

Blockchain Technology for Secure Healthcare Data management with Patient Empowerment

MSc Research Project
MSc Cyber Security

Sidhant Patil
Student ID: x23128577

School of Computing
National College of Ireland

Supervisor: Prof Liam McCabe

National College of Ireland
Project Submission Sheet
School of Computing



Student Name:	Sidhant Patil
Student ID:	x23128577
Programme:	MSc Cyber Security
Year:	2024
Module:	MSc Research Project
Supervisor:	Prof Liam McCabe
Submission Due Date:	12/12/2024
Project Title:	Blockchain Technology for Secure Healthcare Data management with Patient Empowerment
Word Count:	6744
Page Count:	23

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	
Date:	25th January 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).	<input type="checkbox"/>
Attach a Moodle submission receipt of the online project submission , to each project (including multiple copies).	<input type="checkbox"/>
You must ensure that you retain a HARD COPY of the project , both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	<input type="checkbox"/>

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Blockchain Technology for Secure Healthcare Data management with Patient Empowerment

Sidhant Patil
x23128577

Contents

1	Introduction	1
1.1	Background and Problem Definition	2
1.2	Research Question and Objectives	3
1.3	Structure of the report	3
2	Literature Review	4
2.1	Blockchain's Role in Enhancing EHR Systems	4
2.2	Privacy and Security in Blockchain-Based EHRs	4
2.3	Advances in System Design and Automation	4
2.4	Patient-Centric and Lightweight Blockchain Systems	5
2.5	Reviews and Roadmaps	5
3	Research Methodology	6
3.1	Requirement Analysis	7
3.1.1	Stakeholder Analysis	7
3.1.2	Gap Identification	7
3.1.3	Outcome	7
3.2	System design	7
3.3	Implementation	9
3.4	Testing and validation	10
3.5	Ethical Consideration	10
3.6	Tools and Technology	11
4	Implementation	11
4.1	Justification of tools and technologies used	11
4.2	Smart Contract Development	12
4.3	Data Storage and Encryption	12
4.4	UI Development	12
4.5	Work Flow Implementation	13
5	Results and Critical Analysis	14
5.1	Testing	14
5.2	Validation	16
5.3	Comparison with Existing Solutions	17
5.4	Healthcare Use Cases	18

6	Discussion	18
6.1	Implications for the Healthcare Industry	18
6.2	Limitations	19
6.3	Ethical Consideration	20
7	Conclusion and Future Work	20

List of Figures

1	Research Methodology	6
2	Architecture Diagram	8
3	Use Case Diagram	9
4	Verification of contracts deployment	14
5	Transaction Verification	14
6	Encryption Verification on IPFS	15
7	Vulnerability Assessment	15
8	Encryption verification on WireShark	15
9	IPFS Bandwith While Data Transfer	16
10	Postman Test	16
11	Apache Jmeter	17

Abstract

Electronic Health Records (EHR) are the health information stored digitally. These systems contains critical information about patient health. The research addresses the challenges faced by EHR systems such as centralized server vulnerabilities, single point of failures, and limited patient control over data by using Ethereum smart contracts. The system uses blockchains decentralized and immutable nature with AES-256 encryption protocol to enhance data security and integrity. InterPlanetary File System (IPFS) to store large data into a off-chain decentralized network. Patient empowerment through role-based user friendly dashboard provides patients control over their data and access permissions. The testing validated enhancements in security, integrity, and patient control over data. while the scalability and efficiency of system remains a challenge for large healthcare environment. Using a permissioned blockchain to improve efficiency is a suggested improvement. This research provides a practical approach to secure, patient-centric management system to improve overall quality of care within healthcare environment.

1 Introduction

Healthcare systems are one of those complex environments that have gone through significant transformation because of digitalization and data driven technologies. Electronic Health Records (EHR) systems is the core component of these systems. It stores patient information such as medical history, test results, treatment plans and prescriptions. These systems are responsible for improving the healthcare services. It helps in informed decision making by providing easy data access to the healthcare providers. However, these systems are vulnerable to single point of failure, data breaches, provides limited patient control over their data. Such vulnerabilities costs trust, privacy and safety of the

patient. In 2023 there were about 725 healthcare data breached which involved more than 500 records marking as the worst year for such incidents. Also, between the years from 2010 to 2022 cyber-attacks on healthcare escalated, exposing around 385 million medical records. according to a research by (Bischoff; 2024) an average cost for a downtime to a healthcare organization caused due to attacks is estimated at 15.5 million in 2023 (Dive; 2023), (Alder; 2024).

Blockchain technology provides some innovative solutions to address these challenges by using its decentralized framework where no single entity has control over data and the stored data is immutable and tamperproof. Blockchain is known for its applications in financial transaction and also provides a use case in healthcare for creating a secure, decentralized, patient centric systems. Such systems can provide data security, patient control over their data and secure sharing of the information. The decentralized nature improves security and privacy making it a practical solution of managing EHR. This research explores the application of blockchain to improve security of the EHR systems. The objective is to create a system which is secure, scalable and allows patient to share information securely with the healthcare providers. By using the properties of the blockchain to address the vulnerabilities faced by traditional EHR systems and propose a framework that validates patient privacy and data integrity.(OnChain; 2024) (Shahnaz et al.; 2019).

1.1 Background and Problem Definition

Electronic Health Records (EHR) in modern healthcare, provides a digital platform to manage medical records which improves data accessibility and decision making. Such systems can face multiple challenges compromising the effectiveness and reliability of the systems.

- **Security Vulnerabilities:** In 2023, healthcare organizations faced around 744 data breaches affecting more than 500 individuals and exposed over 133 million records. Centralized EHR systems can be vulnerable to data breaches, unwanted access and cyber threats. (Alder; 2024)
- **Interoperability Challenges:** Healthcare providers mostly use isolated system limiting data sharing and compatibility this can cause treatment delays and overall quality of care. Around 32% of patient have faced issues due to insufficient interoperability between the systems.(Telychko; 2024)
- **Limited Patient Control:** Patients having limited control over their data can create trust issue on healthcare systems. Traditional EHR systems usually limit patients' ability for managing permissions to their records which increases concerns with consent and privacy. (de Carvalho Junior and Bandiera-Paiva; 2020)
- **Data Integrity and Scalability Issues:** Storing the medical records while maintaining accuracy and consistency is difficult in the systems with multiple users involved. Traditional system may struggle to scale the data effectively as the volume grows and can be vulnerable to data manipulation. (Medicine; 2022)

Blockchain technology provides a solution to address these challenges by using its decentralized architecture and immutability healthcare data can remain tamperproof and stored securely. By using smart contracts and cryptographic security blockchain can improve

interoperability and patient control over the data. This approach addresses discussed vulnerabilities and provides more secure patient centric healthcare systems. (Reegu et al.; 2023) (OnChain; 2024)

1.2 Research Question and Objectives

Research Question: *"Can the implementation of Ethereum smart contracts be used to enhance the cryptographic security, confidentiality, and patient control over medical records?"*

The objective of this research aims to address the problems faced by EHR systems by using Ethereum blockchain technology to develop a secure, patient centric platform to share medical records to healthcare providers. The objective is to align with the healthcare priorities, patient empowerment and data privacy. (OnChain; 2024)

1. **Security:** Data security is top priority as healthcare breaches are more common as highlighted in studies (Alder; 2024) Decentralized and immutable nature of blockchain prevents data manipulation and maintains integrity of the data. Using the cryptographic protocols like AES-256 for encryption of the sensitive medical records. (Arunkumar and Kousalya; 2020)
2. **Interoperability:** Developing APIs for data sharing between multiple user roles as patient, doctor and pharmacists. Blockchain allows standardized data exchange to improve system compatibility.
3. **Empower Patients:** Providing patients control over their data. By Designing role-based dashboard for patient to interact and manage access to their data easily. (Esmaeilzadeh; 2022)
4. **Ensure Scalability:** Blockchain application often face scalability challenges. By using a off-chain storage like Interplanetary file system (IPFS) to store large files reduces the load on-chain so the system can handle high volume of transaction data. (Vidap et al.; 2023)
5. **Minimize Costs:** To ensure the systems adoption widely the system should be cost effective. Optimizing smart contracts gas consumption can reduce the transaction fees and the storage cost can be reduced by using a off-chain decentralized storage. (Nguyen; 2023)

