



***Dissertation on***

**Securing Healthcare Record Using Blockchain  
Technology**

*Submitted in partial fulfilment of the requirements for the award of degree of*

**Bachelor of Technology  
in  
Computer Science & Engineering**

**UE21CS461A – Capstone Project Phase - 2**

***Submitted by:***

<b>Mohammed Jabir</b>	<b>PES2UG21CS300</b>
<b>Mahamad Sakeeb</b>	<b>PES2UG21CS266</b>
<b>Md Sami</b>	<b>PES2UG21CS287</b>
<b>Mohammed Afnan</b>	<b>PES2UG21CS296</b>

***Under the guidance of***

**Prof. Shruthi L**  
Assistant Professor  
PES University

**June - Nov 2024**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING  
FACULTY OF ENGINEERING  
PES UNIVERSITY**

(Established under Karnataka Act No. 16 of 2013)  
Electronic City, Hosur Road, Bengaluru – 560 100, Karnataka, India



## PES UNIVERSITY

(Established under Karnataka Act No. 16 of 2013)  
Electronic City, Hosur Road, Bengaluru – 560 100, Karnataka, India

### FACULTY OF ENGINEERING

# CERTIFICATE

*This is to certify that the dissertation entitled*

### **Securing Healthcare Record Using Blockchain Technology**

*is a bonafide work carried out by*

**Mohammed Jabir  
Mahamad Sakeeb  
Md Sami  
Mohammed Afnan**

**PES2UG21CS300  
PES2UG21CS266  
PES2UG21CS287  
PES2UG21CS296**

In partial fulfilment for the completion of seventh semester Capstone Project Phase - 2 (UE21CS461A) in the Program of Study -Bachelor of Technology in Computer Science and Engineering under rules and regulations of PES University, Bengaluru during the period June 2023 – Nov. 2024. It is certified that all corrections / suggestions indicated for internal assessment have been incorporated in the report. The dissertation has been approved as it satisfies the 7<sup>th</sup> semester academic requirements in respect of project work.

Signature  
Prof. Shruthi L  
Assistant Professor

Signature  
Dr. Sandesh B J  
Chairperson

Signature  
Dr. B K Keshavan  
Dean of Faculty

#### **External Viva**

#### **Name of the Examiners**

#### **Signature with Date**

1. \_\_\_\_\_

\_\_\_\_\_

2. \_\_\_\_\_

\_\_\_\_\_

## **DECLARATION**

We hereby declare that the Capstone Project Phase - 2 entitled “**Securing Healthcare Record Using Blockchain Technology**” has been carried out by us under the guidance of **Prof. Shruthi L, Assistant Professor** and submitted in partial fulfillment of the course requirements for the award of the degree of **Bachelor of Technology in Computer Science and Engineering** of **PES University, Bengaluru** during the academic semester June – Nov 2024. The matter embodied in this report has not been submitted to any other university or institution for the award of any degree.

**Mohammed Jabir**

**Md Sami**

**Mohammed Sakeeb**

**Mohammed Afnan**

**PES2UG21CS300**

**PES2UG21CS287**

**PES2UG21CS266**

**PES2UG21CS296**

## ACKNOWLEDGEMENT

I would like to express my gratitude to Prof. **Prof.Shruthi L, Assistant Professor**, Department of Computer Science and Engineering, PES University, for her continuous guidance, assistance, and encouragement throughout the development of this UE21CS461A Capstone Project Phase-2.

I am grateful to the Capstone Project Coordinators, Dr. Farida Begam, Professor and Prof. Vandana M. Ladwani, Associate Professor, Department of Computer Science and Engineering, PES University for organizing, managing, and helping with the entire process.

I take this opportunity to thank Dr. Sandesh B J, Chairperson, Department of Computer Science and Engineering, PES University, for all the knowledge and support I have received from the department. I would like to thank Dr. B.K. Keshavan, Dean of Faculty, PES University for his help.

I am deeply grateful to Dr. M. R. Doreswamy, Chancellor, PES University, Prof. Jawahar Doreswamy, Pro Chancellor, PES University, Dr. Suryaprasad J, Vice Chancellor, PES University and Prof. Nagarjuna Sadineni, Pro Vice Chancellor, PES University for providing to me various opportunities and enlightenment every step of the way. Finally, this project could not have been completed without the continual support and encouragement I have received from my family and friends.

# **ABSTRACT**

The growing importance of securing patient data and ensuring the integrity of health records has driven the search for innovative solutions. Centralized systems, while widely used, are increasingly criticized for their susceptibility to data breaches and the challenges of managing access permissions. Blockchain technology has emerged as a promising alternative to address these concerns by offering a decentralized, immutable, and transparent platform for storing and managing healthcare records. By leveraging cryptographic methods and consensus algorithms, blockchain ensures data integrity and minimizes the risk of tampering. Access to sensitive health data is restricted to authorized individuals, with each transaction or modification materialized as a block in the chain, providing a clear and auditable history of data activities.

A decentralized healthcare system based on blockchain could eliminate intermediaries, reducing the risk of unauthorized access or data manipulation. Smart contracts further enhance this framework by automating predefined rules and permissions, streamlining processes and minimizing human intervention. This approach empowers patients by granting them greater control over their health data, allowing access only upon their consent. Additionally, the standardization of formats and interaction protocols on blockchain enables seamless data exchange between various healthcare providers and systems. This not only enhances efficiency but also ensures robust data security and integrity across the healthcare ecosystem, paving the way for a more secure and patient-centric future.

# TABLE OF CONTENTS

Chapter No.	Title	Page No.
1.	INTRODUCTION	01
2.	PROBLEM STATEMENT	04
3.	LITERATURE REVIEW	05
	3.1 Research Papers	05
	3.1.1 Securing Healthcare Records using Blockchain Technology	05
	3.1.2 Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain	05
	3.1.3 Security research of blockchain technology in electronic medical records	06
	3.1.4 Blockchain-based Decentralized Platform for Electronic Health Records Management	06
	3.2 Summary	06
4.	PROJECT REQUIREMENTS SPECIFICATION	08
5.	SYSTEM DESIGN (detailed)	24
6.	PROPOSED METHODOLOGY	30
7.	IMPLEMENTATION AND PSEUDOCODE (if applicable)	33
8.	RESULTS AND DISCUSSION	39
9.	CONCLUSION AND FUTURE WORK	47
	REFERENCES/BIBLIOGRAPHY	48
	APPENDIX A DEFINITIONS, ACRONYMS AND ABBREVIATIONS	49
	APPENDIX B USER MANUAL (OPTIONAL)	50

## LIST OF FIGURES

<b>Figure No.</b>	<b>Title</b>	<b>Page No.</b>
<b>Fig 5.1</b>	<b>High level architecture</b>	<b>24</b>
<b>Fig 5.2</b>	<b>Master Class Diagram</b>	<b>25</b>
<b>Fig 5.3</b>	<b>E-R Diagram</b>	<b>26</b>
<b>Fig 5.4</b>	<b>User Interface Diagram</b>	<b>26</b>
<b>Fig 5.5</b>	<b>Flow Daigram</b>	<b>27</b>

## CHAPTER 1

### INTRODUCTION

#### 1.1 Blockchain Technology

The application of blockchain technology in the digital space is paramount on providing strong security attributes that have seen its wide adoption for the protection of all-round digital assets and process foundations. Here's how blockchain technology improves security: Here's how blockchain technology improves security:

**Decentralization:** Contrasting to the conventional mode of transactions that rest upon a central authority holding the keys to the castle, blockchain uses a decentralized network which spreads the nodes everywhere. This dispersion of decision-making systems is a decisive enemy for the hackers who attempt to seize all the system at the same time.

**Unchangeable Record:** The ledger of transactions on the blockchain is deleted and tampered resistant, as no more than a single unit of data can be stored in the space allotted to each transaction. When there is a transaction in the blockchain, it becomes very difficult to tamper or reverse it so any transaction that has been inputted into the blockchain cannot be manipulated. At every block, the previous block gets encrypted with a cryptographic hash and afterwards, the next block goes on, hence forming a chain of blocks where any kind of edits will not only affect the edited block but will also necessitate you to change any subsequent blocks as well and this is a billionth impossible task.

**Secure Cryptography:** Cryptographic algorithms are used to fix data, security and integrity. Transactions are asymmetrically cryptosignatures whereupon they are authenticated, and only those having the corresponding private key are allowed execute transactions. Furthermore, data encryption provides protection for the blockchain data, which stops the unauthorized parties from getting to the measured blockchain information.

**Smart Contracts:** Smart contracts are contracts where the terms get fulfilled automatically, when the code is the presence of, there is no room for the human element. They likewise independently view and maintain the contract terms as the intermediaries become less relevant and the risk of fraud and



manipulation declines. In the context of the blockchain technology, smart contracts do due diligence to achieve transparent and error-free transactions.

**Permissioned Access:** Different permissioning models can be implemented to the fragments of the chain (Networks), for example, introducing the entered participants for a certain period of time or the distribution can access specific information.

## 1.2 Securing healthcare record using blockchain technology

In the modern society where tech play an important role, the protection of the confidential data is more crucial than ever before. Healthcare data usually contains very sensitive and private information which is related to the lives of people, including the details about patients' medical records, treatment options, insurance policy and payment history. While traditional forms of storing and managing significant amounts of data may not sufficiently address the horizons of security and privacy nor the concerns of accessibility.

The teething problems of the traditional finance system pointed out are a reason for the blockchain technology to exist. Blockchain was initially put forward as a safe and immutable ledger system for cryptocurrency, e.g. Bitcoin. However, this promising technology, in view of the efficiency it provides different industries, including healthcare, is attracting attention among developers, regulators, investors, etc.

Blockchain alienates healthcare record management by means of cryptographic principles, decentralization and consensus mechanisms on back of its blockchain technology. This operation helps maintaining the integrity data, security and privacy therefore. In contrast to central database that is susceptible to single point of failures and unauthorized access, blockchain uses distributed data approach where this data is spread across nodes, which is by its nature resilient to malevolent and technologic attacks.

This report aims to examine the potential impact of blockchain technology on enhancing the security of healthcare information in the health sector. We are going to discuss the goal and target with Blockchain, how it is applicable in the management of health care and the benefits it offers to the

patients, healthcare providers and the others involved.

Moreover, we are going to investigate the issues and the significant factors of implementing blockchain solutions in the integrated and complex environment of the healthcare system which is been heavily regulated. The possibility of blockchain comes with the ability not only of data security and privacy, but also better administrative processing, interoperability and timely management of patient health information is being developed. Digital transformation of the healthcare field has now reached its pinnacle, and the implementation of blockchain technology for medical record keeping is one of those innovations.

## CHAPTER 2

### PROBLEM STATEMENT

The healthcare industry faces significant challenges in managing and exchanging patient records securely and efficiently. Traditional record-keeping methods are often vulnerable to unauthorized access and data breaches, compromising patient privacy and the integrity of critical medical information. Additionally, the resource-intensive and time-consuming nature of data exchange further complicates the process, making it difficult for healthcare organizations to ensure confidentiality and reliability in managing sensitive information.

Blockchain technology has emerged as a powerful tool to address these issues. As a distributed ledger system, it offers immutability, transparency, and decentralization, bringing transformative potential to healthcare data management. By enabling secure and efficient data sharing, blockchain could revolutionize how patient records are handled, ensuring privacy, accessibility, and integrity.

However, implementing blockchain in healthcare comes with challenges. Data security remains a critical concern, as unauthorized access and breaches continue to threaten patient confidentiality. Blockchain's robust cryptographic mechanisms offer a solution by protecting patient records and maintaining data integrity in a digital environment. Privacy preservation is another key focus, requiring effective access controls and permission mechanisms that empower patients to manage their data while complying with privacy laws and regulations.

Interoperability is essential for seamless data exchange across different healthcare systems. Blockchain must enable efficient sharing without compromising care delivery, integrating with existing IT infrastructures to ensure accessibility and efficiency. Regulatory compliance is another critical consideration, as healthcare organizations must align blockchain solutions with laws like HIPAA and GDPR while maintaining patient data confidentiality.

## CHAPTER 3

### LITERATURE REVIEW

#### 3.1 Research Papers

##### **Paper 1: Securing Healthcare Records using Blockchain Technology**

Dr. Ranjana Rajnish<sup>1</sup>

2nd INTERNATIONAL CONFERENCE ON ADVANCE

COMPUTING AND SOFTWARE ENGINEERING (ICACSE-2019)

Test the blockchain techniques for processing health information and investigate how they should be complemented with the current data architecture. Blockchain is a secure, patient focused and a digital decentralized ledgering technology. It records implied transactions between account owners in a digital form. It offers the users an improved data management, safety as well as discoveries in the medical applications. Take a look at what the healthcare system has to deal with (fraud, identity theft etc.), as a place where blockchain technology can solve such problems. How about applying blockchat so as to come up with trusted records and privacy issues-solving systems? Implement Blockchain in the health service sector in order to be ahead of your competitors

##### **Paper 2: Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain**

2019

IEEE Conference on Information and Communication Technology(CICT)

First, EHR security and Privacy, Second, Patient-Centric Modelin, Third, Data Access with Rules and Guidelines, Fourth, Blockchain for Access Controls, Finally, Data Partitioning and Encryption Techniques.Blockchain Metadata Storage, Integration with the Cloud Storage, Security byAsymmetric Cryptography, Data Partitioning for Privacy, Transactions Structuring with the Key Pairs,Encryption.

