. Having access to health information of patients is limited[20].

2. Literature Review

Numerous research projects have delved into the utilization of blockchain technology in the healthcare sector, with a specific emphasis on enhancing the security of EHRs, managing patient consent effectively, and promoting interoperability among various healthcare entities. In addition, there have been research endeavors to utilize decentralized [21]storage solutions such as IPFS to tackle the scalability and privacy issues of conventional medical information management systems. Nevertheless, current methods frequently do not have a complete framework that combines blockchain and IPFS to offer full safety and confidentiality for EHRs[22].

Author	Title	Year	Publication	Paper Objective	Service	Advantage	Limitation
Smith et al.	Blockchain-based EHR System for Privacy and Security	2023	*Journal of Medical Informatics*	Proposes a blockchain framework for secure EHRs, ensuring data integrity and confidentiality.	Patient record management	Enhances data security and privacy	Scalability challenges
Gupta and Patel	Decentralized EHR Management Using Smart Contracts	2022	*International Conference on Health Informatics*	Introduces a smart contract-based approach to manage EHRs, reducing reliance on central authorities.	Access control and auditability	Efficient data sharing	Smart contract complexity
Verma, D.K. et al.	Blockchain-Based Secure Cloud Data Exchange for Electronic Health Records (EHRs) in the Covid-19 Scenario	2022	*Trends in Electronics and Health Informatics*	Addresses EHR security during the pandemic using blockchain.	Cloud-based EHR sharing	Pandemic-specific security	Cloud infrastructure limitations
Lee and Kim	Blockchain-Enabled Consent Management for EHRs	2021	*Healthcare Technology Letters*	Develops a consent management system using blockchain, allowing patients to control data access.	Consent management	Empowers patient autonomy	Limited adoption awareness

Kumar and Singh	Blockchain-Enhanced EHR Authentication and Authorization	2021	*International Journal of Computer Applications*	Enhances EHR security through blockchain-based authentication and authorization.	User access control	Improved security	Blockchain scalability
Chen et al.	Secure EHR Interoperability via Blockchain	2020	*IEEE Transactions on Biomedical Engineering*	Presents a blockchain-based solution for EHR interoperability across healthcare providers.	Data exchange between hospitals	Ensures data consistency	Integration challenges
Park et al.	Blockchain-Based EHR Integrity Verification	2020	*Journal of Medical Systems*	Verifies EHR integrity using blockchain, preventing unauthorized modifications.	Data integrity assurance	Tamper-proof records	Blockchain complexity
Wang and Zhang	Privacy-Preserving EHR Sharing with Blockchain	2019	*Journal of Healthcare Engineering*	Proposes a privacy-preserving EHR sharing mechanism using blockchain and zero-knowledge proofs.	Privacy preservation	Minimal trust required	Computational overhead
Li et al.	Blockchain-Driven EHR Sharing for Research Collaboration	2019	*Journal of Biomedical Informatics*	Facilitates secure EHR sharing among researchers using blockchain.	Collaborative research	Enhanced data availability	Privacy concerns
Singh and Gupta	Blockchain-Enabled EHR Audit Trail	2018	*Health Information Science and Systems*	Implements an audit trail for EHRs using blockchain, enhancing transparency.	Auditability	Accountability	Blockchain adoption challenges
Kim et al.	Blockchain-Based EHR Access Control Model	2017	*Healthcare Informatics Research*	Proposes an access control model for EHRs using blockchain technology.	Role-based access	Improved privacy	Implementation complexity

Table.1. Literature review of previous work.

3. Proposed Framework

Figure 2 shows a graphic depiction of the suggested framework for the health care chain. Information requests are sent from the Dapp to the fabric networks through the composer API, which is run by the Decentralised app development admin[23]. The Angular framework can access data within an on-chain database on the basis of the current state offered by the API by utilising the composer to make GET calls. The smart contract composer's primary goal is to use blockchain technology to create decentralised applications. Network participants can use chain codes, or smart contracts, to validate medical data submissions using the Hyperledger Fabric platform.

