A Project Report On

# A BLOCKCHAIN-BASED HEALTH INFORMATION EXCHANGE WITH A PATIENT-CENTRIC APPROACH

Submitted in partial fulfillment of the requirement for the $8^{th}$ semester

**Bachelor of Engineering**

in

Computer Science and Engineering

## DAYANANDA SAGAR COLLEGE OF ENGINEERING

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078


*Submitted By*

**Govardhan R 1DS19CS052**

**Jagadeesh V Ranagatti 1DS19CS058**

**Lakshminath S M 1DS19CS079**

**Linganand Sangamad 1DS19CS080**

*Under the guidance of*

**Dr. Nagaraja J**

Associate Professor, CSE, DSCE

**Mr. Avinash Chukka**

Co-guide - Industry

**2022 - 2023**

Department of Computer Science and Engineering

DAYANANDA SAGAR COLLEGE OF ENGINEERING

Bangalore - 560078

# VISVESVARAYA TECHNOLOGICAL UNIVERSITY

## Dayananda Sagar College of Engineering

(An Autonomous Institute affiliated to VTU, Belagavi, Approved by AICTE & ISO 9001:2008 Certified)

Accredited by National Assessment & Accreditation Council (NAAC) with 'A' grade

Shavige Malleshwara Hills, Kumaraswamy Layout, Bengaluru-560078

## Department of Computer Science & Engineering


# CERTIFICATE

This is to certify that the project entitled **A Blockchain-Based Health Information Exchange With A Patient-Centric Approach** is a bonafide work carried out by **Govardhan R [1DS19CS052]**, **Jagadeesh V Ranagatti [1DS19CS058]**, **Lakshminath S M [1DS19CS079]** and **Linganand Sangamad [1DS19CS080]** in partial fulfillment of $8^{th}$ semester, Bachelor of Engineering in Computer Science and Engineering under Visvesvaraya Technological University, Belgaum during the year 2022-23.

| **Dr. Nagaraja J** | **Dr. Ramesh Babu D R** | **Dr. B G Prasad** |
|---|---|---|
| Guide | Vice Principal & HOD | Principal |
| Assoc Prof. CSE, DSCE | CSE, DSCE | DSCE |
| Signature: ..... | Signature: ..... | Signature: ..... |

| Name of the Examiners: | Signature with date: |
|---|---|
| 1. ..... | ..... |
| 2. ..... | ..... |

# Acknowledgement

We are pleased to have successfully completed the project **A Blockchain-Based Health Information Exchange With A Patient-Centric Approach**. We thoroughly enjoyed the process of working on this project and gained a lot of knowledge doing so.

We would like to take this opportunity to express our gratitude to **Dr. B G Prasad**, Principal of DSCE, for permitting us to utilize all the necessary facilities of the institution.

We also thank our respected Vice Principal, HOD of Computer Science & Engineering, DSCE, Bangalore, **Dr. Ramesh Babu D R**, for his support and encouragement throughout the process.

We are immensely grateful to our respected and learned guide, **Dr. Nagaraja J**, Professor CSE, DSCE and our co-guide **Mr. Avinash Chukka**, VP of Products, Cardlytics for their valuable help and guidance. We are indebted to them for their invaluable guidance throughout the process and their useful inputs at all stages of the process.

We thank all the faculty and support staff of Department of Computer Science, DSCE. Without their support over the years, this work would not have been possible.

Finally, we would like to express our deep appreciation towards our classmates and our family for providing us with constant moral support and encouragement. They have stood by us in the most difficult of times.