## **Paper 3: Security research of blockchain technology in electronic medical records**

Jia Qu, MSa

2018

our focus is a coming up with an electronic health record (EHR) secure data-sharing scheme based blockchain technology. This is provided that it is possible to address the existing data privacy concerns in healthcare. It leverage blockchain features (for example anti-tampering and decentralization) to achieve data source authenticity and privacy. The protocol encompasses protocols for safe data exchange among legitimate users and utilises the Delegated Proof of Stake(DPOS) mechanism in storing data assets. In analysis simulation, DPOS algorithm is compared with other approach strategies for efficiency. Overall, the article is constructed in such a way that the shared ledger platform is designed to be decentralized, secure, and efficient.

## **Paper 4: Blockchain-based Decentralized Platform for Electronic Health Records Management**

2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS) Naya Raipur, India. Oct 6-8, 2023

The content of this paper is to examine the challenges of EHR (Electronic Health Records) systems, such as the issues of security, privacy, interoperability and integrity of data, by proposing a blockchainbased decentralized platform. The new platform is purposed to explore the advantages of blockchain technology so as to upgrade the confidentiality, interoperability, and security of electronic health-records. It not only implements smart contracts but also pays special attention to consent and access control management to make sure the quality of the healthcare services and patients will be better.

### **3.2 Summary**

- The studies put forth the perspective of how decentralization could serve the health sector, by dwelling on aspects of standard interoperability, immutability, transparency, and traceability.

- Comprehensive assessment of the system, which will comprise the use of blockchain to increase security and privacy. Option 2 The proof of concept testing has been demonstrated with the metrics achieved during the development phase.
- Cryptography tools provide security along with transparency and immutability. Decentralization, which actually removes single points of failure, is an added advantage. Auditability and traceability are issues of accountability. And interoperability facilitates data exchange.
- Among the main challenges is that the centralized blockchain will become easily hack-able, thus, there will be no way for us to ensure the safety of health data.
- Scalability constraints also related to the visibility of data. When it comes to regulatory compliance there are many complexities. High costs and high level of complexity of installations process. Lack of standardized protocols. The same is with energy consumption, through continuously using Proof of Work POW consensus.
- Smart contracts usage: Majority of the papers focus on the application of smart contracts as a data leaser and their specific functions will often differ.
- Privacy preservation techniques: The protection of privacy vary in methods of offering privacy services such as encryption and access control.
- Integration with existing systems: Technologies that are different integrate with existing blockchain infrastructure in healthcare in different ways, but depending on standards and regulatory issue they vary.
- The fact that the model often only has limited real-world testing. Limitations in computing resources. Last but not least, the required higher security measures to respond to these vulnerabilities.
- Consensus mechanisms: Varying blockchain studies make use of more than one consensus mechanisms influencing their scalability and energy resources utilization.

## CHAPTER 4

### PROJECT REQUIREMENTS SPECIFICATION

#### 4.1 PROJECT SCOPE

##### **Introduction:**

The following paragraph is a brief general introduction that highlights why healthcare records security is of utmost relevance nowadays and assesses how integrating blockchain technology into this field is beneficial.

##### **Objectives:**

**The project aims to achieve the following goals:**

The aim to maintain the private and safe health data records of patients. Making it possible to store and share patient electronic healthcare records in a safe and easy way among entitled recipients. Improving data reliability and maintaining Network integrity against records falsification/tampering. The use of the interoperability interfaces as the vehicle of the information flow from one to another healthcare provider and systems.

##### **Technology Overview:**

This section will clearly explain blockchain and gives insight into how it is able to manage healthcare records by presenting an understanding of buzzwords like decentralization, immutability, and consensus mechanism.

##### **System Architecture:**

The blockchain technology is shown by a high level architecture diagram with the components and interactions of the record system of healthcare based on blockchain. It includes a description of each component, such as: It includes a description of each component, such as: User interfaces (for instance healthcare provider portal and patient portal). Nodes (e.g validators, miners) within blockchain network. Providing of Smart contracts for the sake of supervising the matters related to access control and data sharing permissions. Secondly a decentralized storage for large data sets (e.g., IPFS, BigchainDB).

## 4.2 FEATURES

**Immutable Record Keeping:** The use of blockchain immutable ledger and the creation of accurate and unalterable electronic health records is a support of their mission. After confirming and placing data on the blockchain it seals the details, therefore, the data cannot be altered or the information deleted.

**Decentralized Storage:** Restoring health records dispersion by developing the systems so that they are distributed across the multiple nodes within the blockchain network. These actions mean a more secured system with any point that may enable a large-scale intrusion having been diminished.

**Role-Based Access Control:** Utilize the role-based access control technique to set different levels of grants for disposers of data and change on the power of user based on their roles. This functionalities make it possible to the persons permitted to keep the records. The individuals are included, in this, are health care providers and patients. As the provision of a record-sharing consistency exist, an individual may include the non-patient entities also, such as their insurers and health authorities.

**Data Encryption:** Apply most advanced cryptography for records encryption of health records. This will shield from any unauthorized use to all the health info. Cryptographic security usually equips itself with an added measure of safety because an attacker, who successfully gets access to data storage, will not be able to decrypt the information with a brute-force attack without the encryption key.

**Auditable and Transparent:** Set up an information system based on the blockchain, which can collect timestamps and verify records via hashes and the aid from audit record trail. Auditing the documentation allows for transparency, accountability, and simplified life since the thorough description of changes in documents can narrate the history of changes, and serve as a proof of medical records.

**Consent Management:** Develop the schema with suitable actors in charge of the platform to grant patients the authority to allow or prevent the sharing of their health data. Healthcare providers and organizations worldwide should be equipped with credibility of being in favor of or getting patients admit to those situations when they have consent.



**Interoperability Standards:** Implement interoperable systems that can have seamless integration as the healthcare sector follows the standard interoperability protocols of other providers for effective exchange and use of information. HL7 FHIR as a platform standards promote ongoing evolution and ensure that data flows smoothly across disparate systems, therefore, promoting interoperability.

**Smart Contracts for Authorization:** Through smart contracts, which automate the authorization procedures and the access control rules on the blockchain, we can enable self-private data transactions. Smart contracts are not only for the storage of data but also for self-execution of predefined responsibilities and functions, for example, to provide or refuse access to health care records based on given conditions.

**Data Recovery and Backup:** Put in place strong recovery data and backup mechanism to make sure the availability of healthcare records in case the system crashes or natural calamity. Frequent backups and the use of redundant storage configurations decrease significantly the fact of data loss and let you always get at the extremely important medical data.

**Compliance with Regulations:** Make sure that all regulations related to healthcare systems and data protection as in the HIPAA (Health Insurance Portability and Accountability Act) for the United States or GDPR (General Data Protection Regulation) for the European Union are being complied with. Observing of the laws is key to ensure safekeeping of privacy and legal immunity from legal ramifications.

## 4.3 USER CLASSES AND CHARACTERISTICS

### 4.3.1 Healthcare Providers

**Characteristics:** The term health providers seems to cover doctors, nurses, clinicians and all other workers providing care, information and storing the patient records. Affording the patient information, and in the way the patient association gets the required data safely protected while promptly accessible every time, is the leading requirement. Needs: The healthcare providers are into integrating BTC into their confidentiality and properly designed user interphases which facilitate access to patients' records and interpersonal linkage with other healthcare systems in order to streamline the clinical delivery to the advantage of the patients.

### 4.3.2 Patients:

**Characteristics:** This group contemplates the people whose health aspects are all safeguarded and guarded. Thus, the issue of privacy with regard to personal health data is doubtlessly of greatest concern for patients.

**Needs:** They focus on issues of privacy, doing with records keeping, and control. Patients demands of security to access their medical data, and possible consenting and sharing mechanism of it with providers, and assurance of their safety from attackers and tampering is being questioned.

### 4.3.3 Healthcare Administrators

**Characteristics:** Healthcare administrators/managers play an important role in health care: the operations, governance, and compliance of healthcare organizations are under their supervision. They are cherry picking where they dwell, preferences for hospitals, clinics, etc. **Need:** These clinicians demand a comprehensive system for record management for HIPAA or such, regulation compliant, and security over a data breaching or unauthorized access. These attributes are equally important, and thus, such health records require certain attributes, including scalability, transparency, and risk management, which healthcare record blockchain systems offer.

### 4.3.4 Regulatory Authorities

**Characteristics:** They make rules for different security levels and data privacy in the healthcare field in order to protect all medical/healthcare-associated data and patient rights. On this basis, they need to create a policy which allows for fair and secure sharing network while protecting and giving access to patient data. Blockchain Developers and Technologists

**Description:** Fabricated on blockchains, Blockchain developers and technologists work on the whole game-dev cycle iterative approach of blockchain solutions development for hospitals.

**Needs:** so blockchain engineers and tech specialists need to be able to build systems with blockchain protocols, crypto and distributed ledger technologies, secure, interoperable and scalable, to store healthcare records properly. I feel that the involvement of blockchain developers can intensify,

whenever there is a situation where the developers' strategies can mesh with those of other health stakeholders, there is an adaption to industry standards and proactive development of solutions based on blockchain technology.

## 4.4 CONSTRAINTS, ASSUMPTIONS AND DEPENDENCIES

### 4.4.1 Constraints:

- a. Regulatory Compliance:** The e-health records are digitized and private information concerning the patient, therefore, they must follow the privacy law and regulation of the Health Insurance Portability and Accountability Act (HIPAA) in the U.S, General Data Protection Regulation (GDPR) in the European Union and other data protection laws around the world. Compliance with theregulations also means the possibility of imposing a penalty and the loss of the trust and reputation.
- b. b.Performance:** Compared to traditional databases, transactions in the blockchain take more time and consumed more resources. Consequently, the designed solution should be operationally successful as well as consistent with high performance standards.
- c. Interoperability:** An issue that may be encountered is integrating current systems with the blockchain-based health records might not be very smooth, as well. Therefore, a network solution is mandatory for the companies in order to offer either network systems or platforms that can facilitate such a campaign. Costs: It is possible that development, operation, and keeping a blockchain-based system going might be the most expensive thing.
- d. Scalability:** It is problematic due to a consensus mechanism, data replication to multiple nodes and other factors, which make the systems on blockchain networks weakly scalable. We will also have to keep in mind that aesthetics is another factor.

### 4.4.2 Assumptions:

- a.User Adoption:** That the system's blockchain will be able to be implemented successfully by healthcare providers, patients and other players by the fact that, there is passion and seriousness about adopting patient-centered care.' In the absence of technical support, students may be concerned

to use the system on schedule.

**b.Data Accuracy:** Obviously, I would hope that all teams will feed the correct data to the system. Therefore, distrust of the data could lead all parties opt for not to trade on the system as they might get stuck in the trap of the fraudulent transactions. Moreover, the protective measures like a verification system and data processing systems should be created in order to stop this.

**c. Secure Environment:** As an add-on, I am certain that the system's prerequisite infrastructure and its talk services should be secured to some extent to eradicate unauthorized access, system breach, and disaster spread of malicious programs.

## 4.4.2 Dependencies:

**a. Blockchain Platform:** It is the functionality of the system which is expected to be oriented either towards Ethereum or Hyperledger Fabric, that determines the set of features such as smart contracts and consensus algorithm. In order to do that, simply use the platform dependent features, APIs, and development tools, as it can be a high useful instrument.

**b. Third-party Services:** Third-party services including cloud, cryptography libraries, and identity management systems creates this scenario which may unwarily expose our services to several dimensions of risks. Guaranteeing that nodes in the network will produce correct data and make sure that the integrity of the entities are key elements of making the ecosystem secure.

**c. Integration Points:** One of those integrations is the internal system's integration with othersystems using links and buses as intermediaries. The new health care info technology integrated system should be capable of concurrently unite with the existing one in order to eliminate complexityduring data exchange process and thus increase interoperability.

**d. Regulatory Changes:** The hesitation with regulatory policies undergoing regular changes and the rules system, alongside data security, privacy and regulation requirements will be updated. It should be pointed out simply that regulatory monitoring is crucial as far as the observe of the law requirements is infringed.

## 4.5 FUNCTIONAL REQUIREMENTS

### **Input Validation and Data Verification:**

- Navigate within the data to confirm that all data (being) presented is in concordance with preset structures and formats.
- Confirm whether input data is genuine or has been tampered with by applying methods of cryptography like digital signatures or hash functions.
- To ensure that there is no unauthorized entry or alteration, consider permissions together with access controls attached on inputted information.
- Check if data input is real or that it's been modified, by using cryptographic algorithms like digital signatures or hash functions.

### **Data Encryption and Decryption:**

- When authorized individuals want healthcare records or engage in transactions, safely decode coded information.
- Before saving them in blockchain, encode private medical files besides transaction records. Employ robust encryption algorithms as well as cryptographic keys so that confidentiality is maintained while restricting admission into certain details.

### **Smart Contract Execution:**

- Blockchain to supply as a bounded and codified platform for smart contracts trimmed to set up access policies, consent requests and contract execution.
- Confirm the accuracy of healthcare providers, patients or other stakeholders who will be viewing the records by using smart contracts for authentication.
- In the contracts mentioned above, write business rules to facilitate user consent management, data sharing, and audit trail generation.