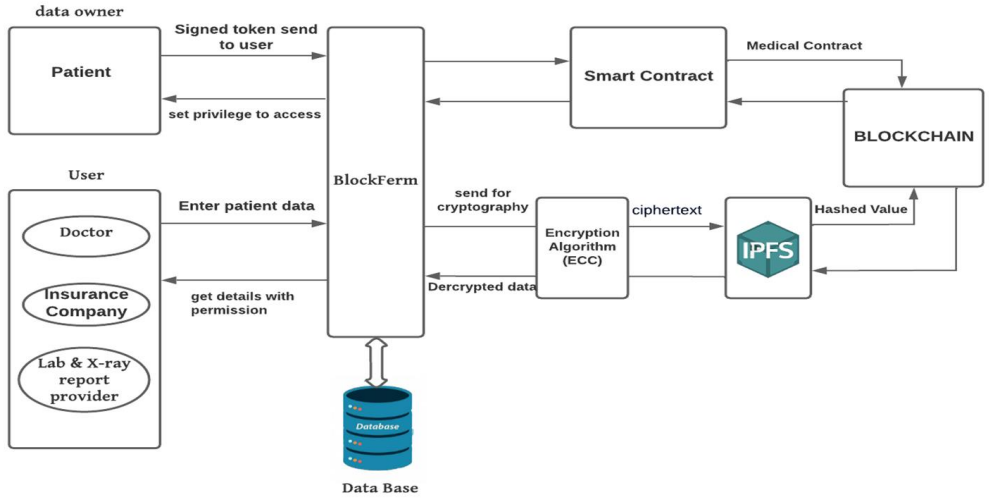


Figure 2. Framework Proposal [24]

It was decided to use this technology for decentralised database systems. Hyperledger is used to store health records, whereas Bitcoin was created for monetary transactions.

A blockchain with permissions driven by Hyperledger Fabric is part of the system architecture that allows web apps for individual organisations with 3 peer nodes to be created. Three peer nodes are used by the organisation; two serve as ordering nodes for registration of stakeholders and one as a verifying peer node. Different users of this system have access to IPFS, the pertinent database, which is used for decentralised storage of information. One way to verify the scalability of the system is to add more peers to different places on different machines[24]. Skilled contractors can use this framework for accessing and employing ledgers. Through the application's smart contracting mechanism, peer nodes that have connections update the ledger. Peer nodes Pn0, Pn1, and Pn2 are all three peer nodes in the organisation. These nodes each have copies of their smart contracts and their own ledger[25].

3.1. Components of the framework

Our multi-tier framework includes the following essential elements:

3.1.1 Exploring Blockchain-Based Health Record Security

- Blockchain technology is used to maintain the truthfulness and immutability of health information. Every transaction is securely connected to the one before it, forming an immutable chain of records[26].
- Smart Contracts: It regulate access control, enabling authorised parties to securely communicate with EHRs. These contracts establish specific rules and permissions[27].

3.1.2. Decentralised Storage Using IPFS

- IPFS offers a decentralized cloud storage solution known as InterPlanetary File System. The health information is encrypted, broken down, and distributed throughout the IPFS network to ensure both fault tolerance and redundancy of data.

3.1.3. Access Control Security

- Our framework emphasises patient confidentiality and authority in the architectural design. Patients provide access to their electronic health records using secure authentication methods[28].
- Emphasising Accountability and Transparency: Every access request and modification is securely recorded on the blockchain, ensuring transparency and accountability.

BlocFERM -SC

The doctor gets the patient's permission before accessing the patient's IPFS health record. As shown in figure 3, role-specific access control authorizations give the patient the ability to accept or reject requests from those who

are authorised. The doctor can create, record, and examine patient records when the patient gives permission. The patient wants to keep his record on file after the write operation[29]. The patient-centric health data for a given session can only be viewed by researchers, pharmacists, and insurance agents inside this framework if their object ID matches the owner's ID and the patient's information. A lab technician is permitted to amend the patient's medical record after receiving clearance from both the patient and the physician. Via a smart contract, the certificate authority provides policies, control of access, and protection agreements; all are managed by the Hyperledger Network fabric[30].