1.3 Structure of the report

The report structure provides a overview of the research starting with Abstract that outlines the overview of the research. Followed by the introduction section to provide background, problem definition and objectives. Next is the literature review exploring blockchains role in improving EHR systems. followed by the research methodology to address the stakeholder needs, gaps, outcomes and Ethical consideration with system design outlining the architecture and use case diagram of the system. The implementation and the testing and validation section in methodology outlines methodological plan of implementation, testing and validation of the system. The tools and technology provides the list of tools required for the development. The implementation section guides through each step starting with justification of tools, smart contract development, Data storage

an encryption, User Interface Development and workflow implementation. Followed by results and critical analysis outlining the testing, validation, comparison with existing solution and healthcare use cases. the discussion section next describes the implication, findings, limitation and ethical consideration. concluding the report with conclusion, future works and references

2 Literature Review

2.1 Blockchain's Role in Enhancing EHR Systems

(Han et al.; 2022) investigates blockchains ability of transforming the EHR systems. Using the decentralized environment for data storage and exchange between the healthcare providers. The research highlights how blockchain can provide standard data exchange protocol to reduce data silos and dependency on the centralized systems. Key findings of the research is trust mechanism as the users are often unable to adopt decentralized models due lack of trust. It also emphasizes the computational inefficiency can cause scalability issues in blockchain environment. The research elaborates the lack of trust and importance of the blockchain based decentralized environment. The research aims to overcome the transaction efficiency by using multiple optimized smart contracts. and access control to maintain trust.

Shrestha and Panta (2023) proposed a decentralized EHR system using Ethereum blockchain and smart contracts to allow patient controlled sharing of data. The framework proposed included MetaMask for authentication of a user and ganache for smart contract testing. using the system a patient can grant and revoke access to the medical records which enhanced data ownership the authors showed increase in data security and integrity highlighting the potential of Ethereum blockchain in healthcare environment but the high energy consumption and slow speed of transaction limits the scalability for large scale deployment the findings are consistent with the project objectives of developing a patient centric EHR system using Ethereum blockchain and addressing the limitations by IPFS for storing Large medical records with reduced gas fees.

2.2 Privacy and Security in Blockchain-Based EHRs

(Sharma and Balamurugan; 2020) had a objective for privacy and security of EHR systems by using the combination of blockchain and advance cryptographic techniques in the proposed framework. It values immutability and confidentiality of the patient records from unauthorized access and tempering. The authors also considers secure data sharing mechanism between the healthcare providers highlighting the blockchains ability to maintain the integrity of the data. The limitations identified in the system was scalability of the system in handling large scale of healthcare data. The research aligns with the objective of securing the sensitive data using blockchain immutability and encryption protocol the limitations identified can be addressed using off-chain storage for storing large data.

2.3 Advances in System Design and Automation

(Chelladurai and Pandian; 2021) proposed EHR systems based on blockchain that uses modified Merkle trees for data access and storage. A Merkel tree is widely used cryp-

tographic data structure technique in blockchain. It organizes the data into tree like structure where every leaf node contains the hash of data block. parent node store the hash of their respective child node combining recursively until the single root hash is produce. modifying the tree by using it for managing records in each block. the merkel root summarizes records in the block and the leaf node represents the hash. 64bit SHA-256 hashing as it generates fixed hash which also helps in verifying integrity. this approach provided reduced latency in retrieval of the records with maintained integrity making it suitable for quick access to accurate medical records. The system is tested and validated showing improved performance, lower latency, secure uploading and retrieval of the records however the system was not validated on large scale network and did not provide interoperability within healthcare providers. The limitation of the project allow to improve the model by implementing scalable framework with interoperability features for real world implication. (Vidap et al.; 2023) developed a EHR system based on permissioned blockchain using the Hyperledger fabric the system highlights the importance of interoperability between the healthcare providers. The architecture of the system is modular and allows easy integration with multiple healthcare system for secure data transfer. The research addresses the Hyperledger fabric for lower latency and energy efficient transaction as compare to the Ethereum blockchain. The system caused difficulties in integrating with multiple systems with different data formats highlighting the need of standardized protocols. The research aims for creating interoperable and scalable system using API based communication to address the integration issues.

2.4 Patient-Centric and Lightweight Blockchain Systems

(Sonkamble et al.; 2023) proposed a patient centered blockchain system that uses smart contract for selective data sharing which allowed patients to dynamically grant and revoke access to the medical records this approach addresses limitations of the EHR system by prioritized patient control and data confidentiality the system faced challenges in handling large volume of increasing medical records. To address these challenges the research propose use of scalable solution such by using off-chain storage which can create a secure data management without affecting the performance of the system the research objective aligns with the project goals to provide patient with secure and efficient management of health records. (Arunkumar and Kousalya; 2020) proposed a lightweight blockchain system that is able to transfer and store the records using AES-256-GCM encryption with minimized computational resources making it suitable for small clinic with limited resources. The system improve energy efficiency but was not evaluated in large scale environment where scalability and interoperability is important. The project proposed fill the gaps by utilizing interoperability for data sharing between the healthcare to expand the architecture of the system to handle large data across multiple healthcare providers.

2.5 Reviews and Roadmaps

(Mamun et al.; 2022) provides a detailed review of blockchain use cases in EHR systems and identifying solution into theoretical, design, development and implementation. The analysis discovered important challenges like scalability, energy consumption and interoperability in the system and find recommendations to address the challenges identified. The critical analysis of these system is useful for the research project to identify the area that requires attention like need of scalable and energy efficient blockchain solutions.

(Karmakar et al.; 2023) provides a review on blockchain potential to secure EHR system highlighting the importance of compliance with regulations, workflow and interoperability within the healthcare environment. (Shaik et al.; 2023) suggests the effectiveness of the permissioned based blockchain network such as Hyperledger fabric for EHR systems in managing the real world complexities and volume of data. This includes secure data sharing and collaboration with multiple healthcare providers the study evaluates the practicality of the application to handle scalability and data integrity within the system the findings support the project implementation objectives and system design.

The Literature reviewed highlights the possibilities and use cases of blockchain technology to address challenges in Electronic Health Records EHR management including decentralization, privacy, security, scalability and patient control over medical records (Han et al.; 2022) and (Shrestha and Panta; 2023). study the ability of blockchain to improve interoperability and patient empowerment this aligns with the project objectives. Research on privacy and security mentioned in (Sharma and Balamurugan; 2020) highlighting the importance of strong cryptographic protocols and access control which are important for the proposed system. (Chelladurai and Pandian; 2021) and (Vidap et al.; 2023) contributes in automation and the design of the system that provides the need of scalable architecture to improve performance. (Sonkamble et al.; 2023) provide a strategy for patient centric design that values accessibility and security of the medical records while (Mamun et al.; 2022) and (Karmakar et al.; 2023) verify the gaps such as interoperability, energy efficiency of the transactions and standardization The results support the proposed research which uses a Blockchain architecture to develop EHR management system prioritizing patient control over the data with security to upload and retrieve records. by addressing the gaps in the project aims to create a practical solution for adopting the blockchain technology for securing the health records.