**Govardhan R 1DS19CS052**

**Jagadeesh V Ranagatti 1DS19CS058**

**Lakshminath S M 1DS19CS079**

**Linganand Sangamad 1DS19CS080**

# ABSTRACT

Patient health data is very sensitive and digitization of healthcare data has led to increased concerns regarding patient privacy, data security, and control over personal health information. Healthcare organizations face numerous obstacles, including unauthorized access to sensitive patient information, data breaches, lack of transparency in data sharing, and difficulties in achieving regulatory compliance. This project proposes a solution that uses the decentralized and immutable nature of Blockchain technology, integrated with the distributed storage capabilities of the InterPlanetary File System (IPFS), to address these challenges effectively. In this project, we aim to design and implement a blockchain-based system that prioritizes patient control and ownership of their health data. Through the utilization of blockchain technology, patients are empowered with control over their data, granting them the ability to selectively share their health information with healthcare providers and other authorized parties. The integration of IPFS with blockchain technology provides a distributed storage layer for encrypted health records and secure data sharing among healthcare providers while maintaining patient privacy. We also developed smart contracts, encryption mechanisms, and user-friendly interfaces for patients and healthcare providers. By adopting a patient-centric approach, we aim to enhance patient engagement, enable personalized healthcare, and improve health outcomes. Patients will have increased access to their health data, enabling them to make informed decisions and actively participate in their own care.

# Table of Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

## 1.1 What are electronic medical records?

Electronic medical records (EMRs) are digital versions of a patient's medical history, including their medical diagnoses, treatments, medications, allergies, laboratory results, and other relevant health information. EMRs are created and stored in a digital format, typically within a healthcare organization or facility.

EMRs have replaced traditional paper-based medical records in many healthcare settings, offering numerous advantages over their physical counterparts. It is important to note that privacy and security measures are crucial when implementing and managing electronic medical records to protect patient confidentiality and comply with applicable data protection regulations.

The main objective of maintaining EMRs is to support the continuity, efficiency and quality of integrated health management. It is also cost-effective as it removes the redundancy of screening and tests. It promotes practice of evidence based medicine and Paperless medical history can be accessed anytime anywhere. The other benefits of EMRs are - apt backup policies that increase the longevity of health records maintenance, secure access, audit and authorization control mechanisms. They enable the exchange of online health data, allowing improved care coordination and flow across various healthcare environments.

While electronic medical records (EMRs) offer numerous benefits, there are also challenges and concerns associated with sharing and storing them. Here are some common problems that healthcare organizations may encounter: Interoperability, Data Security and Privacy, Fragmentation and Duplication, Patient Consent and Data Sharing Policies and other technical challenges. Addressing these challenges requires collaboration between healthcare organizations, software vendors, policymakers, and regulatory bodies. Interoperability standards, data governance frameworks, and enhanced security protocols are necessary to promote seamless sharing and secure storage of electronic medical records while protecting patient privacy.

## 1.2 What is blockchain?

Blockchain is a decentralized and distributed central ledger that records transactions across multiple computers or nodes. It is designed to be transparent, secure and tamper-resistant. Instead of depending on a single central authority, blockchain works by using a network of computers to validate transactions. Blockchain is simply a chain of blocks. Each block in the blockchain contains a list of transactions. These transactions are grouped together, validated and added to the chain in a linear and chronological order. Once a block is added to the chain, it becomes a permanent part of the record, and cannot be altered without the consensus of network participants.

The structure of a block in the blockchain is similar to that of a node in a linked list. While a node in a linked list contains a pointer to the previous node, the block has a hash pointer that points to the previous block. This hash pointer not only tells where the previous block is, but also helps verify that it has not been tampered with. Han et. al. [2] gives the structure of blockchain as shown in *Figure 1.1*.

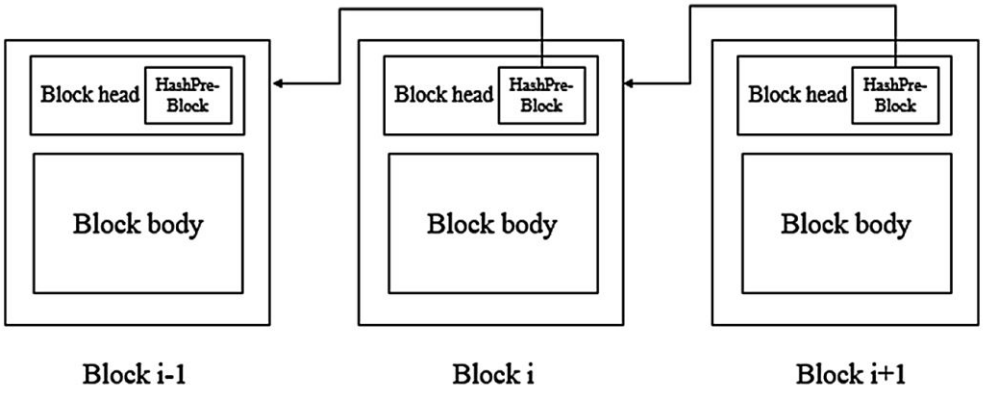


Figure 1.1: Structure of Blockchain

Blockchain technology provides several **key features**. They are

- Decentralization: There is no central authority or entity in the network.
- Transparency: Since the blockchain is a public ledger, the transactions in it are visible to all the participants.
- Immutability: Once a transaction has been written onto the blockchain, it cannot be changed.
- Traceability: We can trace the provenance of every asset or transaction in the blockchain, to verify whether someone claiming to be the owner, is actually the owner.