By changing the settings for privacy, an individual can control the privacy of their private information. Prior to being submitted to the medical record chain network, each level in our framework are configured to modify the circumstances during the transfer of privileges to another authorised user[31].

BlocFERM Algorithm

4. Implementation

Our EHR framework prototype has been developed using open-source blockchain technology platforms like Hyperledger Fabric[32], in addition to utilizing IPFS for decentralized storage. The prototype involves smart contracts for overseeing patient consent, medical professional access, and sharing information permissions. We performed performance evaluations to evaluate the scalability and effectiveness of our framework across different workload scenarios[33]. Moreover, security assessments were conducted to pinpoint and address potential vulnerabilities, guaranteeing strong protection against digital hazards and malicious activities. The system effectively showcased the following:

- **Ensuring Data Privacy:** Healthcare professionals securely accessed patient records with authorization.
- **Immutability:** Health records are secure and cannot be altered thanks to blockchain-based validation.
- **Decentralized Storage:** IPFS guarantees data availability even in the face of network disruptions[34].

4.1 Ensuring that authorized users have access

Patients grant stakeholders access to their medical records in a regulated setting, allowing them to view, amend, and limit access as needed. The ability to manage and limit access to one's medical information is provided to patients by the ability to decide who is permitted access[35]. Furthermore, according to the job type and permission type that have been mutually agreed upon by verified individuals, patients can authorise access to their medical records. Patients can opt out of having their medical records shared with other providers of healthcare by refusing to give specific doctors access to them. Smart contracts will respond to requests, validate them, update data, and grant access permissions whenever users interact with the system. The step-by-step procedure for putting role-based access control and privileges into place is shown in Figure 3[36].

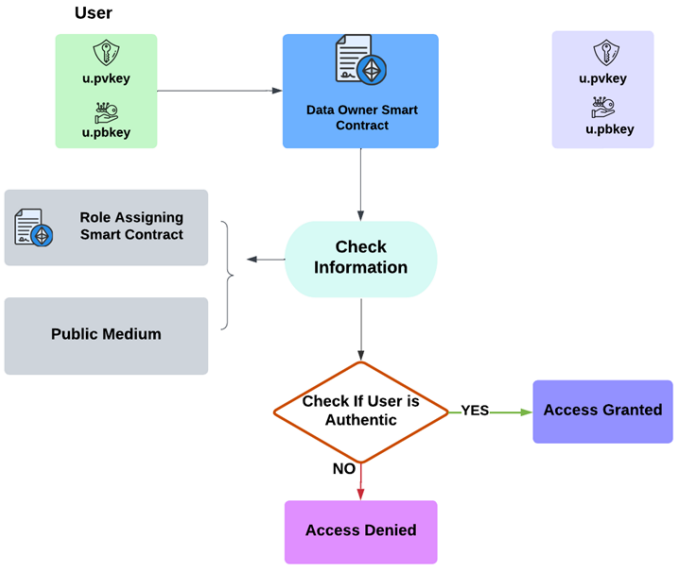


Figure 3. Access control with smart contract

Accessibility to the records, as illustrated in Fig. 3, is the responsibility of the data owners SC. When request has been made, the data owner examines the records that the role-assigning SC posts on a public medium, such as a database or website. The data owner verifies with the user that the role has been authorised and that the permissions have been assigned. The user's credentials are authenticated using the data from the role-assigning

SC[37]. A user can access the records if they can demonstrate their legitimacy. Nevertheless, if the user cannot be found in the role-assigning SC or does not meet the prerequisites, no privilege is awarded to them. The authority granted to the role to grant access to users can also be withdrawn by the resource owner.