3 Research Methodology

The methodology is divided into four phases of software development. Requirement analysis, system design, Implementation and testing and validation. Each phase is explained for understanding development of the project. The Ehtereum blockchain is simulated using Ganache for secure and decentralized environment. Smart contract developed using solidity language and deployed using truffle, decentralized off-chain storage is integrated using InterPlanetary File System IPFS and Role based interfaces developed in VS code using react.js. The objective is to improve the data privacy and security via strong encryption and access control empowering patient with full control over the data. This approach complies to the ethical standards such as GDPR and uses synthetic data for preventing patient confidentiality while testing the application.



Figure 1: Research Methodology

3.1 Requirement Analysis

The technical and functional requirements for the system is defined in this phase. By analyzing the needs of stakeholder within healthcare environment.

3.1.1 Stakeholder Analysis

- **Patients:** Needs a private and secure access to the records with access control to grant or revoke permissions to the records. Blockchain features smart contracts to manage access control for patients so only authorized users can view the data. Esmaeilzadeh (2022)
- **Doctors:** Needs access to the authorized medical records of patient for accurate and effective treatment. Immutable nature of blockchain provide doctors reliable patient records and history maintaining the data integrity. Schmeelk et al. (2022)
- **Pharmacist:** Needs a mechanism to verify the integrity of the prescription with doctor and ensure correct medication to the patient. Transactions logs and verification from doctor provides prescription authentication for pharmacist. Esmaeilzadeh (2022)

3.1.2 Gap Identification

Centralized EHR systems are vulnerable to server breaches and single point of failures causing data loss and attracting cyber threats. With limited transparency and control over data patients can lose trust over healthcare systems. These systems are more scalable in handling large data volume and provides easier integration with existing system. Integration of Blockchain improves security through decentralized environment, provides patient control over their data and transparency through transaction records. The improved security consumes high energy due to the Proof of Work (PoW) consensus mechanism. Banerjee et al. (2024), Jercich (2022), Poteet et al. (2024).

3.1.3 Outcome

A EHR system that uses Ethereum blockchain for data storage and sharing. Manage permissions for patients, doctors and pharmacist using smart contract. Supporting secure data exchange across multiple users and handle data volumes efficiently. Implementation example, A user friendly interface linked to smart contract for patient to grant or revoke access to medical records. Doctor is updated with the access to records for accurate treatment. Pharmacist can verify the prescription shared by the patient with doctor for proper medication. Implementing these features to the system can improve data security, patient privacy, interoperability and trust in healthcare system.

3.2 System design

A technical Architecture based on the requirement analyzed is discussed design phase to ensure security, scalability and interoperability within the system. objective here is to develop a architecture using Ethereum blockchain, decentralized storage such as InterPlanetary file system IPFS and secure interfaces for each user to upload and share the medical records.

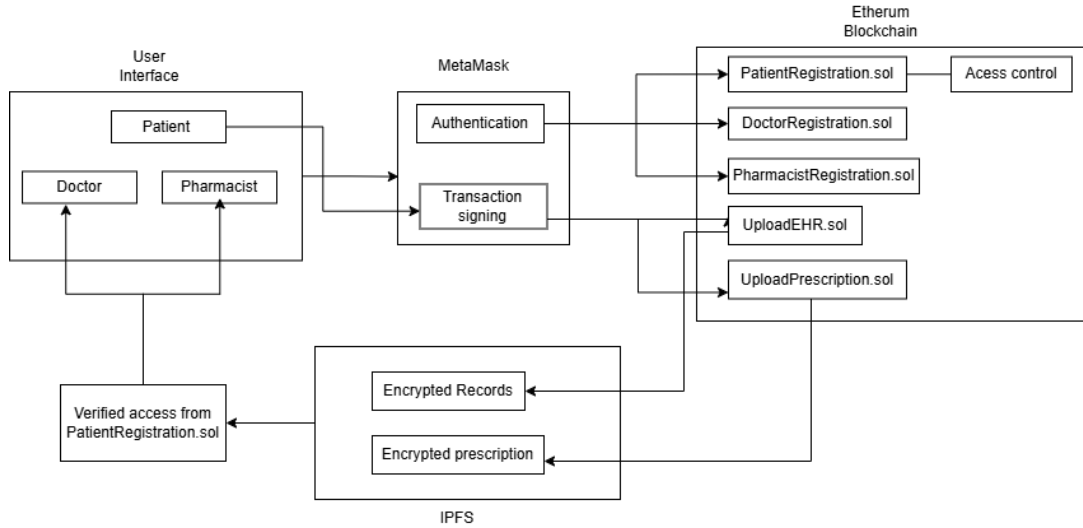


Figure 2: Architecture Diagram

- **Architecture :** There are three different layers in this architecture required for the development of EHR system. Blockchain Layer handles registration, access control and IPFS hash storage. storage layer to store records and application layer provides User friendly interface to interact with the system.
- **Blockchain Layer:** In this layer various essential smart contracts are executed to register the users on the system and authenticate using MetaMask. Multiple smart contracts are used to verify the user and store the IPFS hash on blockchain. It logs immutable records of data access and permissions.
- **Storage Layer:** The InterPlanetary file system IPFS is off-chain decentralized storage system which is used to store encrypted medical data. The Hash of the uploaded records are linked to the blockchain.
- **Application Layer:** This layer provides interactive interface developed using react.js to create a dashboard for each user to register and login based on their role patient, doctor and pharmacist. It also provides a interface for patient to upload and grant access to medical records.
- **Encryption Mechanisms:** AES-256 is a symmetric encryption protocol which uses a single 256 bit key for strong, fast, efficient encryption and decryption process as compare to DES. Maintain standards, suitable to secure the medical records with sensitive information before storing on a decentralized storage. The encryption key is share by the data owner to authorized entities for granting access to the records.
- **Smart Contract:** Multiple Smart contracts are developed using solidity such as doctoregistration.sol, Patientregistration.sol and Pharmascistregistration.sol for role management and access control to the records. allows patient to grant and revoke access. contracts like uploadEHR.sol and Uploadprescription.sol are developed for user to update and interact with IPFS to store medical records.
- **Performance Optimization:** Appropriate blockchain framework is needed to optimize system performance. Ethereum is a public blockchain which offers a decentralized environment and strong capabilities with smart contract. it may face

scalability issues and introduce higher latency within healthcare application. storing the large volume data off-chain on IPFS reduces the load on blockchain providing more stability.

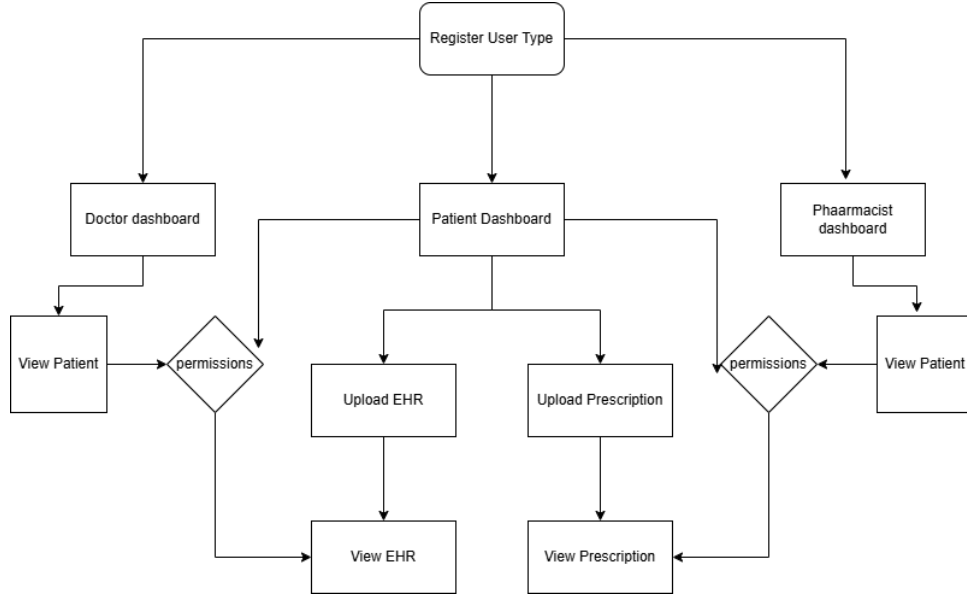


Figure 3: Use Case Diagram

3.3 Implementation

This phase focuses on developing and deploying the proposed blockchain based EHR system. It is critical for converting the system design discussed into a working model the primary objective is to provide a working model that has secure workflows, decentralized storage and a user-friendly interface. The implementation stage make sure the integration of the blockchain technology, decentralized storage and encryption for addressing the challenges discussed in traditional system while maintaining the user experience