The different **types of blockchain** are

1. Public blockchain: Such blockchains are publicly accessible. Reading data is not restricted. Writing to the chain will be governed by a consensus mechanism.
2. Consortium blockchain: These blockchains are partly private. They are managed by a group of organizations instead of a single one. Such blockchains are best for collaboration between the organizations.
3. Private blockchain: Only verified participants can join the network. Writing to the chain is restricted to a fixed set of users. Reading can be public or restricted.

The **genesis block** is the first block in the blockchain. It gives a template that can be followed by all the subsequent blocks in the chain. Since this block is the first block, it does not have a 'previous block' pointer. This field is set to 0, and thus the genesis block is also called 'Block 0'. *Figure 1.2* [18] shows the genesis block in a blockchain.

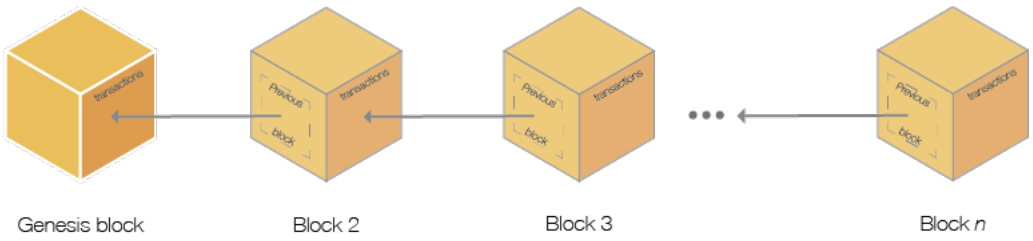


Figure 1.2: Genesis Block

**Consensus mechanisms** are used in blockchain networks to achieve agreement among the nodes about the transactions that have occurred. Each node maintains a list of transactions that are to be added to the blockchain. When the time comes to add the next block, every node wants to propose the new block. The selection of the node that will propose the next block is handled by the consensus mechanism. Most popular consensus mechanisms are Proof-of-Work (POW) and Proof-of-Stake (POS).

In **POW**, nodes try to solve a hash problem for the right to put the next block onto the chain. Solving this mathematical problem requires large computing power and is called 'mining'. The first node to solve this problem (the solution can be easily verified by other nodes) will put the next block onto the blockchain, and obtain the 'block reward'. POW is used by Bitcoin and Litecoin.

**Proof-of-Stake** is a comparatively low-energy consuming consensus mechanism that is used in Ethereum. This model works on the idea that nodes have the power to propose the next block proportional to the virtual currency tokens in their wallet. In POS, power is delegated by wallet size.

**Smart contracts** are programs on the blockchain that are automatically executed when predefined conditions are met. They allow agreements to be carried out among anonymous participants in the blockchain network. Smart contracts reduce the time taken to execute agreements drastically. These contracts will be written by the programmer according to the business application requirements.

## 1.3 Applications of blockchain

- Finance: Blockchain technology can facilitate transactions that are quicker, cheaper, and more secure as well as smart contracts that run automatically in accordance with predetermined rules. Digital currencies like Bitcoin may be created and exchanged more easily thanks to blockchain technology.

- Healthcare: The interoperability and effectiveness of healthcare systems, as well as the security and privacy of medical records, can all be enhanced by blockchain. Drugs, devices, and vaccinations may be tracked and verified using blockchain technology.

- Supply Chain: Blockchain can improve product and material traceability and transparency from point of origin to point of use. Along with lowering fraud, waste, and errors, blockchain can help raise product quality and safety.

- Government: Blockchain can improve how public services like voting, taxation, identity management, and land registration are delivered and held accountable. Additionally, government procedures that use blockchain have less bureaucracy, corruption, and inefficiency.