4.2 Evaluating performance

Medical records, particularly medical imaging data, tend to be quite extensive. Storing information directly in the blockchain is not practical due to cost, space, and time constraints[38]. Therefore, the suggested system guarantees scalability by storing the encrypted data off-chain in IPFS and only storing the appropriate IPFS hash in the blockchain. To assess the system's performance and efficiency, we measured the time taken for retrieving the image files from IPFS. While bigger files typically begin loading in 5 to 7 seconds, the complete image may occasionally take up to 1 minute to appear on the screen[39]. The collected data has been depicted in a chart in Fig. 4. Based on the chart, it's clear that there is a direct relationship between file size and latency. Larger files result in longer retrieval times. On the other hand, retrieving the same files from IPFS for the second time is much faster due to IPFS caching the data locally after the initial delivery, which helps reduce latency. Either way, enhancements are necessary to efficiently retrieve larger files.

5. Results and Performance Analysis

A dataset retrieved from US health records, sourced from the Kaggle platform, encompassed a variety of images and texts of varying lengths. These health records were employed for testing objectives. The performance of a blockchain-based application was assessed using Hyperledger Caliper, a tool designed to gauge the efficiency of Hyperledger technology. Caliper conducts an analysis of multiple metrics, including throughput, latency, and success rates (averages, minimums, maximums, and percentiles). Additionally, it provides insights into resource allocation, such as CPU memory, within the system[40].

The following metrics are used to obtain the outcome from Hyperledger Calliper reporting benchmarks:

1. Success and failure rates.
2. Transaction and read throughput.
3. Metrics for read/transaction latency (min, max, avg, %ile).
4. Use of resources (CPU, memory, and network).

An essential component of the suggested application is scalability. By requesting services from various numbers of peers, the proposed architecture was put to the test. Initially, three peer nodes and one organisation were used to assess the network's performance. In order to compare peers among nodes and finally ascertain the efficiency of the system, the benchmark report was helpful.

The initial study measured transaction latency using a Hyperledger fabric[41]. The latency of a transaction can be determined by measuring how long it takes to complete. It is dispersed throughout the network's nodes. The health chain network's transaction latency may be computed when there are n nodes by using TrLn, TrCtn, and TrStn, where TrLn denotes the transaction latency, TrCtn the network nodes' confirmation time, and TrStn the transaction submission time in seconds. The link between TrLn, TrRCtn, and TrStn is depicted in Equation 1.

$$TrLn = TrCtn - TrStn \quad (1)$$

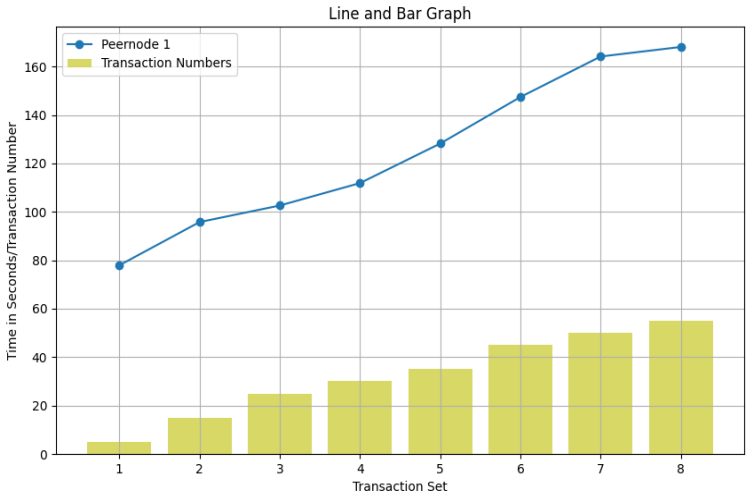
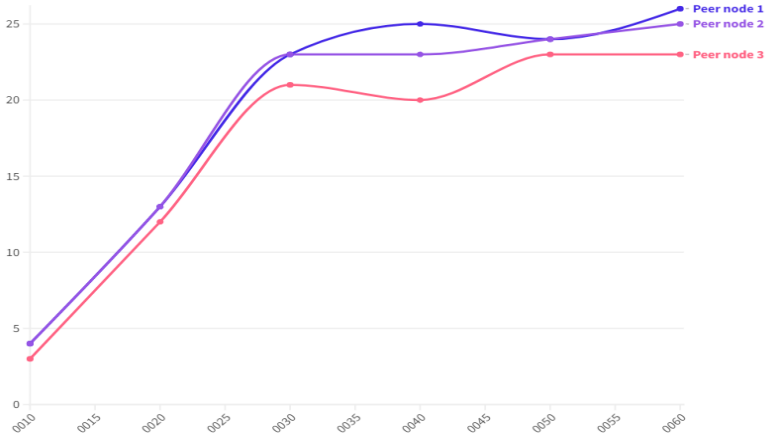