1. **Smart Contracts:** The system uses smart contract which are developed using solidity and deployed using truffle. The contracts handle major functionalities like user registration for patients, doctors, and pharmacist to securely register to the system. Provides access control to data owners to grant and revoke access to their medical records. Smart contract are also used to store the IPFS hash on blockchain for storage and retrieval of the records.
2. **Frontend Development:** Role based dashboard are developed using react.js to provide a user experience for the patient, doctor and pharmacist. Patients can upload their medical records manage permissions to view the data. Doctors can view the records shared by the patients to treat accordingly. and pharmacist is able to view and verify prescription by uploading it to patient records. Every dashboard provides allows users to interact with the system with maintained security.
3. **Development Environment:** The system uses node.js which allows secure communication within users and blockchain. APIs to handle the workflow for user registration through /register-user endpoint to log and verify the user details in a

secure way. /Upload-ehr API to link the blockchain with the encrypted records uploaded to the IPFS. The /view-records endpoint decrypt and retrieve the records to make sure the data is access and managed securely..

4. **Data Storage:** Data security and scalability can be achieved Using hybrid storage. The encryption of medical records is performed using AES-256 encryption standard before uploading it to IPFS. The hash of each file uploaded is recorded on the blockchain maintaining integrity and easy retrieval of the records. This approach of data storage reduces the load on blockchain for tamper proof records and verified access control.
5. **Authentication:** To make sure the every interaction with the blockchain is safe and secure. MetaMask is used for authentication it is a browser extension tool which allows user to manage the wallet connected to the blockchain and records every transaction securely. Every action like registration, uploading records or granting access requires authorization from MetaMask for maintain transparency, consent driven sharing and security of all interactions.

3.4 Testing and validation

- **Function Testing:** To verify that the system behaves as intended across various interaction. To verify the workflows of the system to for errors or uninterrupted operation. Testing the registration using smartcontracts and redirection of the user to their role specific dashboard. Interacting with IPFS for storing and Validating the access control feature for granting and revoking access to the uploaded records.
- **Security Testing:** check the implementation of the security and access control protocols to prevent unauthorized access. Validation of encryption protocols to maintain confidentiality of the data stored. Network scanning to ensure encryption protocols used while data transmission. simulate test to access the records without permissions. Vulnerability assessment of smart contracts and APIs to identify potential vulnerabilities.
- **Scalability Testing:** Evaluates the performance and behavior of the system with increase in number of transactions, users and data upload. Throughput is calculated by the capability of the system to process transaction per second and latency provide the time delay in processing transactions.

3.5 Ethical Consideration

To ensure data privacy, informed consent and responsible data usage the system is designed and tested considering ethical principles. Specific measures were taken to achieve compliance with GDPR and HIPAA. All the sensitive medical records are encrypted before storage to maintain privacy and confidentiality of the patient. Smart contracts used to log the patient consent while sharing data maintaining the GDPR requirements. Role based access control to grant and revoke access to the records for controlled information sharing. The system maintains immutable logs of data sharing and access modification aligning to HIPAA regulation. Synthetic data is used while testing the system to avoid ethical risk related with handling real patient data. Maintaining research integrity and validation standards.

3.6 Tools and Technology

Category	Tool/Technology	Purpose
Blockchain Frameworks	Ethereum	smart contract execution in decentralized environment.
Smart Contract Development	Solidity	developing secure smart contracts.
	Truffle	compiling, deployment and migration of contracts.
	Ganache	Simulate a private blockchain network and record transactions.
Decentralized Storage	IPFS	off-chain storage.
User Interfaces	React.js	Frontend development.
	MetaMask	authentication and signing transactions.
Development Environment	Node.js	APIs and dependencies for web3 and encryption functionalities.

Table 1: Tools and Technologies Used

4 Implementation

The implementation stage of the project converts the system design into a functional system providing a practical application of blockchain. The process includes developing smart contracts to manage operations like registration, access control and storing IPFS hash. Integration of decentralized storage solutions to ensure secure data handling. Creating a secure role-based User interface to interact and with the system and testing the system for security, performance and reliability.

4.1 Justification of tools and technologies used

- **truffle:** This tool provides a simple command line interface to develop, deploy and test smart contract it support multiple contract deployment. remnix is an alternative option which was used to test the smart contracts.
- **Ganache:** It is open source for local development and testing. Provides a Ethereum blockchain test network with 10 accounts preloaded with 99eth. It helps in monitoring the smart contracts deployment and interaction with the network.
- **MetaMask:** Is a browser extension used to interact with the blockchain using smart contract providing secure authentication and transaction approvals process. it logs every transaction to maintain transparency and consent driven interaction.
- **IPFS:** Provides a decentralized storage to faster access to data by enabling retrieval for multiple locations. It is to store large medical records and store the CID on Blockchain to reduce load on blockchain.

- **Solidity:** It is a Primary programming language for developing Smart contracts on Ethereum Virtual Machine EVM.
- **React.js:** Used for building frontend and user interfaces. It renders code faster. easy to understand reusable components and single file is used for logic and code for better understanding of the code.
- **Node.js:** is used to create Development environment and provides all the necessary dependencies to handle web3 interactions. it can handle multiple concurrent connection without overhead. a necessary tool for developing dAPP.

4.2 Smart Contract Development

Smart contracts can be used to validate critical processes in a blockchain based application. It provide secure and modular functions to implements the core functions like user registration, access control and storage links. By using truffle the contract can be compiled and deployed on the local blockchain network. Ganache provides environment to simulate the interactions with the blockchain it is useful to optimize the gas fees and evaluate errors in the transactions before deployment to real network. MetaMask is used for testing the transactions during the implementation phase.

Smart Contracts

1. **DoctorRegistration.sol:** This smart contract is responsible for registration of doctors and verifying the credentials.
2. **PatientRegistration.sol:** This smart contract is used to register patients and provides access control.
3. **PharmacistsRegistration.sol:** Manages pharmacists registration and allows to link the prescription provided to the patient their medical records for doctors verification.
4. **UploadEHR.sol:** links blockchain to IPFS storage by storing the hash of the uploaded health record.
5. **UploadPrescription.sol:** This contract is used to upload prescription to IPFS and stores hash of the prescription uploaded.

4.3 Data Storage and Encryption

IPFS service is configured to run on localhost:5001 and to connect with the frontend using ipfs-http-client. The system uses ethereum blockchain and IPFS storage to manage records with maintained security, privacy and scalability. Medical records are encrypted using AES-256 encryption protocol from Node.js module crypto-js. A random 256 bit key and a Initialization vector(IV) is generated for each file. and then passed to ipfs.add() to store the data on IPFS. The encrypted file stored on IPFS generated a unique Content Identifier (CID) which is stored on blockchain using UploadEHR.sol and Uploadprescription.sol to verify the integrity. The encryption key is shared with the authorized user for accessing the data with patient consent.

4.4 UI Development

The user interface of the system is developed in Visual Studio code software designed using React.js. using 'npx create-react-app EHR system'. to create a folder with all the

necessary files src contains the application code. app.js is the main application component and node_modules with all the dependencies. Creating simple and easy interaction between all the components and routing to improve usability while maintaining security.