## **Consensus Mechanism and Transaction Validation:**

- Establish the algorithm for the validation of a healthcare data blockchain transaction and present the blockchain history integrity.
- The blocks containing the healthcare information will be transmitted into the system only if there is approval from all the network's members (consensus).
- Proof of Work (PoW) or Proof Of Stake algorithms are the examples that officers have to verify the implementation and execution conflicts

## **Auditability and Transparency:**

- Transparency and traceability of all transaction activities on blockchain are not optional, but obligatory and are seen by anyone involved.
- The blockchain is supposed to be transparent. Therefore, keep an auditable record of every transaction that happens on the blockchain, including who and when transacted, and why they did it.
- Make the logs which automatically permit tracking of medical records, what information has been changed there, and activities connected with enlisting consent from patients.

## **Integration with Identity Management Systems:**

- Render the integration with the ID management systems and enable users authenticate and verify their identities in order to allow them to access their medical records.
- Enhance security and block unauthorized access to systems with multi-factor authentication approach combining new technology like biometrics.

## Error Handling and Exception Management:

- Develop rules of fault detection to specify the wrong inputs, the correction procedure or avoidance methods of errors in addition to exceptions.
- Implement tactics of recovering from an error so that it brings back the whole system into a consistent state which is also dependable.
- Informative error messages should be given together with notifications when the system fails in validating information during transaction or malfunctions at any point.

## 4.6 HARDWARE REQUIREMENTS

### Server Infrastructure:

**High-performance Servers:** The nodes on the blockchain should have strong servers that can manage transaction data, embody the data, and encrypt it too.

**Redundancy and Scalability:** For ongoing operation, the capacity of providing backup of failover failure and making necessary adjustments to cope up with increased volumes of information storage is mandatory by the enterprise.

**Enterprise-grade Storage:** The NAS or SSD that is equipped with an anti-virus system will be utilized to store health data after an encryption procedure has been carried out.

### Block Chain Nodes:

**Scattered Nodes:** The block chain network organizes around many nodes not connected and are responsible for all the deals registration and recording. They may be hosted on server nodes located in dedicated data centers or on cloud platforms.

**Node Communication:** P2P networking includes the TCP/IP protocols that are used by nodes in communicating with one another and to agree on transactions information and keep things same on both ends.

## Network Infrastructure:

**Protected Network Construction:** The data journey should be under tight security and security is provided by setting up a firewall, a system that identifies intruders (IDS), among others encryption such as SSL/TLS.

**High-speed Internet Connection:** Litecoin uses SPV (simplified payment verification protocol) for channeling real time data transmission and block chain synchronization. Therefore, incredible speed internet connectivity has to be not only reliable but also available.

## Client Devices:

**Desktop Computers:** Healthcare experts shall use computers with a desktop or station, which is equipped with web browsers or specialized clients to access the online system.

**Mobile Devices:** The use of mobile phones, tablets and others could be promoted through mobile specialized apps or interfaces.

**End-user Devices:** Stable interaction that applies to medical devices and IoT sensors gathering and transferring the healthcare data to the control center may be feasible with end user device participation.

## 4.7 SOFTWARE REQUIREMENTS

### Blockchain Platform:

**Name and Description:** Healthcare record is managed by Ethereum or Hyperledger Fabric which are mostly used blockchains, such platforms.

**Version / Release Number:** The point versions is variable;ethereum is one of the several examples, it is the one and only Ethereum 2.0.

**Databases:** If you are a blockchain platform, you are fat-free, and thus you have your own distributor ledger database (e.g. levelDB for Ethereum).



**Operating Systems:** Backing most used operating systems like Linux, Windows, and Mac OS this is the most important point.

**Tools and Libraries:** Solidity (Solidity) for smart contract development (Ethereum), Chain-code (Hyperledger Fabric) for smart contract development, and web3.js for Ethereum blockchain interface.

## **Database Management System (DBMS):**

**Name and Description:** MongoDB, PostgreSQL, or any RDBMS or NoSQL databases for the storage of the regular non-blockchain data.

**Version / Release Number:** On the other hand, however, data models changes as the DBMS is chosen also.

**Databases:** The non-digital data such as user accounts details, access logs, search results or buy history, are all an integral part of these systems.

**Operating Systems:** Work with Windows and macOS, which are the systems that run current computers.

**Tools and Libraries:** Because ORM frameworks like Sequelize for Node.js, native database drivers, or others might be used.

**Source:** They can be distributed as free software available online or via app stores.

## **Application Layer:**

**Name and Description:** Engaging in creating custom tools both web and mobile apps to support the use of blockchain and records.

**Version / Release Number:** These could reportedly be connected with development, updates or just anything else.

**Databases:** The interface should be developed between the blockchain ledger and the DBMS that can respond to any queries regardless of the information content such as user's access, permissions, and metadata.

**Operating Systems:** One attractive feature of web applications is their portability. They can be used on any hardware platform and run through an updated browser. The applications are either for iOSs or for Androids.

**Tools and Libraries:** Building UI with React.js, Angular, or Vue.js. Using Node.js or Express.js for backend development. Swift or Kotlin application development for mobile.

**Source:** Being done internally or with an external development agency.

## **Security Components:**

**Name and Description:** Authentication and authorization partitions, encryption libraries or compliance equipment.

**Version / Release Number:** This applies in diverse ways, when considering the fact that different libraries and technologies are applied in construction of different versions.

**Databases:** File store access permissions, encryption keys, and audit logs.

**Operating Systems:** Suitable for different operating systems and available on many operating systems.

**Tools and Libraries:** OAuth2 for authentication, JSON Web Token for authentication, Open-SSL for encryption, Vault HashiCorp for secret management.

**Source:** Various are free of charge or open source, while some may be proprietary or provided by third-party vendors.

## **Integration Layer:**

**Name and Description:** Middleware or integration services for hooking them to external systems and APIs.

**Version / Release Number:** It's a platform specific thing and it might be the middleware or the integration tools that are being used.

**Databases:** Provide carrier services such as message queues or caching systems for better data optimization.

**Operating Systems:** Also, can be adapted to major operating systems.

**Tools and Libraries:** Used of Apache Kafka, RabbitMQ, or Redis for message queuing and RESTful APIs for external integration.

**Source:** Open-source or purchased software solutions.

## **4.8 NON-FUNCTIONAL REQUIREMENTS**

### **4.8.1 Performance Requirement**

**Reliability:** The database should be dependable in handling healthcare records, making sure that they are retrievable and free from any errors as well as data loss.

**Robustness:** The program should be good enough to rule out, exceptions and error circumstances without risk of compromising the data as well as being crashed.

**Availability:** The system should be available round the clock with the bare minimum of downtime for relevant maintenance or upgrades carried out periodically, it will assure healthcare professionals to have access to the patients' records whenever necessary.

**Scalability:** The system needs to have the mechanism of huge scale without any compromise on performance when the number of users, records, and transactions are becoming higher by time.

**Throughput:** The machine should be provided with the ability to perform large numbers of transactions to cater for the demand in cases where a large number of people may be requesting access to services at the same time without performance degradation.

**Latency:** The time taken to process health data should be reduced in order to enable fast and easy access to health care records and services.

## 4.8.2 .Safety Requirements

**Encryption:** The encryption of all medical information and sensitive data must be implemented during the data transfer and encryption of data storage to avoid the control by unauthorized persons.

**Access Control:** Create interface control mechanisms that differentiate the access to a patient's these reports based on the user role and permission.

**Disaster Recovery:** Back up data should be performed on a regular basis and have a schedule that outlines the disaster recovery process in order to decrease the risks of data loss due to outage or event that may bring unfortunate results to our technological assets.

**Audit Trails:** Conduct all-encompassing information logs to account for activity, modifications, as well as they are authorized made in healthcare records maintaining security and legislative operation.

## 4.8.3 Security Requirements

### Identity Authentication Requirements:

- Make use of MFA as the central component of a complex risk management.
- Develop strong password guidelines such as changing passwords after every few months.

It is advisable to use different password for each accounts.

- Furthermore, users should have an easy access permission management in order not to be denied access at no reason.
- A genuinely safe transmission protocol, can be SSL/TLS which encapsulate data transmission between client devices and the server constituents, is just in order.
- Apply the blockchain technology solution which keeps the record of transactions safe and staunch, meaning the provenance and privacy of traders would be secure and any edits and deletions nullified.

## 4.9 OTHER REQUIREMENTS

**Scalability:** Develop the system to be scalable whereby it is both Scale horizontally and vertically such that as the load grows and the user base expand the service provider can incorporate more storage space in the future.

**Maintainability:** It should be perfect, modular, clear in documentation that will provide easy solution by means of fixing the bugs and enriching their function.

**Portability:** Declare the platform capacitance of the system being realizable on different operating systems and environments, and cloud and in-house deployment as well as hybrid infrastructure are also supported.

**Interoperability:** Establish an interface that is perceived as conversational with the existing healthcare IT infrastructure and standards and, thus, could communicate and allow data integration with the systems from the outside.

**Regulatory Compliance:** The system has to be audited for strict compliance with healthcare regulations and standards among them HIPAA (Health Insurance Portability and Accountability Act), as well as GDPR (General Data Protection Regulation) whose main objective is to shield patient's data from unauthorized access and to assurance its safety.

**User Training and Support:** The training materials should have comprehensive schedules and guide users to get accustomed to the operations of system inventories and the best record management procedures as well.