Figure 4. Latency of organization peer nodes for sample set of Transactions.

The network ledger has been refreshed with eight batches of transactions within the organization, with peer node1 processing transactions valued between 5 and 55, as shown in Figure 15. According to the configuration, the first five transactions were handled within 101 seconds, while the subsequent 55 transactions took an average of 160 seconds. To determine transaction time, additional transactions ranging from 55 to 400 were included in the experimental outcome[42].

In Figure (Throughput comparative analysis with 1 org), it is evident that the transaction success rate is greater for the peer node of organization 1 compared to those of organization 2 and organization 3.



Once assets are loaded and written into a database, the system evaluates the latency of these assets. In a blockchain network comprising n nodes, As_Ln represents the Asset Latency. The response time, TrRsn, is quantified in milliseconds, while the asset submission time, Tr_As_Sn, is also measured in milliseconds[43].

$$As\_Ln = TrRsn - Tr\_As\_Sn. \quad (2)$$

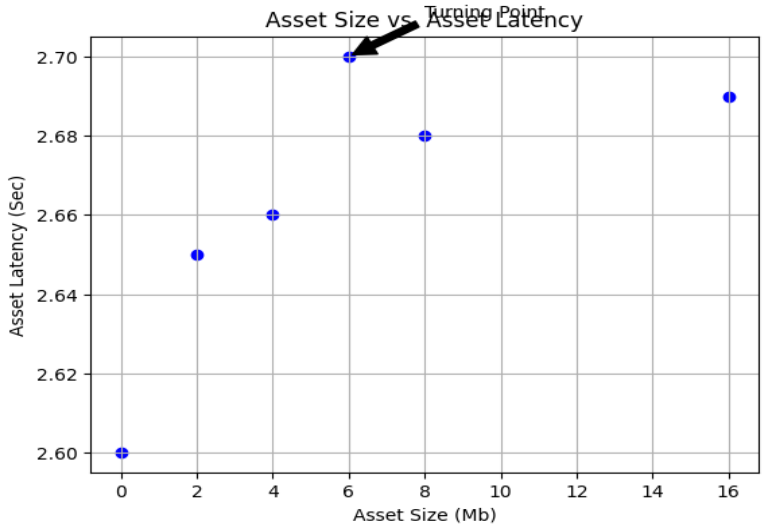


Figure 5. Average time taken for asset submission and response.

Figure 5 illustrates the duration required for assets to be recorded in the blockchain utilizing a sample collection of transactions. As a result, the system exhibits the ability to manage substantial data volumes with negligible latency[44]. To scrutinize the variability in asset latency, the investigation was broadened to encompass a spectrum of user counts spanning from 20 to 120, along with data sizes ranging from 200 k bytes to 20,574 k bytes.

Conclusion and Future Directions

Presented in this paper is a new framework for enhancing the security of Electronic Health Records through the utilization of blockchain and IPFS technologies. Our framework tackles important security and privacy issues in EHR systems by utilizing the immutability and transparency of blockchain, along with the decentralized storage capabilities of IPFS. By implementing a proof-of-concept and evaluating performance, we have shown the practicality and success of our method in improving the security and integrity of EHR data. For upcoming projects, we aim to improve our framework by delving into advanced cryptographic methods, maximizing resource

efficiency, and incorporating new healthcare interoperability and data exchange standards. Our multi-tier framework provides a promising solution for improving EHR security, privacy, and accessibility. Future tasks include conducting scalability testing, ensuring interoperability with current systems, and incorporating user feedback to enhance the implementation.