- **Patient dashboard:** Allows user to upload, view and manage access to the health records prescription uploaded on IPFS

- **Doctor Dashboard:** Allows the healthcare professionals to securely access the records shared by the patient and verify the prescription updated by the pharmacists on patient records.

- **Pharmacist Dashboard:** healthcare providers can access just the prescription records shared by the patient and upload the prescription to patient records for the doctor to verify the prescription.

Blockchain Integration: The interaction with the blockchain is achieved through web3.js component 'npm install web3' after compiling and deploying the contracts developed using 'truffle compile' and 'truffle migrate' the contract address and abi is verified in the code for correct behavior. MetaMask is used for authentication of the wallets while login and approval of the transactions. user confirmation is required for every transaction to ensure safety against unauthorized actions.

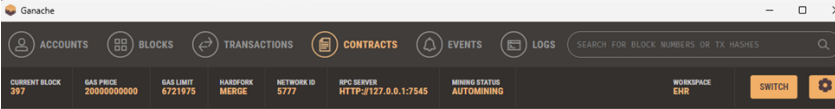
4.5 Work Flow Implementation

1. **User Registration:** The system provides a secure registration for all users with their respective registration dashboard. MetaMask wallet address and ID number created while registration is a unique identifier for every user. the system logs transaction while registration. Then a user can login to the system by using the ID number and password created while registration to login to their specific dashboard.
2. **Data Upload:** Patient can upload their medical records securely by using the upload records and upload prescription tab choose a file to upload and submit this will pop MetaMask for verifying the transaction. The data stored is encrypted and successfully stored on ipfs and the CID and the encryption keys are stored on the smart contract. The pharmacist can upload the prescription provided by the patient to their records to verify with doctor.
3. **Access Management:** Patient have complete access to manage permissions to the medical records through the grant permissions dashboard these permissions can be updated and stored in the smart contract which allows the user to access the data with full control privacy and trust in the system.
4. **Data Retrieval:** The users authorized by the patient can access the records. only doctors can access the medical records and the pharmacist can access just the prescription . After granting access the system shares the encryption key and IV with the authorized user to view the records. The process ensures that the information is accessed just by authorized users maintaining security.

5 Results and Critical Analysis

5.1 Testing

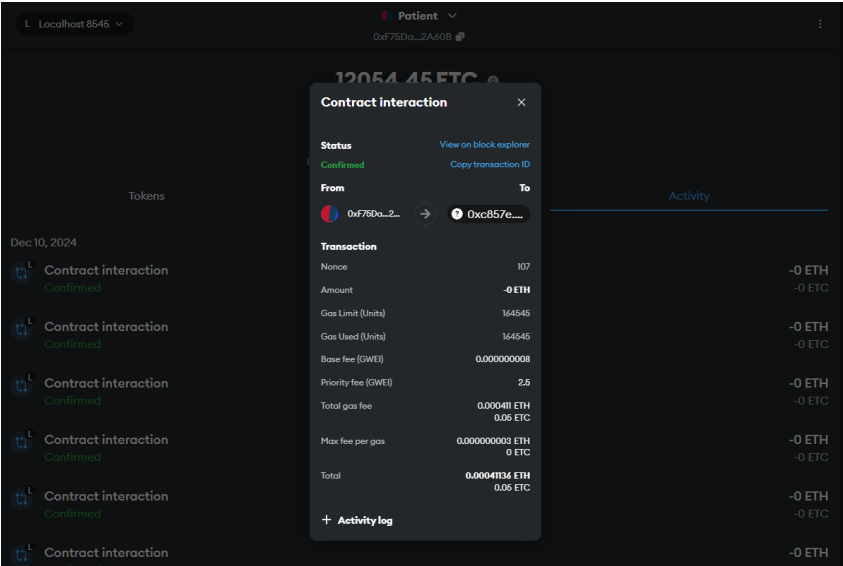
- **Functional testing** is conducted to carryout tests the core functionality and workflow of the like user registration, role based redirection, and interaction with smart contract. ensure every transactions is validated while registration and uploading the medical records to the IPFS storage. validated every transaction on MetaMask and ganache. Testing the Access control function to verify only selective data shared with authorized entity.



The screenshot shows the Ganache application interface. At the top, there are tabs for ACCOUNTS, BLOCKS, TRANSACTIONS, CONTRACTS, EVENTS, and LOGS. The CONTRACTS tab is active, displaying a list of deployed contracts. The table below represents the data shown in this tab.

NAME	ADDRESS	TX COUNT	STATUS
DoctorForm	0x01ede3d9f89B8D06E262Fe2Fbd4bCA8976A19180	0	DEPLOYED
DoctorRegistration	0xC53138DEa8CcCE32f05CdfC224484613c191203d	6	DEPLOYED
PatientRegistration	0xB762dCC5A6AcC8CFE01ef9d6b624B0A6932Bc0B9	2	DEPLOYED
PharmacistForm	0x2B4A39EDBDe4d3c34F155094bDd3C5c06D8F2383	1	DEPLOYED
PharmacistRegistration	0xDC78d39C7F40581C88B35839C21635ef459cb720	4	DEPLOYED
UploadEhr	0xc857e30a97b2EE05D0EFE61b7585B68eABE7145a	7	DEPLOYED
UploadPrescription	0x6947c0670bEdf29E8F9B1eF33b725c3945914538	4	DEPLOYED

Figure 4: Verification of contracts deployment



The screenshot shows a 'Contract interaction' window in a wallet interface. It displays transaction details for a confirmed transaction. The table below represents the data shown in this window.

Field	Value	Unit
Status	Confirmed	
From	0xF75Da...2A60B	
To	0xc857e...	
Nonce	107	
Amount	-0 ETH	
Gas Limit (Units)	164545	
Gas Used (Units)	164545	
Base fee (GWEI)	0.000000008	
Priority fee (GWEI)	2.5	
Total gas fee	0.00041136 ETH	
Max fee per gas	0.000000003 ETH	
Total	0.00041136 ETH	

Figure 5: Transaction Verification

- **Security testing** focused on validating data integrity and identifying potential vulnerabilities in the environment. Verified Unauthorized access to the medical

records and prescription data to ensure only authorized user can view the records. Validate data on IPFS network is encrypted and only the hashes of the records are stored to maintained confidentiality and integrity of the records.