## CHAPTER 5

### SYSTEM DESIGN

#### 5.1 High Level System Design

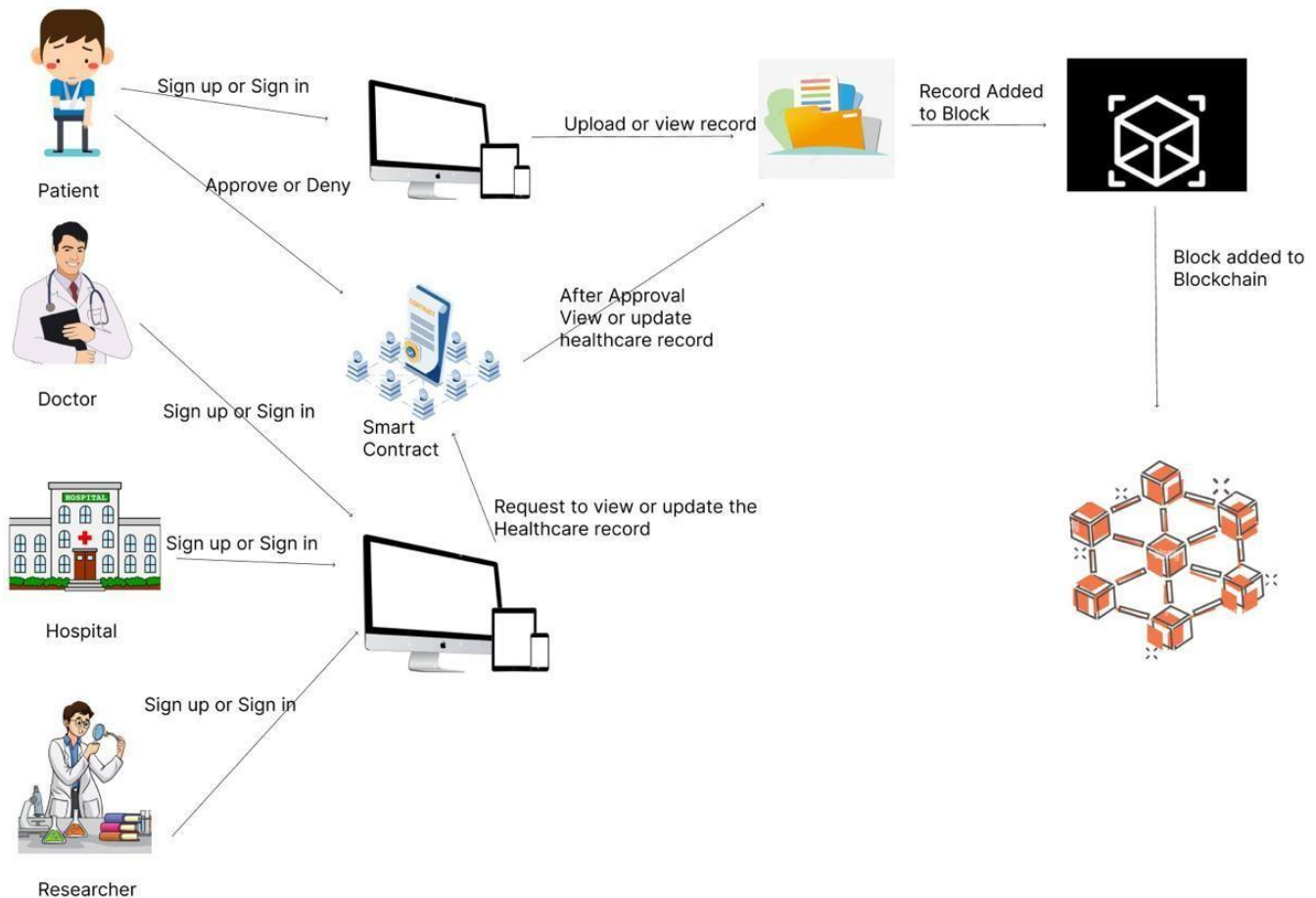


Fig 5.1 – High level architecture

## 5.2 Master Class Diagram

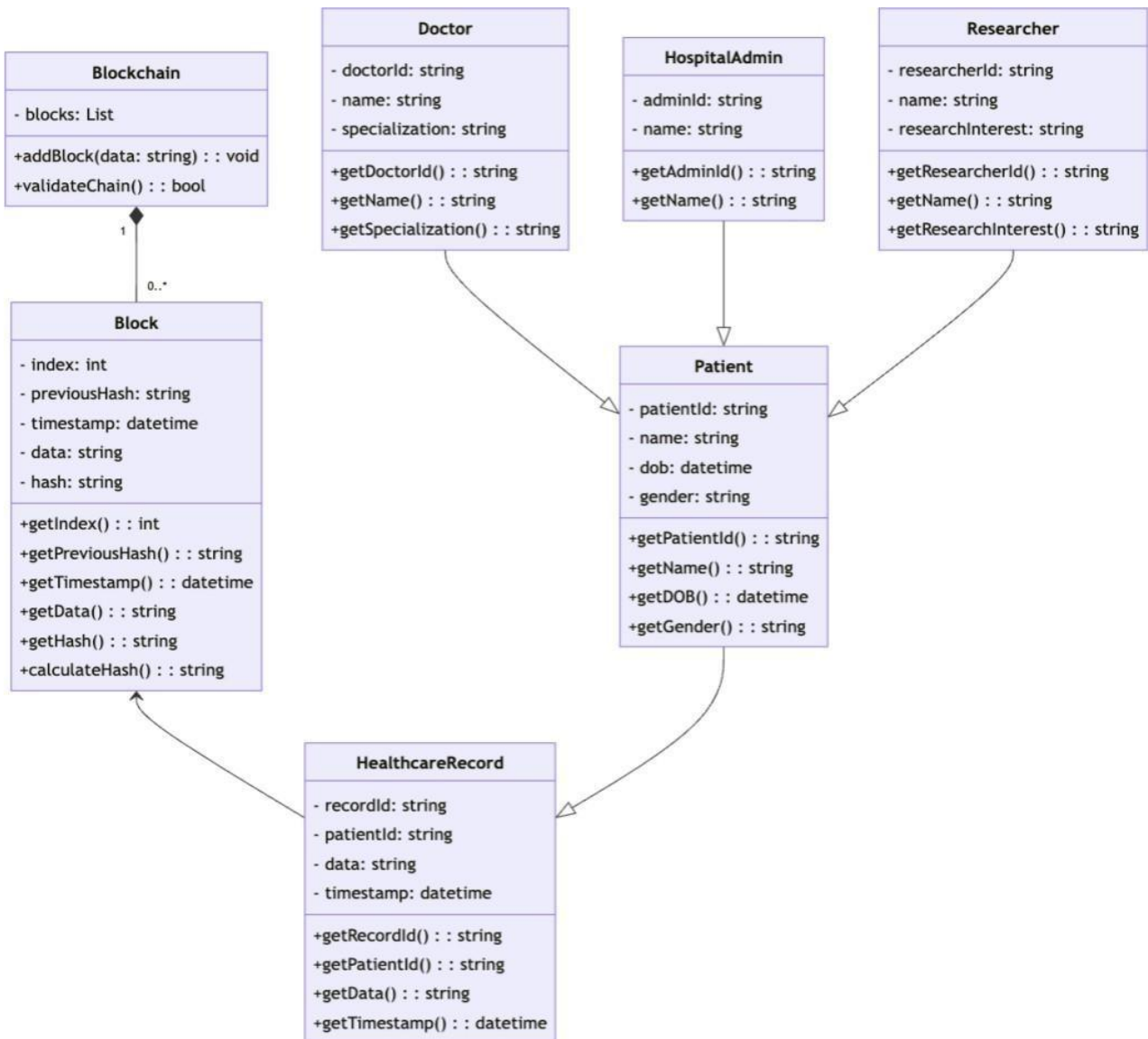


Fig 5.2 – Master class diagram



## 5.3 E-R Diagram:

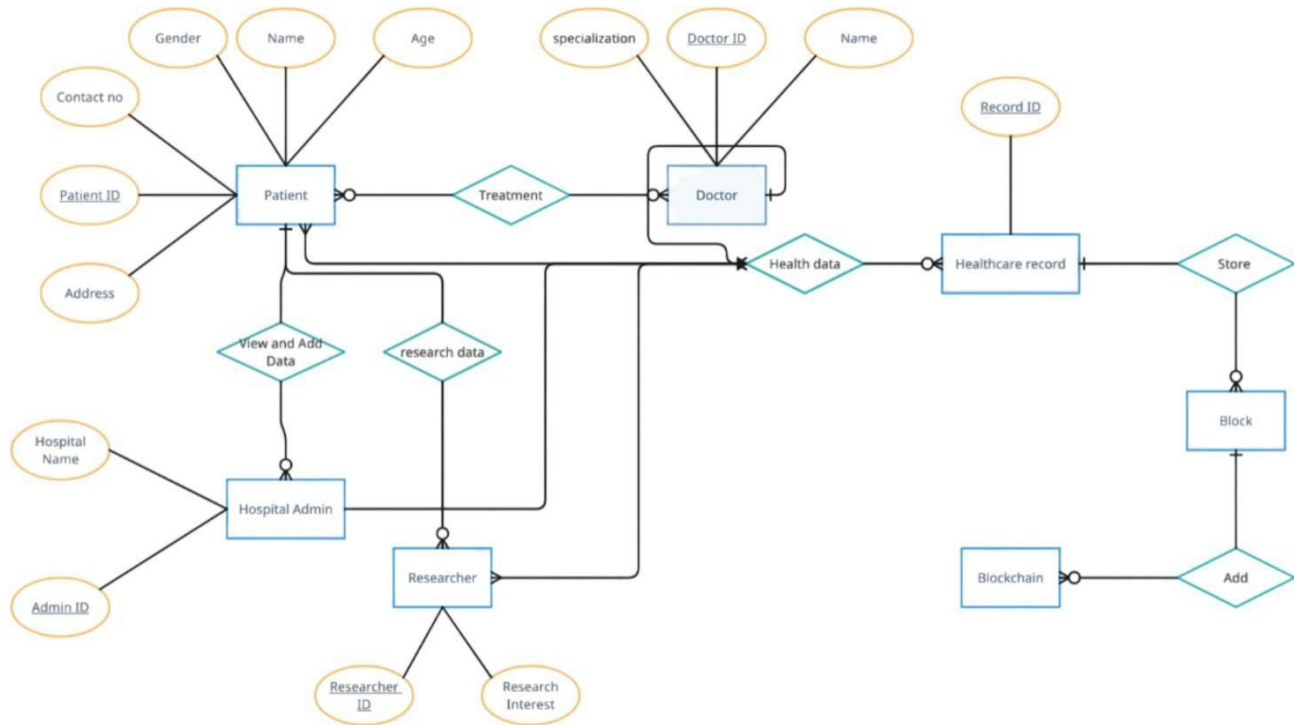


Fig 5.3 – State diagram

## 5.4 User Interface Diagrams

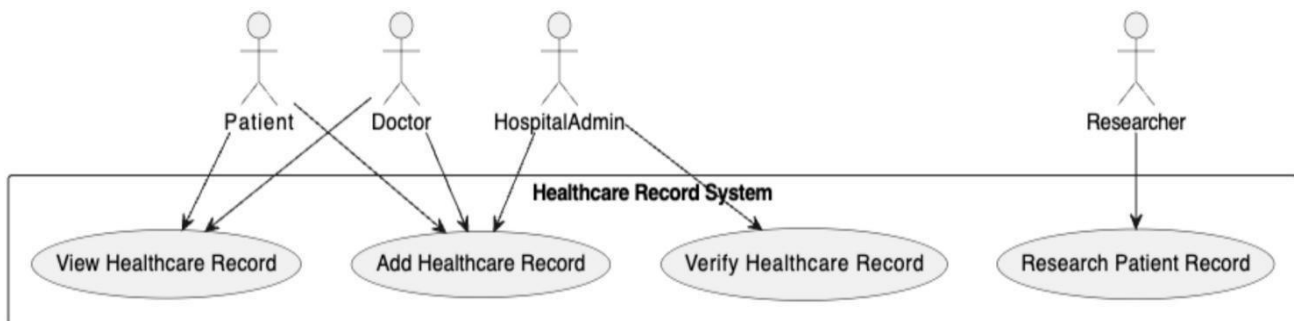


Fig 5.4 – Use case diagram

## 5.5 Flow Daigram:

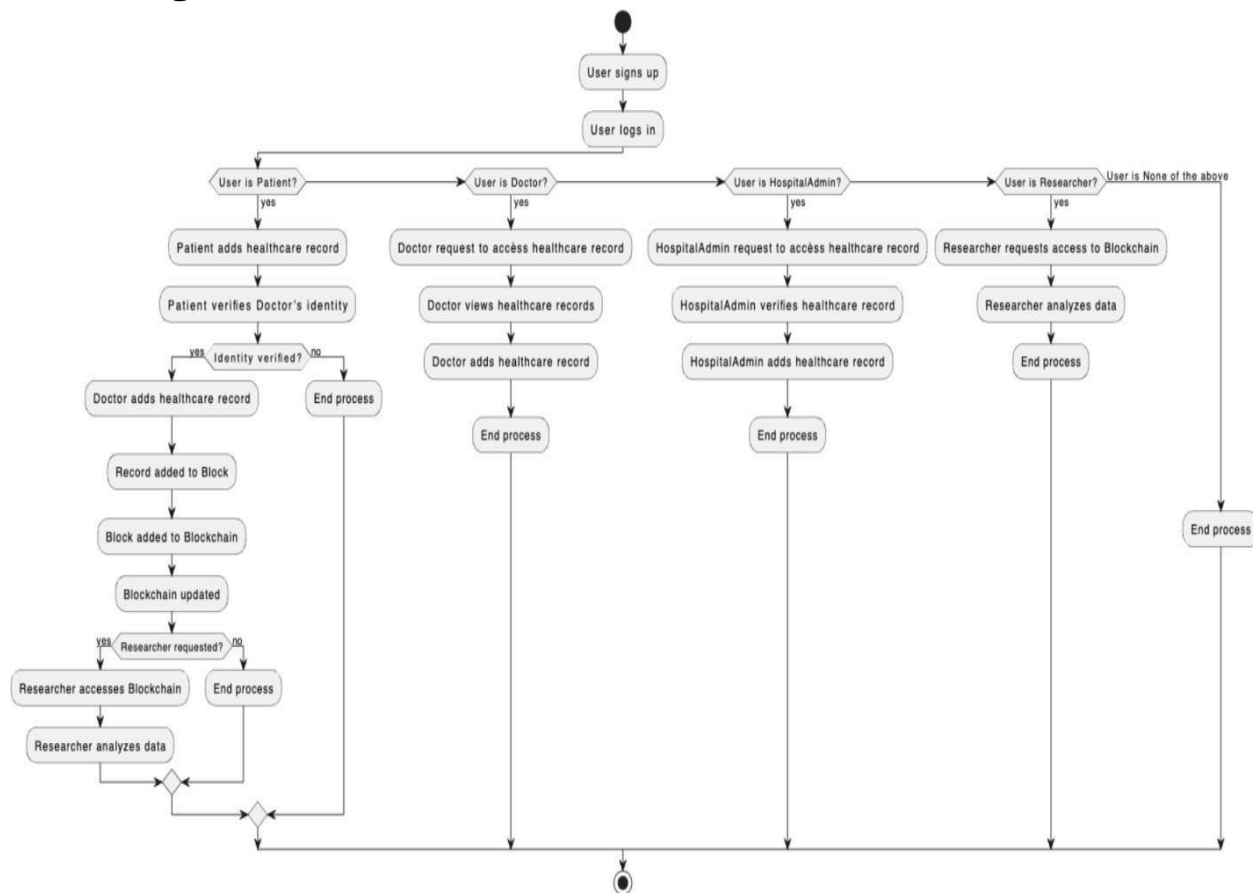


Fig 5.5 - Flow Daigram

## 5.6 DESIGN DETAILS

**Novelty & Innovativeness:** Make use of the emerging blockchain technology that stands for enhanced data security and confidentiality of information.

**Interoperability:** Forming and implementation of the regulations incorporating the data transfer among different health information networks, while preserving the safety of the data transferred.

**Performance:** Enhancing network blockchain properties (speed and scalability) in that they can handle a great amount of healthcare data transactions without slow down.

**Security:** Supporting cryptographic practice which would help to protect identity of patients and medical information of the negative access.

**Reliability:** The reliability of having healthcare records permanently stored on widespread and redundant blockchain networks shall be ensured through blockchain technology.

**Maintainability:** Establish the communication routes that are supposed for providing the maintenance and updates that might be able to cure the holes in the integrity of the system.

**Portability:** Moreover, architecture of the blockchain solutions which should be simple so that they are easily implemented across various healthcare settings and platforms.

**Legacy to Modernization:** The movement from the older record storage facilities in the healthcare system to the blockchain aimed solutions, this will result in the migration and integration of data.

**Reusability:** Assembling modular blockchain constituents that could later be re-assembled in different health services and organizations.

**Application Compatibility:** Establishing compatibility with already used healthcare software and platforms which would make implementation processes easy to implement by different providers.

**Blockchain Technology:** At the very center of all this lies the blockchain which is a decentralized and distributed digital ledger. It accomplishes this purpose by safeguarding, ensuring the integrity and providing the transparency of the health records. Healthcare applications will necessitate every application specific blockchain platforms for instance: Ethereum, Hyperledger Fabric; among other on the market.