ACKNOWLEDGMENT

This work is acknowledged under Integral University manuscript No. IU/R&D/2024-MCN0002628.

Reference

[1] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-Less Medical Data Sharing among Cloud Service Providers via Blockchain," *IEEE Access*, vol. 5, pp. 14757–14767, Jul. 2017, doi: 10.1109/ACCESS.2017.2730843.

[2] S. Athanere and R. Thakur, "Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 4, pp. 1523–1534, Apr. 2022, doi: 10.1016/j.jksuci.2022.01.019.

[3] E. Balistri, F. Casellato, C. Giannelli, and C. Stefanelli, "BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten," *ICT Express*, vol. 7, no. 3, pp. 308–315, Sep. 2021, doi: 10.1016/j.icte.2021.08.006.

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

[5] E. Daraghmi, Y. Daraghmi, and S. Yuan, "MedChain : A Design of Blockchain-Based System for Medical Records Access and Permissions Management," *IEEE Access*, vol. 7, pp. 164595–164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

[6] L. Hang, E. Choi, and D. H. Kim, "A novel EMR integrity management based on a medical blockchain platform in hospital," *Electron.*, vol. 8, no. 4, Apr. 2019, doi: 10.3390/electronics8040467.

[7] S. M. Pournaghi, M. Bayat, and Y. Farjami, "MedSBA: a novel and secure scheme to share medical data based on blockchain technology and attribute-based encryption," *J. Ambient Intell. Humaniz. Comput.*, vol. 11, no. 11, pp. 4613–4641, Nov. 2020, doi: 10.1007/s12652-020-01710-y.

[8] M. F. Farooqui, M. Muqeem, S. Ahmad, J. Nazeer, and H. A. M. Abdeljaber, "A Fuzzy Logic based Solution for Network Traffic Problems in Migrating Parallel Crawlers," no. March, 2023, doi: 10.14569/IJACSA.2023.0140252.

[9] M. Sultana, A. Hossain, F. Laila, K. A. Taher, and M. N. Islam, "Towards developing a secure medical image sharing system based on zero trust principles and blockchain technology," *BMC Med. Inform. Decis. Mak.*, vol. 20, no. 1, Oct. 2020, doi: 10.1186/s12911-020-01275-y.

[10] O. Ajayi, M. Abouali, and T. Saadawi, "Secure architecture for inter-healthcare electronic health records exchange," Sep. 2020, doi: 10.1109/IEMTRONICS51293.2020.9216336.

[11] M. Faisal, H. Sadia, T. Ahmed, and N. Javed, *Blockchain Technology for Healthcare*, no. November 2021. 2022.

[12] O. For and R. With, "A N E XTENDED M ODEL FOR E FFECTIVE M IGRATING P ARALLEL W EB C RAWLING WITH," vol. 3, no. 3, pp. 85–93, 2012.

[13] M. D. Praveen, S. G. Totad, M. Rashinkar, R. Ostwal, S. Patil, and P. M. Hadapad, "Scalable Blockchain Architecture using off-chain IPFS for Marks Card Validation," *Procedia Comput. Sci.*, vol. 215, pp. 370–379, 2022, doi: 10.1016/j.procs.2022.12.039.

[14] R. M. Parizi, S. Homayoun, A. Yazdinejad, A. Dehghantanha, and K. K. R. Choo, "Integrating Privacy Enhancing Techniques into Blockchains Using Sidechains," May 2019, doi: 10.1109/CCECE.2019.8861821.

[15] Z. Ying, L. Wei, Q. Li, X. Liu, and J. Cui, "A Lightweight Policy Preserving EHR Sharing Scheme in the Cloud," *IEEE Access*, vol. 6, pp. 53698–53708, 2018, doi: 10.1109/ACCESS.2018.2871170.