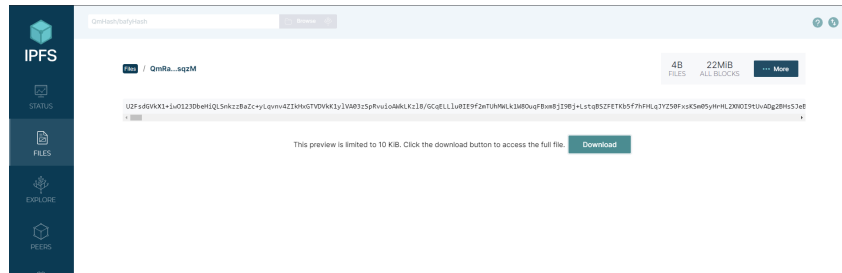


Figure 6: Encryption Verification on IPFS

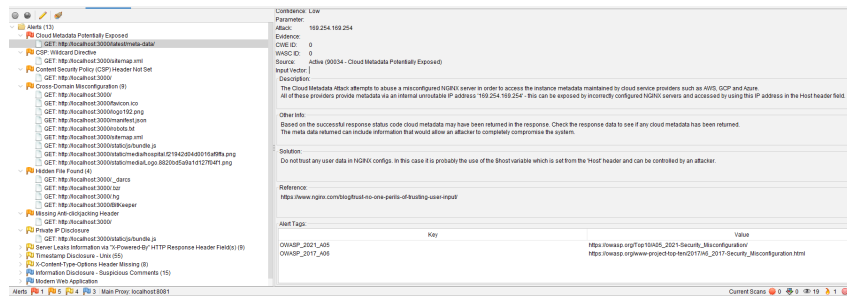


Figure 7: Vulnerability Assessment

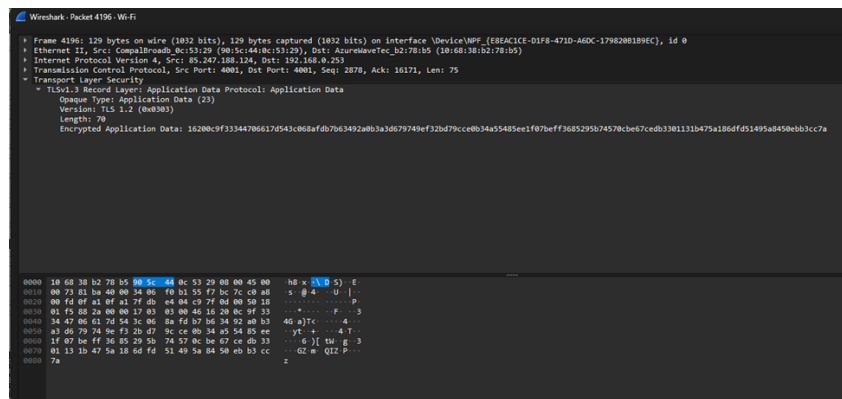


Figure 8: Encryption verification on WireShark

- **Scalability** of the system was tested using apache Jmeter. Throughput and the stability of the system demonstrate the ability of the system handle scaling without performance loss.

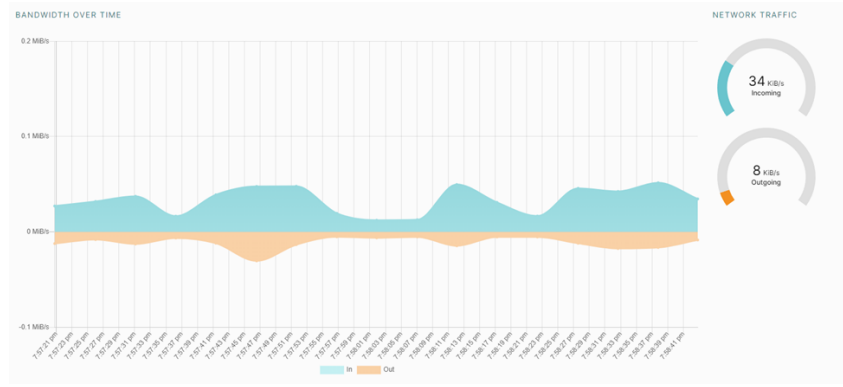


Figure 9: IPFS Bandwidth While Data Transfer

- **Performance testing** of the system was determined using latency and efficiency of every transaction to upload, retrieve files from IPFS and other blockchain interaction every transaction was complete in acceptable time on an average 2 seconds. The performance of the storage system for storing and retrieving the data was observed in the bandwidth of the IPFS while data transmission.

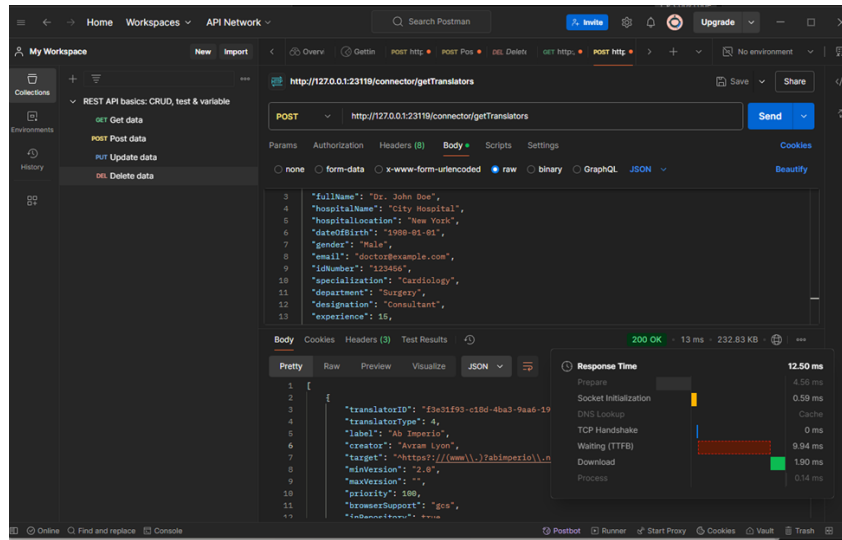


Figure 10: Postman Test

- **Ethical consideration** and Compliance with GDPR were consider while testing the system by using the encryption of the medical records before uploading the data to IPFS and using synthetic test data for safety from the risks associated with real patient data which maintained the integrity while testing the system.

5.2 Validation

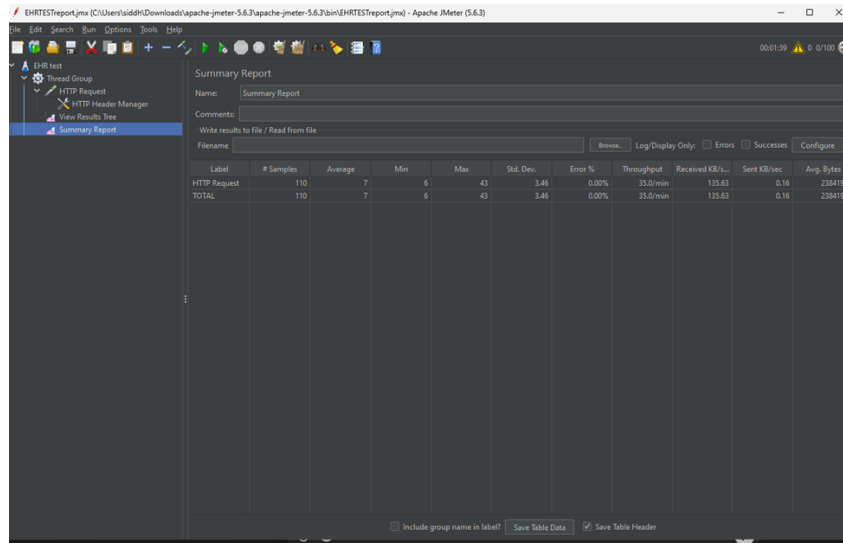
1. Security Improvements

The proposed system improves data protection and user trust. The role-based access control implemented using smart contract confirmed its effectiveness. while testing it prevented unauthorized access to the uploaded records and prescriptions indicating strong security measure. Patient can grant and revoke access to the

uploaded data ensuring control over data. By storing the IPFS hash of the records on blockchain prevents manipulation or deletion. Records are encrypted using AES-256 encryption protocol before storing on IPFS to ensure only authorized users can decrypt and read the data maintaining confidentiality and compliance.

2. Efficiency and Performance

The performance of the system is optimized by storing large medical records on IPFS which reduces the load on blockchain as well as the transaction costs. Transactions include registration and uploading the records which executed with average latency of 2.5 seconds. The system was able to handle around 40 transactions per minute capable to operate efficiently in moderate healthcare environment.



The screenshot shows the Apache JMeter Summary Report window. The report is titled 'Summary Report' and displays the following data:

Label	# Samples	Average	Min	Max	Std. Dev.	Error %	Throughput	Received KB/s	Sent KB/s	Avg. Bytes
HTTP Request	110	7	6	43	3.46	0.00%	35.0/min	135.63	0.16	238419.0
TOTAL	110	7	6	43	3.46	0.00%	35.0/min	135.63	0.16	238419.0

Figure 11: Apache Jmeter

3. Interoperability

The systems provides advance interoperability by secure data exchange between healthcare providers. Role based workflows provides user friendly dashboard for multiple user type. The smart contracts manage access control and data exchange successfully to maintain EHR workflow. This approach is supported by the research(Sonkamble et al.; 2023) highlighting the importance of interoperability within healthcare applications and discuss the consideration of architecture and standards for integration of EHR systems with blockchain.