**Healthcare Information Systems:** Since these system storage both healthcare record and Electronic Health Records (EHRs) and Personal Health Records (PHRs). The processors should be compatible with the blockchain platform for data to be transferred continually between the chain and the processing system.

**Smart Contracts:** These are smart contracts with code embedded and containing what the agreement demands. They provide procedures through which the physician and the rest of healthcare professionals grant access to healthcare records by making ideas of data privacy and security prevail.

**Identity and Access Management Systems:** These systems take care of identities of healthcare providers and patients, therefore, persons with specific information types can only be given access to specific healthcare records.

**APIs:** Achieving interoperability would be impossible without application programming interfaces (APIs) to connect diverse systems of blockchain platform, health information systems, and identity and access management systems.

**Cybersecurity Measures:** The very significant need for more cyber security while ensuring the secrecy of the blockchain network at the same time is one of the greatest challenges the entire system faces. Here, one must consider various things such as encryption, firewalls, intrusion detection systems and audits from time to time.

**Regulatory Compliance:** Complying with healthcare regulations, like HIPAA within the U.S must be carried out. Such a measure can be accomplished through tasking (if it is required) or conducting regular audits (if the data is sensitive).

**User Training:** Putting together enough coaching to healthcare workers and patients about the working of the system is a prerequisite for correct usage of the system and common understanding of the security measures implemented.

**To make these systems more effective and efficient, vital changes may include:**

**Upgrading Legacy Systems:** The removal of the obsolescent system in place and replacing it into the platform with brand new ones which are able to translate each other.

**Improving Performance:** Being able to process large volumes of data and a lot of transactions, which will be implemented on the blockchain platform in order to focus on scalability.

## CHAPTER 6

### PROPOSED METHODOLOGY

#### **Decentralized Data Storage Solutions**

**IPFS (InterPlanetary File System):** Use IPFS for storing health care data in a distributed fashion. Contains Patient files as encrypted documents whose access can only be granted through specific IPFS hashes. This eliminates cases of data alteration and ensures high levels of confidentiality.

**Blockchain Storage:** Only keep the references (IPFS hashes) and the metadata on the blockchain, since this will reduce the level of on-chain data and still be efficient, durable and cost-effective since large files are not directly stored on the blockchain.

#### **Data Access Control**

**Smart Contracts as a Tool for Access Management:** Make use of smart contracts for management of access privileges. These contracts can also be used to give or restrict data access rights to health care providers and even to patients or insurance companies.

**Role-Based Access Control:** Use smart contract to specify certain roles e.g. patient, doctor, insurance and assign corresponding permits. Only users with valid permits will be able to access the data and information.

#### **Privacy through Encryption**

Administer the healthcare information held in documents through manipulation of Word Templates. Draft encryption policies that stipulate how healthcare records shall be uploaded on the word processing software.

**Data Encryption:** The healthcare records physician or any other authorized person uses should be encrypted before uploading to IPFS. The authorized organizations holding the encryption keys can provide them to the required users through smart contracts allowing only users with valid keys to decrypt the data and see the healthcare records.

**Private Keys:** Allow patients to manage and own their data through encrypting it with their private keys, hence can select who can access their data.

## Identity Verification and Authentication

Verification of identities of users (patient, doctor, insures) using DID systems. DIDs provide an extra layer because only verified users can view or change the information.

**Authentication Mechanism:** Using self-sovereign or blockchain wallet identities, authenticate access control using various protocols.

## Data Integrity and Auditing

**Hashing for Data Integrity:** Maintain data consistency through data hashes on the blockchain. Every healthcare record is hashed before the upload and the hash puts on blockchain. Changes in the data will yield a different hash thus aiding in the detection of illegitimate modifications.

**Audit Trails:** For every activity (creation, access, modification or deletion) related to healthcare documents, it is important to record those transactions in the blockchain. The measure improves the security aspect of the data as trust is automatically ensured.

## Payment System for Services

**Smart Contract Based Payments:** Use Eth to buy the contract and allow for payment of healthcare data access. Eth can be sent by healthcare providers to access data, and such a transaction can be set to activate the corresponding access rights within the contract.

## User Interface and Integration

**Frontend UI:** Provide a clear graphical interface that will enable the user to access their records, set limits on authorizations and perform their payments. Tools such as React should be employed on the front end to cater for such interactions with the users.

**Integration with Existing Systems:** Highlight the merge with the existing Blockchain based solution to the IT infrastructure of the healthcare administrators to promote its uptake. This could be through standards based interface with health information systems such as HL7 FHIR through APIs, or through bespoke mapping of such standards.

## **Compliance and Data Privacy**

**GDPR and HIPAA Compliance:** Design such that there would be respect to the law including GDPR, HIPAA and others, by considering privacy by design, dealing with requests for deletion of certain data, and tracking changes to the systems.

**Data Ownership:** Data will belong to the patients, who should be able to grant or retract their consent in whatever fashion, thereby upholding privacy and control.

## **Implementation Overview**

**Smart Contracts:** There is a need to create a smart contract that will handle the access control management, give permissions, and enable payments on the Ethereum network or any similar network.

**IPFS Integration:** IPFS must be connected for the storing of off chain data and use of hashes to secure link those data to smart contracts.

**Front-End Application:** Design the front end in React framework which will take care of the end users and their needs, while for blockchain interactions, Ethers.js will be employed that is the management of the Ethereum blockchain.

**Security Audits:** Make security audits of smart contracts cos, data flow to prevent vulnerabilities and breaches.

## CHAPTER 7

### IMPLEMENTATION AND PSEUDOCODE

#### 7.1 Implementation Steps

##### 7.1.1 Technology Stack

**Solidity:** Smart contract programming language used to write the healthcare record system.

**Ethereum:** The blockchain platform where the smart contract is deployed.

**IPFS/Pinata:** Decentralized storage solution for off-chain storage of healthcare data.

**Remix IDE:** A web-based Solidity development environment for writing, testing, and deploying smart contracts.

**MetaMask:** A browser-based Ethereum wallet used for managing accounts and interacting with the blockchain.

**Web3.js or Ethers.js:** JavaScript libraries for integrating the smart contract with a front-end React application.

**Ganache:** A local blockchain emulator used for testing the smart contract.

##### 7.1.2 System Design

**Role-based Access Control:** Users are assigned different roles (Patient, Doctor, Hospital Admin, Researcher), each with specific permissions in the system.

**Smart Contracts:** Used to manage healthcare records securely, enforce access control, and provide audit trails for every interaction.

**Decentralized Storage (IPFS/Pinata):** Healthcare records are stored off-chain to ensure scalability, while only the hash of the data is stored on-chain for verification.

##### 7.1.3 Steps for Implementation

###### Development of Smart Contract:

The Solidity contract code for the healthcare record system was written and tested locally using the Remix IDE. This contract includes the functionality for adding, viewing, and verifying healthcare



records, as well as enforcing access control based on user roles.

## **Deployment:**

The smart contract was deployed to an Ethereum test network (such as Ropsten or Goerli) using MetaMask and Remix IDE. During deployment, we initialized the contract by assigning initial roles (e.g., HospitalAdmin, Doctor, Patient).

## **Integration with IPFS:**

To handle large healthcare records, the data was stored off-chain using IPFS or Pinata. The smart contract only stored a hash of the healthcare record, while the actual data was saved in IPFS.

## **Example IPFS interaction:**

```
const ipfs = require('ipfs-http-client');

const ipfsClient = ipfs.create({ host: 'ipfs.infura.io', port: '5001', protocol: 'https' });
const fileHash = await ipfsClient.add(healthcareData);
// store `fileHash` in the blockchain smart contract
```

## **Frontend Application (React):**

A React application was built for interacting with the deployed smart contract. Using Web3.js or Ethers.js, users (patients, doctors, admins) could log in, add records, view records, and validate access permissions.

The app allowed users to upload healthcare data to IPFS/Pinata, generate a hash, and then interact with the smart contract to store this hash on the blockchain.

## **Testing with Ganache:**

Before deploying to a testnet, the smart contract was tested using Ganache, a local blockchain emulator, to ensure proper behavior of role-based access, record addition, and viewing.

## **7.1.4 Key Components**

**Assign Role:** The hospital admin assigns roles (Doctor, Patient, Researcher) using the assignRole() function.

**Add Healthcare Record:** Doctors add healthcare records (with a reference to IPFS hash) using the addHealthcareRecord() function.

**View Healthcare Record:** Patients and authorized doctors can view healthcare records using the viewHealthcareRecords() function.

**Anonymized Data for Researchers:** Researchers can access anonymized records using viewAnonymizedRecords() function for research purposes.

## 7.1.5 Models used in Pseudocode

### 1. UserSignUp

**Model:** User Authentication with Fee

**Purpose:** Handles user sign-up and sign-in processes with a required payment (sign-up/sign-in fee).

### 2. Payment Contract

**Model:** Payment and Withdrawal System

**Purpose:** Facilitates Ether payments and provides withdrawal functionality.

### 3. MessageApproval

**Model:** Message Approval System

**Purpose:** Enables sending, approving, and denying messages between users with tracking and auditing.

## 7.2 Pseudocode

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract UserSignUp {
    uint256 public signUpFee = 0.001 ether; // Fee for the sign-up and sign-in process

    event OnUserSignedUp(address user);
    event OnUserSignedIn(address user);

    // Sign-up function that requires payment
    function signUp() public payable {
        require(msg.value >= signUpFee, "Not enough ether for sign up");
        emit OnUserSignedUp(msg.sender);
    }
}
```

```
// Sign-up function that requires payment
function signIn() public payable {
    require(msg.value >= signUpFee, "Not enough ether for sign in");
    emit OnUserSignedIn(msg.sender);
}

// this function allows to transfer the balance of the smart contract
function withdraw() public {
    payable(msg.sender).transfer(address(this).balance);
}
}
```

```

/  :  SPDX-License-Identifier:  MIT
pragma solidity ^0.8.0;
uint agreement of medical treatment store;
// Event to log payments
event PaymentReceived(address sender, uint256 amount,);

function pay() external payable {
    require(msg.value > 0, "Payment must be greater than zero.");
    emit PaymentReceived(msg.sender, msg.value);
}

// Withdrawal Function (onlyOwner can withdraw
function withdraw() public {
    // Only the contract owner should be able to withdraw funds
    payable(owner).transfer(address(this).balance);
}

// Fallback function to receive Ether
receive() external payable
emit PaymentReceived(msg.sender, msg.value);
}

// Owner of the contract
address public owner;

constructor() {
    owner = msg.sender; // Set the deployer as the owner
}
}
```

END

```
//  SPDX-License-Identifier:  MIT
pragma solidity ^0.8.0;
```

```
contract MessageApproval {
    // Structure to store message data and status
    struct Message {
        address sender;
        address recipient;
        string content;
        bool isApproved;
        bool isDenied;
    }
    // Mapping to store messages by ID
    mapping(uint256 => Message) public messages;

    // Event to notify when a message is sent
    event MessageSent(uint256 messageId, address sender, address recipient, string
        content);

    // Event to notify when a message is approved
    event MessageApproved(uint256 messageId);

    // Event to notify when a message is denied
    event MessageDenied(uint256 messageId);

    uint256 public messageCount;

    // Send message
    function sendMessage(address _recipient, string memory _content) public
    { messageCount++;
        messages[messageCount] = Message(msg.sender, _recipient, _content, false, false);
        Emit MessageSent(messageCount, msg.sender, _recipient, _content);
    }

    // Function to approve a message
    function approveMessage(uint256 _messageId) public
    { Message storage message = messages[_messageId];

        require(msg.sender == message.recipient, "Only the recipient can approve the
            message.");
        require(!message.isApproved, "Message is already approved.");
        require(!message.isDenied, "Message is already denied.");

        message.isApproved = true;

        emit MessageApproved(_messageId);
    }

    // Function to deny a message
    function denyMessage(uint256 _messageId) public
    { Message storage message = messages[_messageId];
```