[16] R. Charanya, R. A. K. Saravanaguru, and M. Aramudhan, "Sefra: A secure framework to manage ehealth records using blockchain technology," *Int. J. E-Health Med. Commun.*, vol. 11, no. 1, pp. 1–16, Jan. 2020, doi: 10.4018/IJEHMC.2020010101.

[17] A. Gharat, P. Aher, P. Chaudhari, and B. Alte, "A Framework for Secure Storage and Sharing of Electronic Health Records using Blockchain Technology," *ITM Web Conf.*, vol. 40, p. 03037, 2021, doi: 10.1051/itmconf/20214003037.

[18] M. M. Sheeraz, M. A. I. Mozumder, M. O. Khan, M. U. Abid, M. I. Joo, and H. C. Kim, "Blockchain System for Trustless Healthcare Data Sharing with Hyperledger Fabric in Action," in *International Conference on Advanced Communication Technology, ICACT*, 2023, vol. 2023-February, pp. 437–440, doi: 10.23919/ICACT56868.2023.10079423.

[19] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications, PIMRC*, Feb. 2018, vol. 2017-Octob, pp. 1–5, doi: 10.1109/PIMRC.2017.8292361.

[20] E. K. Christiansen, E. Skipenes, M. F. Hausken, S. Skeie, T. Østbye, and M. M. Iversen, "Shared Electronic Health Record Systems: Key Legal and Security Challenges," *J. Diabetes Sci. Technol.*, vol. 11, no. 6, pp. 1234–1239, 2017, doi: 10.1177/1932296817709797.
[21] N. Javed, "BLOCKCHAIN : NEXT-FRONTIER IN CLOU COMPUTING TECHNOLOGY," no. July, 2022.
[22] H. S. Jennath, V. S. Anoop, and S. Asharaf, "Blockchain for Healthcare: Securing Patient Data and Enabling Trusted Artificial Intelligence," *Int. J. Interact. Multimed. Artif. Intell.*, vol. 6, no. 3, p. 15, 2020, doi: 10.9781/ijimai.2020.07.002.
[23] P. Kamboj, S. Khare, and S. Pal, "User authentication using Blockchain based smart contract in role-based access control," *Peer-to-Peer Netw. Appl.*, vol. 14, no. 5, pp. 2961–2976, 2021, doi: 10.1007/s12083-021-01150-1.
[24] Abida Khanam, M. F. Farooqui, "Enhancing the Security and Privacy of eHealth Records through Blockchain-based Management: A Comprehensive Framework," *Int. J. Recent Innov. Trends Comput. Commun.*, vol. 11, no. 9, pp. 450–456, 2023, doi: 10.17762/ijritcc.v11i9.8827.
[25] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," in *Proceedings - 2016 2nd International Conference on Open and Big Data, OBD 2016*, Sep. 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.
[26] R. Akkaoui, X. Hei, and W. Cheng, "EdgeMediChain: A Hybrid Edge Blockchain-Based Framework for Health Data Exchange," *IEEE Access*, vol. 8, pp. 113467–113486, 2020, doi: 10.1109/ACCESS.2020.3003575.
[27] Y. Zhang, S. Kasahara, Y. Shen, X. Jiang, and J. Wan, "Smart contract-based access control for the internet of things," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1594–1605, 2019, doi: 10.1109/JIOT.2018.2847705.
[28] M. M. Madine *et al.*, "Blockchain for Giving Patients Control over Their Medical Records," *IEEE Access*, vol. 8, no. October, pp. 193102–193115, 2020, doi: 10.1109/ACCESS.2020.3032553.
[29] A. Saini, Q. Zhu, N. Singh, Y. Xiang, L. Gao, and Y. Zhang, "A smart-contract-based access control framework for cloud smart healthcare system," *IEEE Internet Things J.*, vol. 8, no. 7, pp. 5914–5925, 2021, doi: 10.1109/JIOT.2020.3032997.
[30] A. I. Taloba, A. Rayan, A. Elhadad, A. Abozeid, O. R. Shahin, and R. M. A. El-Aziz, "A Framework for Secure Healthcare Data Management using Blockchain Technology," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 12, pp. 639–646, 2021, doi: 10.14569/IJACSA.2021.0121280.