- Media: By allowing content producers and users to own, control, and monetize their digital assets, blockchain can empower both groups. Blockchain technology can also stop information tampering, plagiarism, and censorship.

- Education: Blockchain can make it possible to create and verify electronic credentials like degrees, certificates, and badges. The sharing and acknowledgement of learning results across institutions and countries can also be facilitated by blockchain.

- Energy: Blockchain can enable peer-to-peer trade of renewable energy sources like solar and wind, which will enable the decentralization and democratization of energy production and consumption. Energy systems can function more effectively and reliably thanks to blockchain.

- Gaming: By facilitating the production and ownership of distinctive digital assets, such as characters, goods, and skins, blockchain can improve the gaming experience. The commercialization and trading of these assets between platforms and games can also be made possible by blockchain.

- Travel: By facilitating the verification and preservation of identity documents like passports and visas, blockchain can increase the security and convenience of travel. Additionally, loyalty and incentive programmes for consumers and service providers can be made possible through blockchain.

- Art: By facilitating the creation and ownership of digital art, including paintings, music, and movies, blockchain can empower artists and collectors. Along with enabling the protection of intellectual property rights, blockchain can also help with the authentication and provenance of pieces of art.

## 1.4 Blockchain in healthcare

Blockchain fueled medical data exchange can unlock the true potential of interoperability. Blockchain-based systems have the ability to lower or eliminate the friction and intermediary costs. Blockchain has the capability to redefine healthcare, keeping patients at the epicenter of the healthcare ecosystem helping increase security, privacy and interoperability of health data. This path breaking technology can revolutionize the health information exchange system by making electronic medical data more efficient, disintermediated, and secure. This new field provides a prolific ground for experimenting, investing, and proof-of-concept testing.

The blockchain has turned out to have a significant impact on the healthcare system's stakeholders. In the foreseeable future, a countrywide blockchain network for storing electronic medical records can improve efficiencies and reinforce better health results for patients. It's important to note that while blockchain technology offers significant potential, its adoption in healthcare is still in its early stages. Challenges such as scalability, regulatory compliance, and integration with existing systems need to be addressed for widespread implementation.

The proposed system tries to represent an exciting prospect for the future of healthcare, combining blockchain's security and transparency with smart contracts' automation capabilities. As the technology evolves and matures, further advancements can be expected in blockchain-based health systems and their potential to transform the healthcare landscape.

## 1.5 Organization of project report

The project report is organized as follows: Chapter (2) defines the problem statement for this project, and also addresses the various problems present in the existing systems. Chapter (3) describes the survey of existing blockchain-based systems categorized as on-chain and off-chain based on the storage mechanism used. Chapter(4) discusses the design of the proposed solution and the methodology used. The proposed system is divided into five major modules and the working of each of these modules has been discussed. Chapter(5) contains the implementation of the proposed system. This chapter also contains pseudocodes of the smart contracts used. The results of the implementation are discussed in Chapter(6) by giving the detailed working of different pages in the application. Chapter (7) gives conclusion and future work.

# Chapter 2

# Problem Statement & Blockchain Solution

## 2.1 Problem statement

To develop an end-to-end solution for a healthcare system while securely storing patient medical records, and giving patients control over their data.

## 2.2 Problems in existing systems

- **Data exchange limitations**: In the healthcare system, there are a variety of stakeholders that must securely and effectively exchange health data, including patients, providers, insurers, researchers, and regulators. The existing approach, however, relies on centralized databases and middlemen, which can lead to data silos, discrepancies, lag times, and mistakes.

- **Issues with the supply chain**: The healthcare system relies on the timely and safe delivery of pharmaceuticals and medical devices to patients. However, the current method is susceptible to fraud, forgery, theft, and spoiling, which could jeopardize the trust of patients.

- **Obstacles to using patient data in clinical research**: The healthcare system depends on clinical research to identify new diseases and remedies. But the existing system has trouble finding patients, getting their permission, protecting their privacy, and motivating them to participate.

- **Data privacy and compliance**: The healthcare system deals with sensitive and private health information that needs to be guarded against misuse, disclosure, and unauthorized access. However, the current system has difficulties adhering to data protection laws and regulations that differ across nations and regions.