```
        require(msg.sender == message.recipient, "Only the recipient can deny the
            message.");
        require(!message.isDenied, "Message is already denied.");
        require(!message.isApproved, "Message is already approved.");

        message.isDenied = true;

    emit MessageDenied(_messageId);
}

// Function to get message details
function getMessage(uint256 _messageId) public view returns
    ( address sender,
      address recipient,
      string memory content,
      bool isApproved, bool isDenied
    )
{
    Message memory message = messages[_messageId];
    return (
        message.sender,
        message.recipient,
        message.content,
        message.isApproved,
        message.isDenied
    );
};
```

## CHAPTER 8

### 8. RESULTS AND DISCUSSION

#### 8.1 Results

With the blockchain, securing health records gets several noticeably achieved results with some benefits and challenges. Here is an outline of the findings and key considerations:

##### 1. Better Data Security and Integrity

**Outcome:** This is actually storing healthcare records on IPFS in an encrypted format, while the file hashes get recorded on a blockchain, this assures data immutability and can't allow unauthorized tampering.

**Discussion:** This minimizes the risks of data breaches and unauthorized alterations. The blockchain stores immovable hashes; therefore, any such alteration of the data is easily detectable to provide authenticity and integrity to the patient's records.

##### 2. Decentralized Data Control

**Impact:** Patients retain ownership and control over their data. Access is granted or denied through smart contracts.

**Discussion:** With decentralized control, it will allow patients to be fully in charge and therefore determines who should read their medical records. This changes the trend from the traditional centralized databases that further enhance the privacy of the users and empower patients to take control over sensitive health information.

##### 3. Efficient Access Management

**Outcome:** Smart contracts allow for automated role-based access control, thus enabling authorized healthcare providers to access records on demand.

**Discussion:** Since the permissions are defined in smart contracts, access to particular records by who -- doctor, patient, insurer -- can be safely controlled. This will save the overhead of administrative work, prevent delay, and still satisfy data access regulations such as HIPAA and GDPR.

## 4. Improved Data Privacy

**Result:** Since the data are encrypted prior to writing them to IPFS, readable records would only be available to authorized users with the decryption key.

**Discussion:** Encrypting data and access management through private keys introduces a robust level of protection against unauthorized actors, including those operating in a blockchain network, from reading the encrypted data. Managing keys remains challenging and important to assure .

## 5. Transparency and Traceability

**Outcome:** The blockchain's audit trail results in a transparent account of all events (access, modifications) related to a patient's health record.

**Discussion:** The audit trail fosters transparency since every access request to update or delete data is evident on the blockchain. When disputes or audits arise, traceable records could provide accountability for what actions are performed with healthcare data.

## 6. Payment System Based on a Smart Contract

**Outcome:** The integration of the payment system in the framework of smart contracts enables the healthcare provider to pay access to data in a secure and efficient way.

**Discussion:** It is of a great value to both the health care providers and the insurers who need access to Lead to patients' records for various needs. This payment mechanism can encourage safe sharing of data, which may an anonymized health data marketplace for research.

## 7. Compliance with Regulatory Requirements

**Outcome:** The system is compliant with GDPR and HIPAA as well as granting ownership, privacy, and transparent audit trails to the patient.