[31] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, vol. 22, no. 2, pp. 177–183, 2021, doi: 10.1016/j.eij.2020.07.003.
[32] S. Srivastava, T. Ahmed, and A. Saxena, "an Approach To Secure Iot Applications of Smart City Using Blockchain Technology," *Int. J. Eng. Sci. Emerg. Technol.*, vol. 11, no. 2, pp. 71–78, 2023, [Online]. Available: https://www.researchgate.net/publication/375060152.
[33] N. Al Asad, M. T. Elahi, A. Al Hasan, and M. A. Yousuf, "Permission-based blockchain with proof of authority for secured healthcare data sharing," *2020 2nd Int. Conf. Adv. Inf. Commun. Technol. ICAICT 2020*, no. November, pp. 35–40, 2020, doi: 10.1109/ICAICT51780.2020.9333488.
[34] A. I. Mendoza Arvizo, L. Avelar Sosa, J. L. García Alcaraz, and O. Cruz-Mejía, "Beneficiary Contracts on a Lightweight Blockchain Architecture Using Smart Contracts: A Smart Healthcare System for Medical Records," *Appl. Sci.*, vol. 13, no. 11, 2023, doi: 10.3390/app13116694.
[35] R. Bayer, J. Santelli, and R. Klitzman, "New challenges for electronic health records confidentiality and access to sensitive health information about parents and adolescents," *JAMA - J. Am. Med. Assoc.*, vol. 313, no. 1, pp. 29–30, 2015, doi: 10.1001/jama.2014.15391.
[36] 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.
[37] T. Dey, S. Jaiswal, S. Sunderkrishnan, and N. Katre, "HealthSense: A medical use case of Internet of Things and blockchain," *Proc. Int. Conf. Intell. Sustain. Syst. ICISS 2017*, no. Iciss, pp. 486–491, 2018, doi: 10.1109/ISS1.2017.8389459.
[38] S. Wang *et al.*, "Blockchain-Powered Parallel Healthcare Systems Based on the ACP Approach," *IEEE Trans. Comput. Soc. Syst.*, vol. 5, no. 4, pp. 942–950, 2018, doi: 10.1109/TCSS.2018.2865526.
[39] M. M. M. Pai, R. Ganiga, R. M. Pai, and R. K. Sinha, "Standard electronic health record (EHR) framework for Indian healthcare system," *Heal. Serv. Outcomes Res. Methodol.*, vol. 21, no. 3, pp. 339–362, 2021, doi: 10.1007/s10742-020-00238-0.
[40] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Inform.*, vol. 92, no. October 2018, p. 103140, 2019, doi: 10.1016/j.jbi.2019.103140.
[41] D. A. M. Budida and R. S. Mangrulkar, "Design and implementation of smart HealthCare system using IoT," *Proc. 2017 Int. Conf. Innov. Information, Embed. Commun. Syst. ICIIECS 2017*, vol. 2018-Janua, pp. 1–7,

2018, doi: 10.1109/ICIIECS.2017.8275903.
[42] A. Roehrs, C. A. da Costa, R. da Rosa Righi, V. F. da Silva, J. R. Goldim, and D. C. Schmidt, "Analyzing the performance of a blockchain-based personal health record implementation," *J. Biomed. Inform.*, vol. 92, no. March, p. 103140, 2019, doi: 10.1016/j.jbi.2019.103140.
[43] A. Hossain, R. Quaresma, and H. Rahman, "Investigating factors influencing the physicians' adoption of electronic health record (EHR) in healthcare system of Bangladesh: An empirical study," *Int. J. Inf. Manage.*, vol. 44, no. September 2018, pp. 76–87, 2019, doi: 10.1016/j.ijinfomgt.2018.09.016.
[44] S. Amofa *et al.*, "A blockchain-based architecture framework for secure sharing of personal health data," *2018 IEEE 20th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2018*, pp. 1–6, 2018, doi: 10.1109/HealthCom.2018.8531160.