5.3 Comparison with Existing Solutions

1. Security: EHR system are dependent on centralized architectures which can be vulnerable to breaches. Around 70% of healthcare organization reported data breaches in 2023. The proposed system uses decentralized architecture eliminating single point of failure. Role based access control and AES-256 encryption to ensure security and confidentiality. Alder (2024) OnChain (2024)

2. Efficiency: The system is based on Ethereum which may experience latency issues due to network congestion and delays in proof of work consensus mechanism. The system address this by using off-chain decentralized storage for storing large records. Reducing

the load on blockchain to increase latency and throughput.

3. Interoperability: The system facilitates data sharing between patient, doctor and pharmacist to mimic the behavior and workflow of healthcare system

4. Cost: Traditional EHR systems requires investment in infrastructure and maintenance. due to gas fees Ethereum based systems experience high transaction costs. By developing multiple optimized smart contracts for each function and using IPFS for storage the system offers advance functionality with lower cost.(Bischoff; 2024)

5.4 Healthcare Use Cases

- **Enhancing Data Security in Hospitals:** To protect data integrity and confidentiality required in hospital environment the system uses AES-256 encryption and blockchains immutability. The test performed prevented unauthorized access providing a secure framework and a reliable solution for storing health records.
- **Facilitating Interoperability Among Providers:** The system provides secure data sharing between patients, doctors and pharmacists. Simulated tests highlight secure sharing of records and prescription data with doctors and pharmacists for collaborative care of patient.
- **Patient Empowerment with Data Control:** The permissions workflow of the systems tested verified Patient control over their data which allows them to successfully grant and revoke access to the records. This benefits patient for treatment from multiple specialists maintaining privacy and selective sharing of medical records.
- **Improving Access and Verification of Prescriptions:** The patient can share the prescription records with selected pharmacies which is further added to their medical records for doctors' verification to ensure proper medication and pharmacy workflow with EHR systems.

6 Discussion

The section discussed the project findings, their alignment with objective and implication within the healthcare environment with opportunities of future enhancements and limitations faced. The outcome of the proposed system highlights improvement in security, interoperability, scalability and patient empowerment the discussion provides insights in systems contributions and its potential for healthcare data management.

6.1 Implications for the Healthcare Industry

Data Security: Using decentralized storage and strong encryption protocols the system mitigates the risk associated with unauthorized access and data breaches. Cyber attacks on centralized system can be frequent and costly. Supported by the research highlighting decentralized environment to improve security of health data due to reduced single point of failure. (Haddad and Ali; 2022) (Alder; 2024)

Interoperability and Collaboration: Interoperability is important for data exchange between patients and healthcare providers. The need of standardized formats for compatibility across different healthcare provider is highlighted in the study. The system employs multiple role-based user dashboard and APIs to share selective medical records

provides coordinated care. (Han et al.; 2022) (Shaik et al.; 2023)

Scalability: The systems architecture provides a scalable solution for data management, able to handle increasing data load for a moderate healthcare environment. A scalable system is essential for data management to handle increasing loads of medical records without compromising performance. (Sharma and Balamurugan; 2020)

Empowering Patients: The system provides patient full control over their data allowing patient centric care, informed decision making to maintain trust within patient and healthcare providers. As per the studies on patient managed information exchange, Patient empowerment is a key factor in improving patient engagement and satisfaction.

Objective	Findings
Security	AES-256 encryption and immutability nature of blockchain is effective against data breaches. Access control and IPFS hash storage is managed by smart contracts, ensuring tamper proof records. This approach aligns with (Shaik et al.; 2023) findings, who confirmed that end-to-end encryption in blockchain based EHR systems improves confidentiality and integrity of the data.
Scalability	The system is able to process on an average 50 transactions per minute, enough to handle moderate healthcare data. Scalability of the system is improved by using IPFS for data storage reducing the load on blockchain. Consistent with the (Sharma and Balamurugan; 2020) work, who proposed a multilayer architecture to improve scalability for sharing data.
Interoperability	Secure data exchange between patient, doctors and pharmacist is achieved by the system providing interoperability. Recent studies on traditional EHR systems highlights the importance of standardized data formats for effective data exchange.
Patients Empowerment	The dashboards enable patients to upload and manage permission to grant access to authorized healthcare providers to their health records as required. the approach is centered to patients, giving more control over their data, As the principles discussed regarding patient data ownership by (Han et al.; 2022).

Table 2: Findings Aligned with Objectives

6.2 Limitations

1. **Scalability :** The system was tested within a simulated environment with and average throughput result of 35/min. Scalability challenges may cause on public blockchain in real-world due to network congestion and transaction latency. the study (Donawa et al.; 2020) verifies that Ethereum blockchain may not support high transaction throughput required in large healthcare organization leading to 7.5 million unsealed data transaction per day.
2. **Efficiency:** Ethereum blockchain can be energy-intensive due to its Proof of Work (PoW) consensus mechanism. Transition to more efficient protocol used in Ethereum 2.0 such as Proof of Stake (PoS) or by using a permissioned blockchain like

Hyperledger Fabric. This is essential to maintain sustainability issues associated with energy consumption of blockchain. Nguyen (2023)

3. **Cost:** large scale deployments can be costly due to pinning services for data retrieval from IPFS storage. It is important to manage cost for economic survival of the system.
4. **Testing on Synthetic Data:** Using the synthetic dataset limits to fully test the ability of the system to handle complexities of the high data volume in real healthcare records. This may lack to identify all the challenges in actual patient data. (Ghosh et al.; 2023)

6.3 Ethical Consideration

Patient Privacy and Data Ownership: The system allows patient greater control over their data through dynamic permissions, with each sharing activity logged ensuring transparency. This ensures compliance with regulations like General Data Protection and regulation (GDPR) and Health Insurance Portability and Accountability Act (HIPAA) with data security and patient trust. As per (Ettaloui et al.; 2024) characteristic of blockchain can improve interoperability, anonymity and access control over data. Compliance with regulatory is important to increase the systems potential in real world.

Informed Consent: The workflow of the system allows patient to monitor the access and its purpose via logs. Providing consent-driven transfers of the records which maintains patient autonomy and informed consent which are the fundamental principles in healthcare. As observed by Ivan et al. (2016) blockchain can improve security in health records storage and sharing. Improving the patient consent. (Shaik et al.; 2023)

Use of Synthetic Data for Testing: To preserve patient privacy and confidentiality the system was validated using synthetic data which may not include the complexities and volume of real health records. which could impact in the real-world applicability of the system.

Compliance with Regulations: The system designed aligns with ethical standards like GDPR and HIPAA by prioritizing data security and patient rights over their data. It is important to comply with ethical and legal ways of managing healthcare data. (Ettaloui et al.; 2024) highlights the compliance of blockchain application with regulatory framework to increase the acceptance in real-world.

7 Conclusion and Future Work

The blockchain based EHR system provides a strong framework to manage healthcare data in secure and scalable way to use the system more efficiently multiple ways can be used to expands its capabilities to overcome its limitations proposed improvements can enhance the systems capabilities and applicability in real world healthcare. To improve the scalability of the system permissioned blockchain can be used like Hyperledger fabric Quorum etc. Permissioned blockchain can reduce the transaction cost with increased throughput which can make the system more suitable for large scale deployment. Integrating the system with layer 2 solutions like polygon or optimism can be used to mitigate the latency issue lowering the transaction fees while using public blockchain. The current

Ethereum proof of work consensus mechanism uses more energy. To make the system efficient Ethereum 2.0s proof of stake blockchain network can be used which could align the system with sustainability goals to make it environment friendly. The data availability of the system can be improved using alternative off chain storage. The file coin solution offers more cost effective and reliable solution to maintain the access to the stored files with scalability for large scale implementation without extra operational cost. Integrating the system with AI and IoT devices can transform the system for predictive analysis and decision making. The data from IoT devices such as smart watches, trackers to provide real time data which can be securely stored through blockchain and analyzed using AI for predictive analysis to identify patterns and trends for preventative care improving health care.