**Discussion:** It brings trust on the blockchain network and health-related sensitive information is properly handled through compliance. Still, on blockchain networks, it becomes challenging to provide regulatory compliance, especially in the case of the erasure of data.

## 8. Limitations and Challenges

**Data Management Complexity:** Managing large healthcare datasets in a blockchain system is complex in spite of decentralized storage by IPFS. Updating or deleting records makes it even more complicated.

**Key Management:** The security is largely based on private keys and needs very cautious handling. Losing access to a private key by a patient will somewhat be difficult to get to or even to revoke access to his data.

**Scalability and Cost:** Although the use of IPFS mitigates the costs of storage, scaling the system up to support millions of users and millions of transactions is expensive. High gas fees on the blockchain for updates about access control, such as create or delete access key, are barriers to adoption.



## Screenshots:

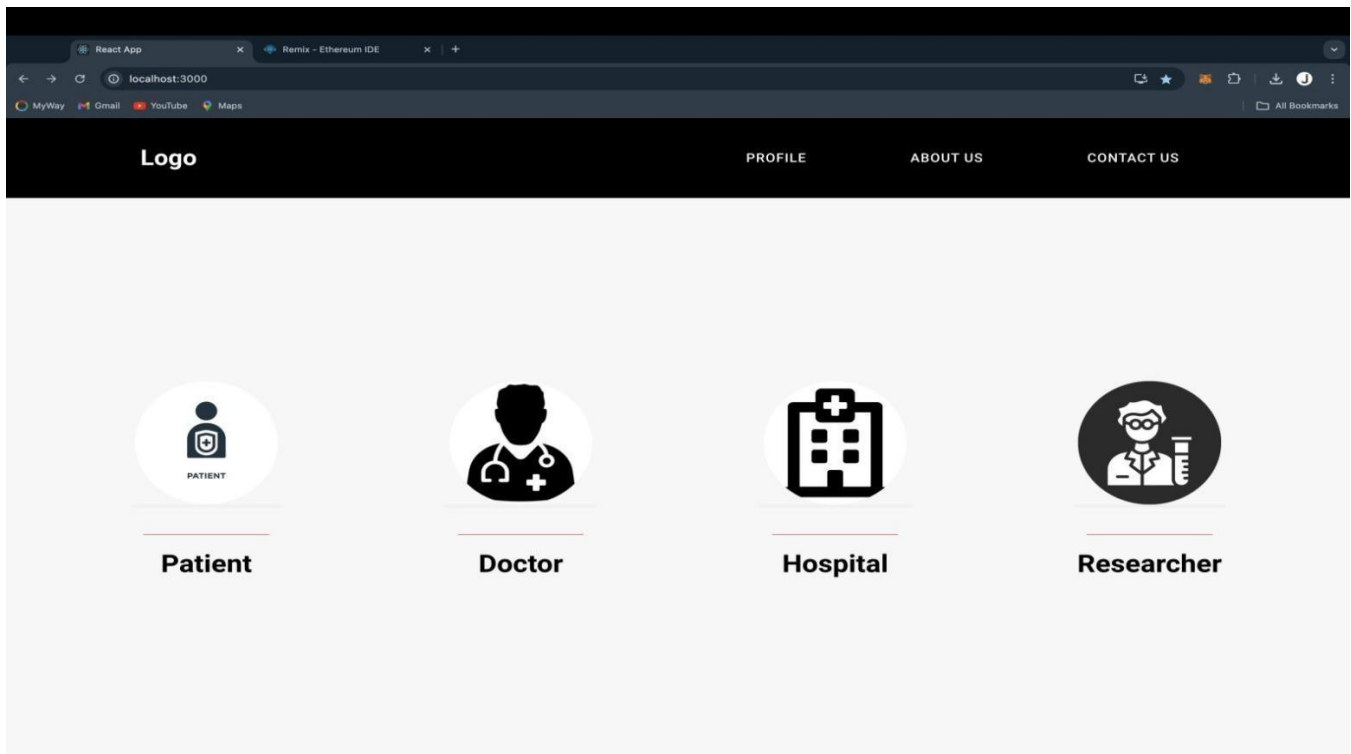


Image 8.1

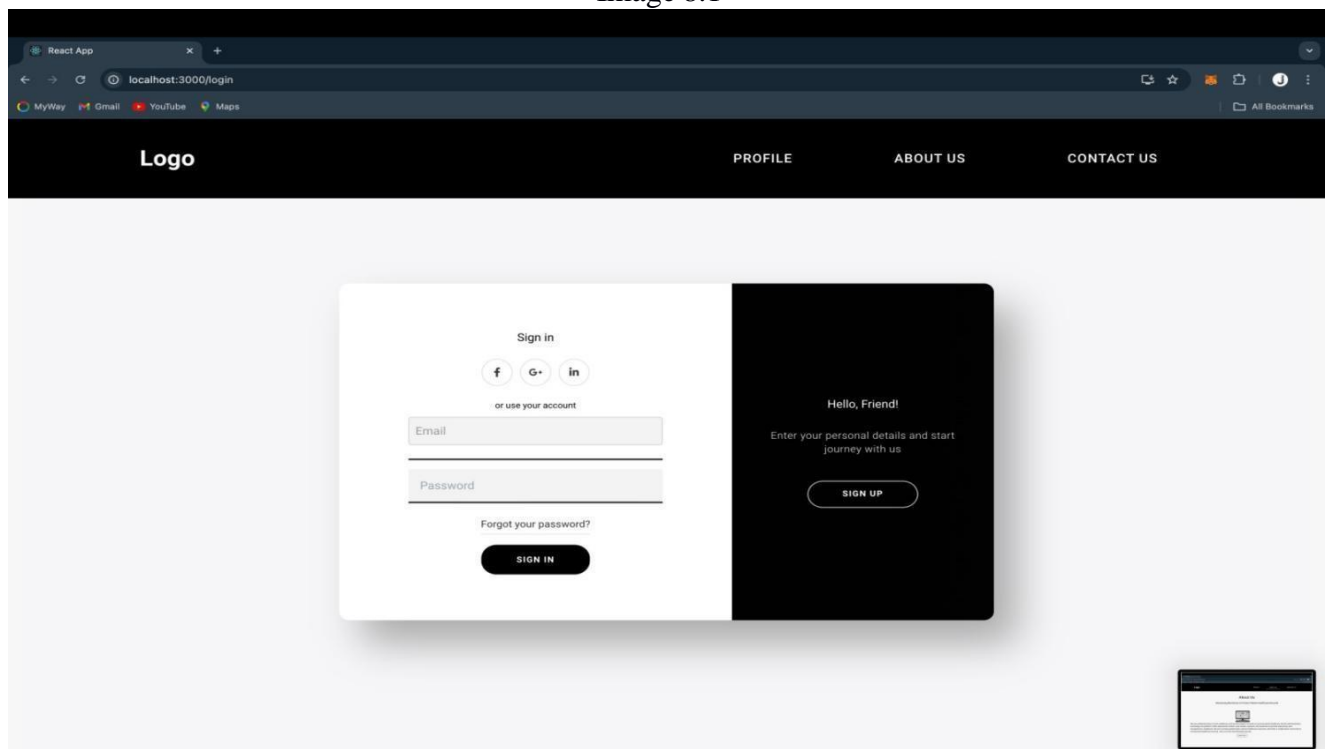


Image 8.2

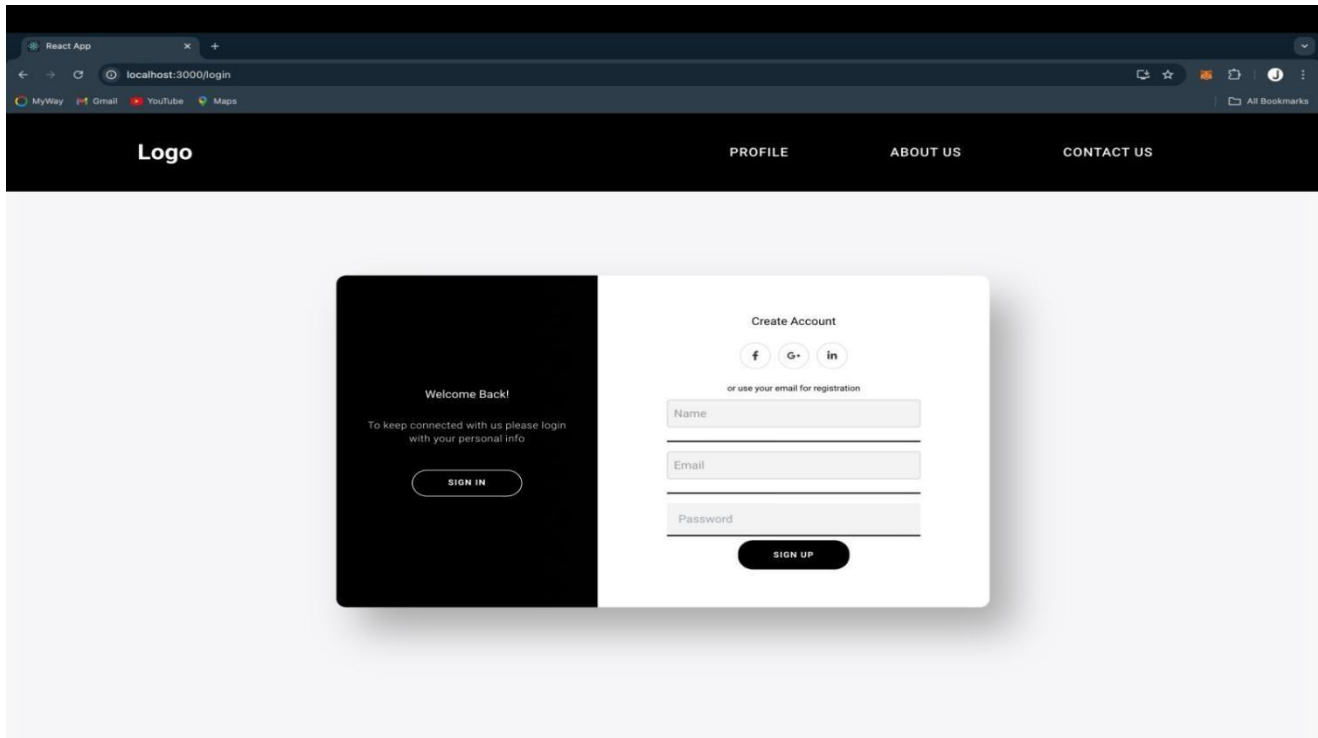
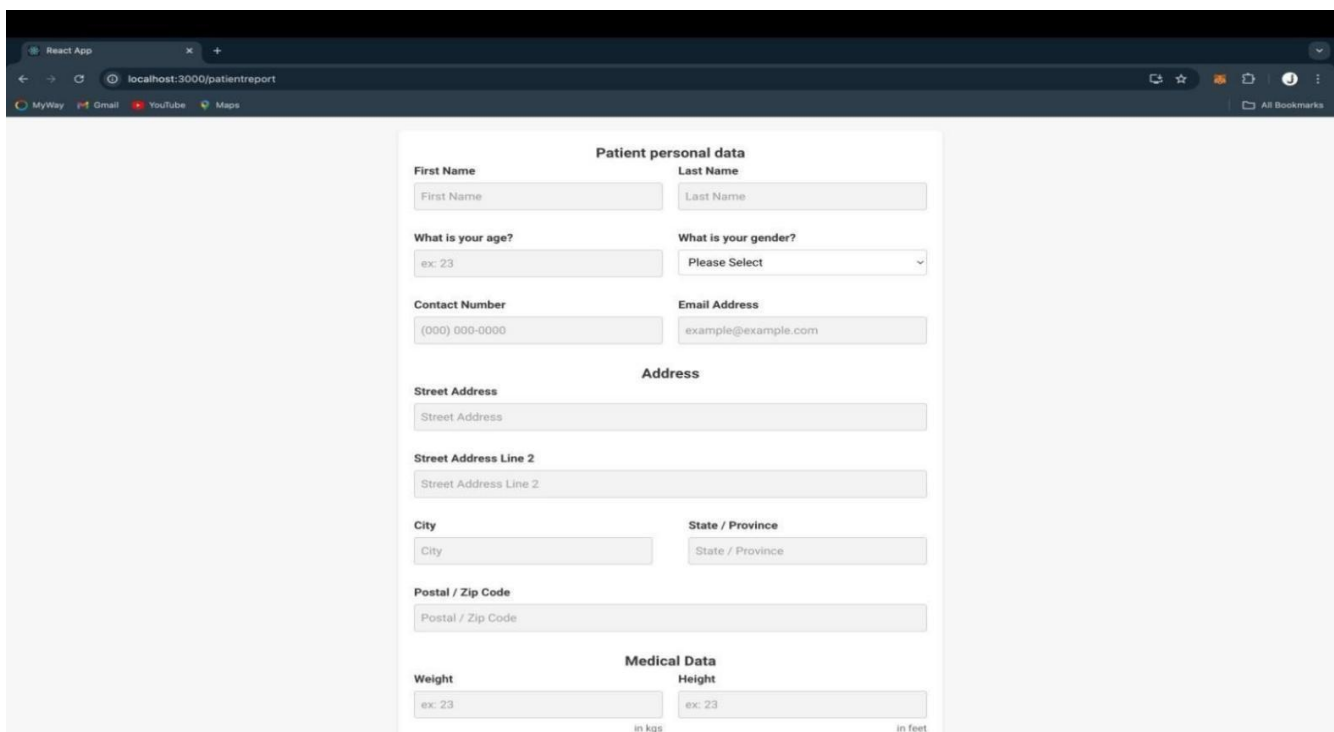


Image 8.3



The screenshot shows a web browser window with the URL `localhost:3000/patientreport`. The form is titled "Patient personal data" and is organized into several sections. The "Patient personal data" section includes input fields for First Name, Last Name, Age (with an example of 23), Gender (a dropdown menu), Contact Number (with a format example of 000) 000-0000), and Email Address (with an example of example@example.com). The "Address" section includes input fields for Street Address, Street Address Line 2, City, State / Province (a dropdown menu), and Postal / Zip Code. The "Medical Data" section includes input fields for Weight (with an example of 23 and a unit of in kgs) and Height (with an example of 23 and a unit of in feet).

Image 8.4

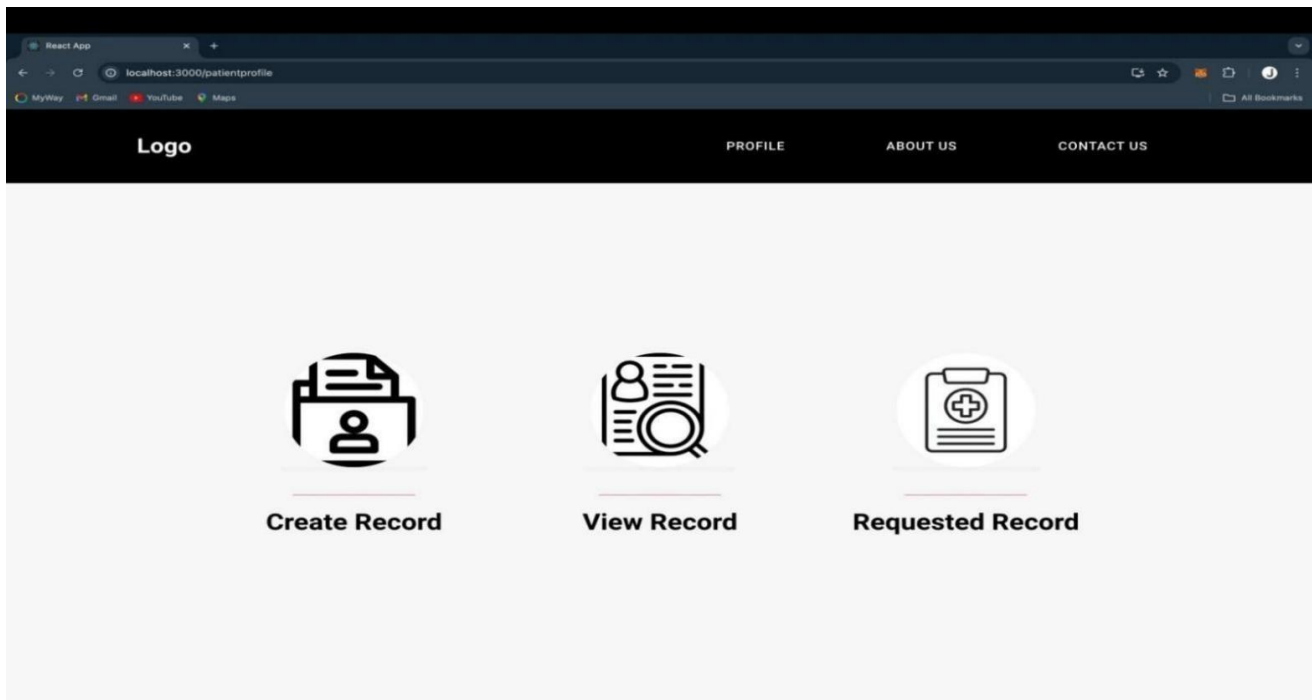


Image 8.5

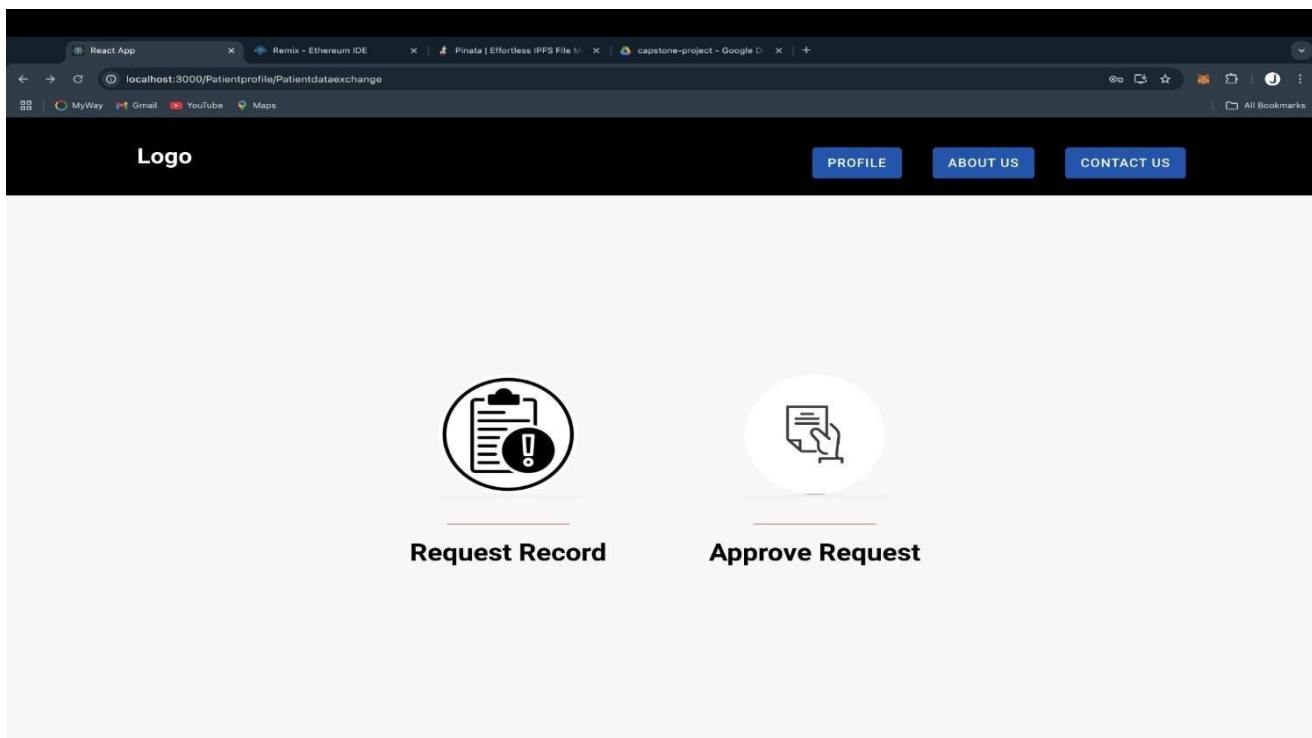


Image 8.6

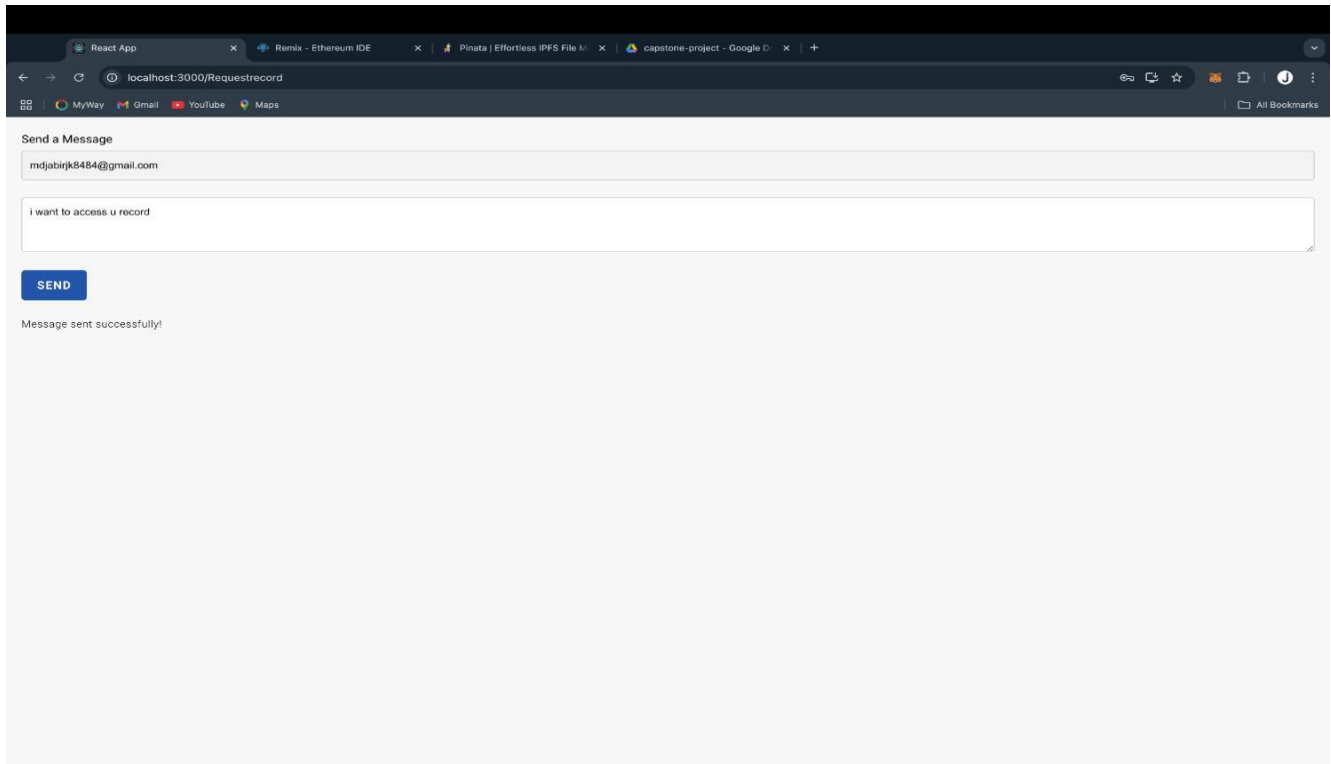


Image 8.7

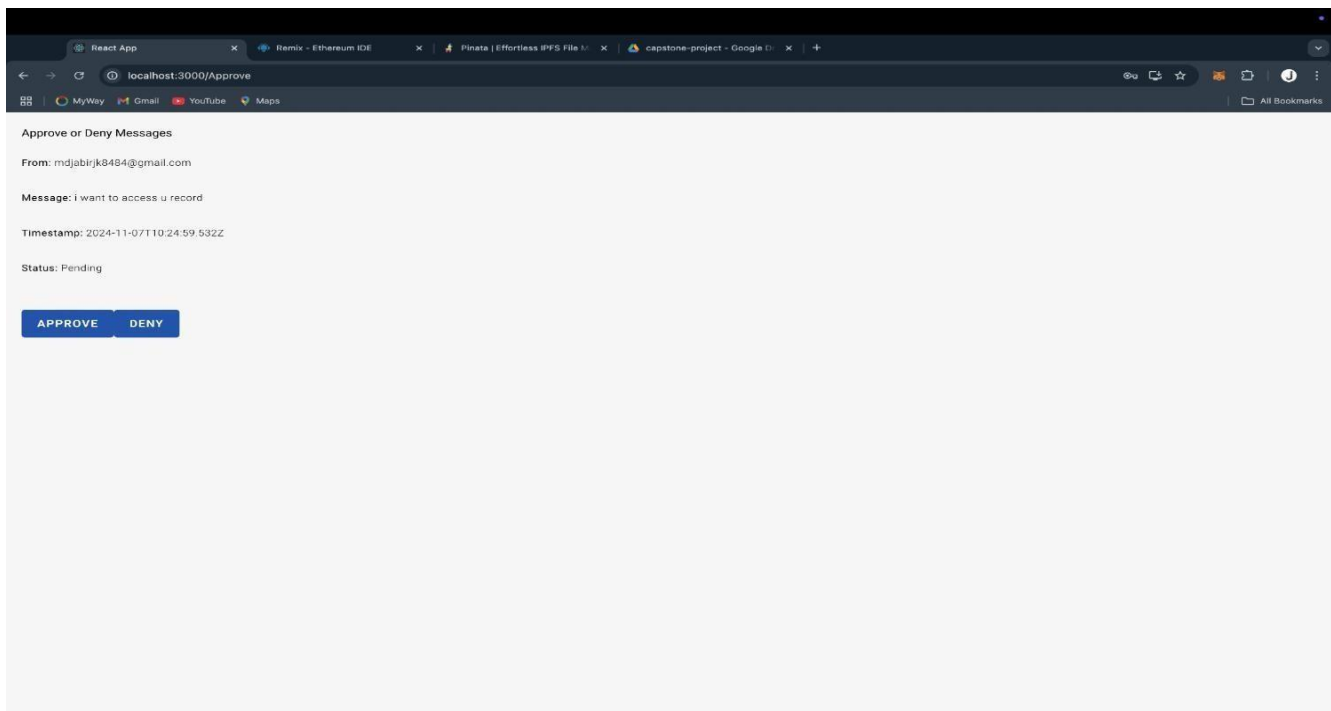


Image 8.8

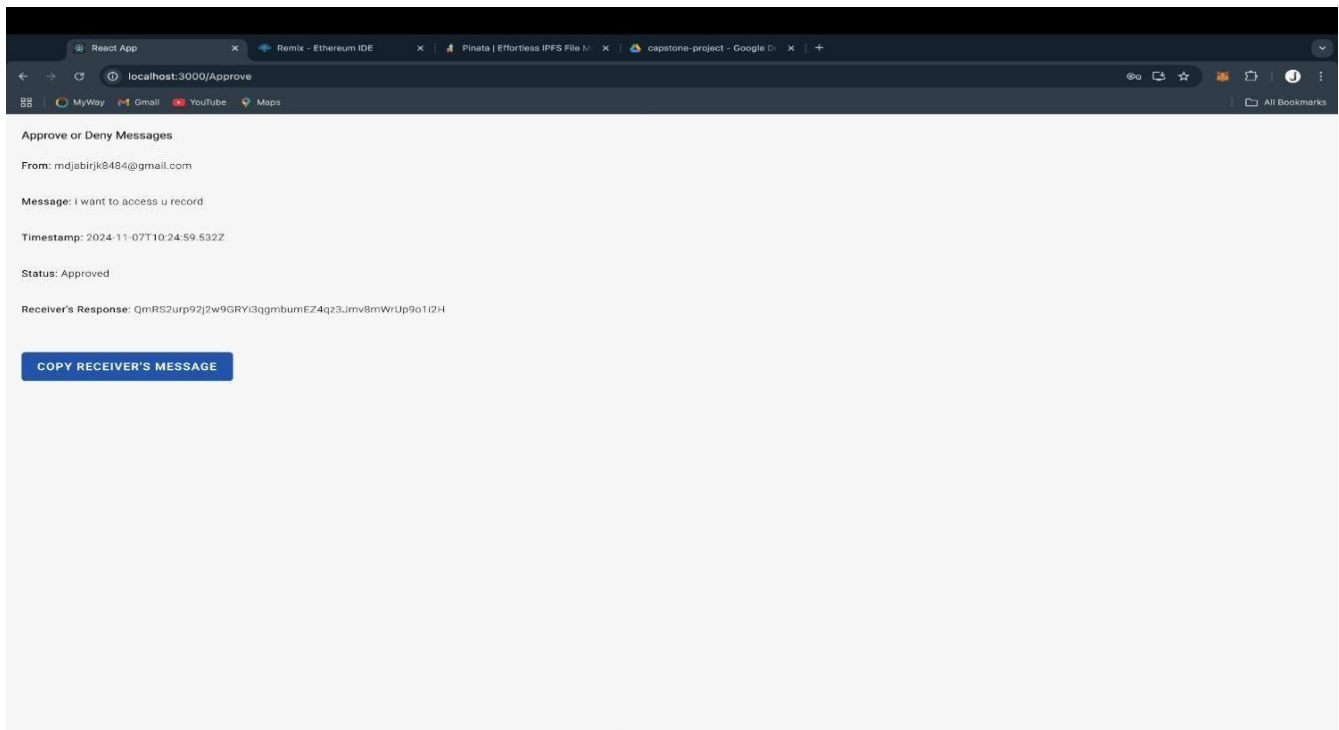


Image 8.9

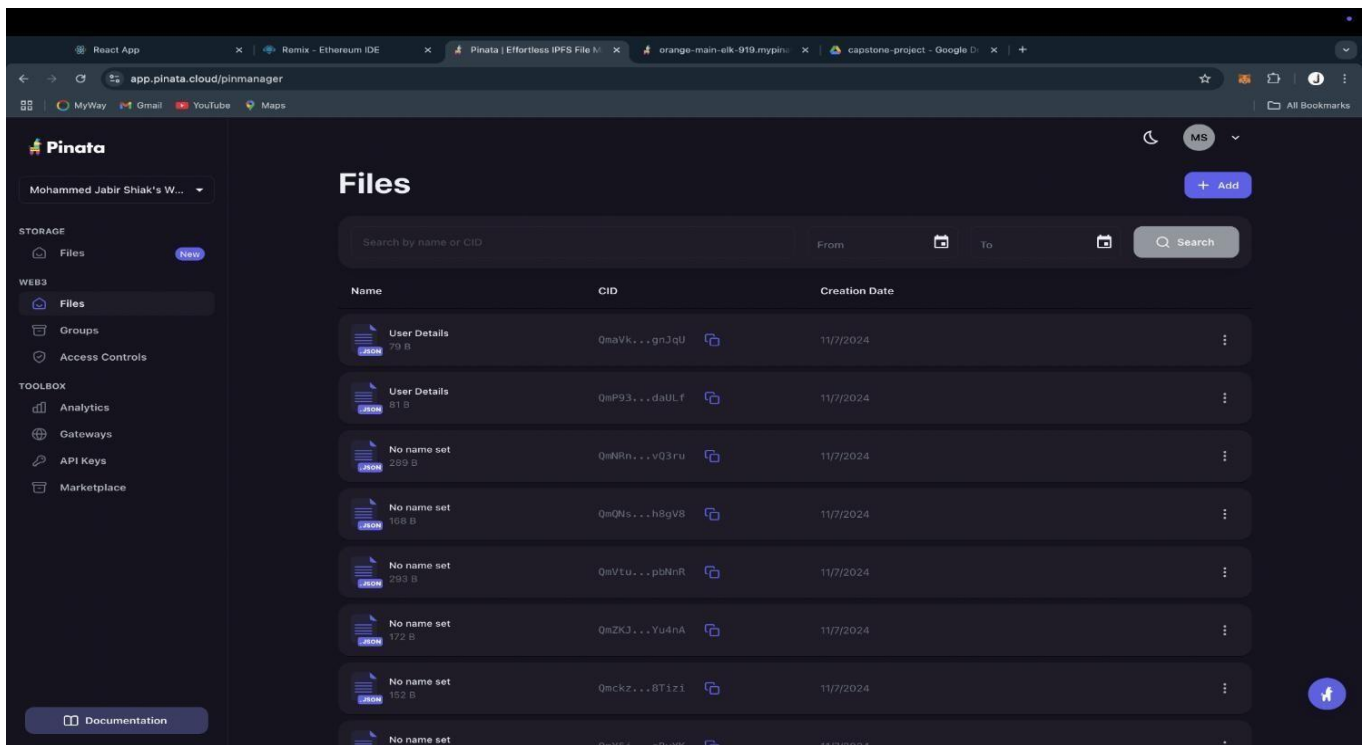


Image 8.10

## CHAPTER 9

### CONCLUSION AND FUTURE WORK

#### 9.1 Conclusion

The exploration plan for further improving the blockchain-based healthcare record system involves enhancing security and scalability, integrating with traditional healthcare systems, expanding roles, and introducing advanced AI-driven features. By following the outlined phases, the system can evolve into a robust, scalable, and innovative platform for secure healthcare data management while maintaining patient privacy and regulatory compliance.

#### 9.2 Future Work

**Encryption Enhancements:** Currently, data is stored on IPFS with its hash on-chain. For additional privacy, we plan to implement encryption before uploading to IPFS, ensuring that even in IPFS, the data remains encrypted.

**Off-Chain Computation:** Explore off-chain computation frameworks (like Layer 2 solutions) to improve transaction speed and reduce latency in a public network setting.

**Interoperability with Existing Healthcare Systems:** Integrate with existing Electronic HealthRecord (EHR) systems to allow seamless transfer of data between traditional databases and blockchain.

**Permissioned Blockchain:** Explore permissioned blockchains (e.g., Hyperledger Fabric) to allow for a more controlled and faster environment, especially in healthcare institutions.

## REFERENCES/BIBLIOGRAPHY

- 1) V. Mahore, P. Aggarwal, N. Andola, Raghav, and Dr. S. Venkatesan, "Secure and Privacy Focused Electronic Health Record Management System using Permissioned Blockchain," Proceedings of the 2019 IEEE Conference on Information and Communication Technology (CICT), 2019.
- 2) S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
- 3) R. Rajnish, "Securing Healthcare Records using Blockchain Technology," Proceedings of the 2nd International Conference on Advanced Computing and Software Engineering (ICACSE-2019), 2019.
- 4) S. Saha, J. Poray, and B. Jana, "A Study on Blockchain Technology," International Journal of Computer Science and Engineering (IJCSE), vol. 7, no. 4, pp. 350-358, 2019.
- 5) Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE Access, vol. 7, pp. 10,350-10,375, 2018.
- 6) Y. Han, Y. Zhang, and S. H. Vermund, "Blockchain Technology for Electronic Health Records," Journal of Medical Systems, vol. 45, no. 3, pp. 1-12, 2021.
- 7) J. Qu and M. Sa, "Security Research of Blockchain Technology in Electronic Medical Records," International Journal of Security and Privacy, vol. 14, no. 2, pp. 159-168, 2020.

## APPENDIX A DEFINITIONS, ACRONYMS AND ABBREVIATIONS

### Definitions

**Blockchain:** A decentralized, immutable ledger technology that records transactions across many computers in a way that the registered transactions cannot be altered retroactively.

**Smart Contracts:** Self-executing contracts with the terms of the agreement directly written into code, allowing for automatic execution when predefined conditions are met.

**Interoperability:** The ability of different systems and organizations to work together and exchange information seamlessly.

**Decentralization:** The distribution of data across multiple nodes in a network, reducing the risk of a single point of failure.

### Acronyms and Abbreviations

**EHR:** Electronic Health Record

**HIPAA:** Health Insurance Portability and Accountability Act

**GDPR:** General Data Protection Regulation

**DPO:** Delegated Proof of Stake

**CSE:** Computer Science and Engineering

**UI:** User Interface

**IPFS:** InterPlanetary File System

**BTC:** Blockchain Technology



## APPENDIX B USER MANUAL (OPTIONAL)

### 1. Introduction

This user manual provides instructions for using the blockchain-based healthcare record management system. It is designed for healthcare providers, patients, and administrators to facilitate secure and efficient management of healthcare records.

### 2. User Roles

**Healthcare Providers:** Doctors, nurses, and clinicians who access and manage patient records.

**Patients:** Individuals whose health records are stored and managed in the system.

**Healthcare Administrators:** Personnel responsible for overseeing the system and ensuring compliance with regulations.

### 3. Getting Started

#### System Requirements:

Internet connection

Supported web browser (e.g., Chrome, Firefox)

User account (created by the healthcare organization)

### 4. User Registration

#### For Healthcare Providers:

Visit the registration page.

Fill in the required fields (name, email, role).

Submit the registration form.

Await approval from the system administrator.

#### For Patients:

Receive an invitation link from your healthcare provider.

Click on the link to access the registration page.

Complete the registration form.

Verify your email address.

### 5. Logging In

Go to the login page.

Enter your username and password.

Click on the "Login" button.

## 6. Accessing Healthcare Records

### For Healthcare Providers:

Log in to the system.

Navigate to the "Patient Records" section.

Search for a patient using their ID or name.

Click on the patient's record to view details.

### For Patients:

Log in to your account.

Navigate to the "My Health Records" section.

View your medical history, treatment options, and insurance details.

## 7. Managing Permissions

### For Patients:

Go to the "Settings" section.

Click on "Manage Permissions."

Select which healthcare providers can access your records.

Save changes.

## 8. Using Smart Contracts

### For Healthcare Providers:

Access the "Smart Contracts" section.

Create a new contract for accessing patient data.

Define the terms and conditions.

Submit the contract for approval.

## 9. Security Features

**Data Encryption:** All patient data is encrypted to ensure privacy.

**Audit Trails:** Access logs are maintained for transparency.