The aim of the research was to address the challenges faced by the traditional EHR systems by using the blockchain technology and its ability to improve data security, interoperability, patient control over data. The research highlights the potential of decentralized blockchain technology to upgrade the healthcare systems while maintaining patient centric care. The system was able to achieve strong security through blockchains immutable nature and AES-256 encryption. It successful in preventing unauthorized access to the data while testing. The role based dashboard empowers patient to manage access to the uploaded records enhancing trust and allowed data exchange to improve interoperability. scalability of the system is validated thorough simulated testing of the transactions request per minute the system sustained up to 35 transaction per minute. The transaction cost is reduced using multiple optimized smart contracts and using off-chain storage to store large medical data which also lower the cost of storage.

References

- Alder, S. (2024). Healthcare data breach statistics. Accessed: 2024-12-10.
URL: <https://www.hipaajournal.com/healthcare-data-breach-statistics/>
- Arunkumar, S. and Kousalya, P. (2020). Lightweight blockchain system for small clinics using aes-256-gcm encryption, *International Journal of Computer Applications* **182**(5): 27–33.
- Banerjee, S., Barik, S., Das, D. and Ghosh, U. (2024). Ehr security and privacy aspects: A systematic review, in D. Puthal, S. Mohanty and B.-Y. Choi (eds), *Internet of Things. Advances in Information and Communication Technology*, Springer Nature Switzerland, Cham, pp. 243–260.
- Bischoff, P. (2024). Ransomware attacks on hospitals: 5 years of data, *Comparitech* .
URL: <https://www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/>
- Chelladurai, U. and Pandian, M. (2021). A novel blockchain-based electronic health record automation system, *Journal of Ambient Intelligence and Humanized Computing* **12**(5): 4327–4340.
- de Carvalho Junior, M. A. and Bandiera-Paiva, P. (2020). Strengthen electronic health records system (ehr-s) access-control to cope with gdpr explicit consent, *Journal of Medical Systems* **44**(172). Accessed: 2024-12-10.
URL: <https://link.springer.com/article/10.1007/s10916-020-01631-5>

- Dive, H. (2023). Hacking healthcare: With 385m patient records exposed, cybersecurity risks abound. Accessed: 2024-12-10.
URL: <https://www.healthcaredive.com/news/cybersecurity-hacking-healthcare-breaches/643821/>
- Donawa, A., Orukari, I. and Baker, C. E. (2020). Scaling blockchains to support electronic health records for hospital systems, *arXiv preprint arXiv:2001.05525* . <https://doi.org/10.48550/arXiv.2001.05525>.
- Esmailzadeh, P. (2022). Benefits and concerns associated with blockchain-based health information exchange (hie): a qualitative study from physicians' perspectives, *BMC Medical Informatics and Decision Making* **22**: 80. Received: 06 January 2022; Accepted: 10 March 2022; Published: 28 March 2022.
URL: <https://bmcmidinformedecismak.biomedcentral.com/articles/10.1186/s12911-022-01815-8>
- Ettaloui, N., Arezki, S. and Gadi, T. (2024). An overview of blockchain-based electronic health record and compliance with gdpr and hipaa, *in* Y. Farhaoui, A. Hussain, T. Saba, H. Taherdoost and A. Verma (eds), *Artificial Intelligence, Data Science and Applications*, Springer Nature Switzerland, Cham, pp. 405–412.
- Ghosh, P. K., Chakraborty, A., Hasan, M., Rashid, K. and Siddique, A. H. (2023). Blockchain application in healthcare systems: A review, *Systems* **11**(1).
URL: <https://www.mdpi.com/2079-8954/11/1/38>
- Haddad, S. and Ali, B. (2022). Systematic review on ai-blockchain based e-healthcare records management systems, *Journal of Healthcare Informatics* **15**(2): 45–60.
- Han, Y., Zhang, Y. and Vermund, S. H. (2022). Blockchain technology for electronic health records, *International Journal of Environmental Research and Public Health* **19**(15577): 1–6.
- Jercich, K. (2022). Hhs cyber arm warns of ehr vulnerabilities, *Healthcare IT News* . Accessed: 2024-12-11.
URL: <https://www.healthcareitnews.com/news/hhs-cyber-arm-warns-ehr-vulnerabilities>
- Karmakar, S., Bhaduri, A., Kumari, P. and Soni, K. (2023). Blockchain technology for securing electronic health records: A comprehensive review and future directions, *International Journal for Research in Applied Science Engineering Technology* **11**: 2266–2271.
- Mamun, A. et al. (2022). Blockchain use in ehr systems: A comprehensive review, *Blockchain for Healthcare Journal* **5**: 1–19.
- Medicine, M. (2022). The benefits and challenges of ehr scalability. Accessed: 2024-12-10.
URL: <https://www.modmed.com/resources/blog/the-benefits-and-challenges-of-ehr-scalability>
- Nguyen, A. M. (2023). Challenges of blockchain applications in digital health: A systematic review, *arXiv preprint arXiv:2304.04101* . <https://doi.org/10.48550/arXiv.2304.04101>.

- OnChain (2024). Electronic health record systems using blockchain: 4 examples, *OnChain Magazine* .
URL: <https://onchain.org/magazine/electronic-health-record-systems-using-blockchain-4-examples/>
- Poteet, J., Gault, M., Khurshid, A., Sivagnanam, S., Norta, A. and Treiblmaier, H. (2024). Ehr systems and blockchain: Potentials, challenges and the road ahead: Conv2x 2023 cme session, *Blockchain in Healthcare Today* **7**(1). Accessed: 2024-12-11.
URL: <https://doi.org/10.30953/bhty.v7.312>
- Reegu, F. A., Abas, H., Gulzar, Y., Xin, Q., Alwan, A. A., Jabbari, A., Sonkamble, R. G. and Dziyauddin, R. A. (2023). Blockchain-based framework for interoperable electronic health records for an improved healthcare system, *Sustainability* **15**(8).
URL: <https://www.mdpi.com/2071-1050/15/8/6337>
- Schmeelk, S., Kanabar, M., Peterson, K. and Pathak, J. (2022). Electronic health records and blockchain interoperability requirements: a scoping review, *JAMIA Open* **5**(3): ooac068.
URL: <https://doi.org/10.1093/jamiaopen/ooac068>
- Shahnaz, A., Qamar, U. and Khalid, A. (2019). Using blockchain for electronic health records, *IEEE Access* **7**: 147782–147795.
- Shaik, M. et al. (2023). Permissioned blockchain networks for managing ehr systems, *Journal of Blockchain in Health* **9**(2): 67–78.
- Sharma, P. and Balamurugan, B. (2020). Preserving the privacy of electronic health records using blockchain, *Procedia Computer Science* **170**: 603–610.
- Shrestha, A. and Panta, S. (2023). Blockchain-based electronic health record management system, *Journal of Artificial Intelligence and Capsule Networks* **7**(3): 12–25.
- Sonkamble, M. et al. (2023). Patient-centric blockchain systems for medical data sharing, *Journal of Health Informatics* **18**: 100–112.
- Telychko, O. (2024). Challenges of interoperability in healthcare. Accessed: 2024-12-10.
URL: <https://codeit.us/blog/challenges-of-interoperability-in-healthcare>
- Vidap, K. et al. (2023). Blockchain solution to electronic healthcare records, *Electronics* **12**(10): 1015.