- **Bureaucracy and manual inefficiencies**: The healthcare system is filled with complicated, time-consuming procedures that demand a lot of paperwork, verification, and coordination between various stakeholders, including patients, providers, insurers, and regulators. However, the current system is vulnerable to mistakes, holdups, fraud, and conflicts that can raise costs and degrade service quality.

- **Lack of innovation and incentives**: The healthcare system depends on innovation and incentives to find new diseases and remedies as well as to enhance patient outcomes in terms of health. However, the lack of data sharing, collaboration, and reward mechanisms among researchers, creative individuals, and patients makes it difficult for the current system to encourage innovation and incentives.

- **Lack of transparency and trust**: The healthcare system depends on the cooperation of many stakeholders, including patients, providers, insurers, regulators, and researchers. However, the absence of accountability, verification, and auditability in the current system makes it difficult to build confidence and transparency.

## 2.3 How can blockchain help solve these problems?

The use of blockchain enables the storage of patient health records among the network participants by the use of encryption, consensus and smart contracts. This improves data interoperability, accessibility and reliability across the healthcare system. Blockchain can help keep track of the provenance of drugs and medical instruments right from the manufacturers up until it reaches the hands of the consumer. This ensures the authenticity and quality of medicines and other products. Patients can employ control over their own data and participate in clinical research if a patient-centric and collaborative environment is made available to them. Such an environment can be developed by the use of blockchain. Blockchain provides a secure ledger for the storage and usage of patient medical records. Using digital identities, access rights and smart contracts, blockchain ensures compliance with data privacy laws and regulations. Blockchain can help reduce errors and delays in the system by eliminating intermediaries and paperwork. The use of blockchain can bring about a collaborative, incentivized environment where researchers and other stakeholders come up with new innovations to improve the network. Trust and transparency can be achieved in the network by the use of blockchain.

## 2.4 Motivation

The different problems that exist in the field of secure sharing of patient medical records have been discussed. The research work that has been conducted in this field will be discussed in the following chapter. The summary in *Section 3.3* speaks about the problems that have not been addressed in the research conducted so far. The system proposed in this report aims to resolve these concerns and bring about a new system of healthcare where patients can wield access over their data.

# Chapter 3

# Literature Survey

Various research works have been published in the field of storing medical records using blockchain. Surveyed papers are divided according to the 2 major data storage paradigms in blockchain - **On-chain** and **Off-chain**. The following subsections discuss various on-chain and off-chain storage mechanisms.

## 3.1 On-chain

Sudeep et. al. in [1] propose a system utilizing blockchain technology for building an EHR sharing model based on Hyperledger in the context of Healthcare 4.0 applications to facilitate safe and efficient data sharing. The system also allows patients to be in control of their data and permit access to authorized entities. Several Access Control Policies have been proposed and refined to improve data access for participants in the system.

Huirui Han et. al. [2] propose a system that leverages blockchain's salient features for storage and access of health data.The system uses a hybrid blockchain between private and consortium blockchain. The private blockchain to store health data of medical facilities whereas consortium blockchain for storing shared health data. This system incorporates identity management mechanisms to prevent unauthorized access. To ensure data integrity the authors have used encryption techniques like asymmetric encryption and smart contracts.

The authors [3] have proposed a privacy-protection and secure health information sharing scheme aiming to address the challenges in improving the diagnosis procedure in electronic health systems using blockchain technology. They have formulated consensus mechanisms and data structures to build 2 types of blockchains - private and consortium blockchain. The private one for storing the personal health data while the consortium blockchain stores the indices of the secure data. It promotes decentralized governance and agreement between participating entities.

## 3.2 Off-chain

This section is further divided according to the different mechanisms of data storage used.

### 3.2.1 Cloud

The system that is proposed in the work [4] aims to provide a useful method for gathering high-quality health data for a variety of research and commercial purposes. Health data should be accessible to users and under their control, however they are typically handled by other organizations. The authors suggest a simple and safe blockchain design that makes use of cloud storage. In order to check the data quality, they have also applied machine learning.

In this research, S. Wang et al. [5] offer a method for protecting personal health information stored on cloud platforms. The cloud-stored encrypted data is accessible to users and patients. Before being stored, the data is encrypted to prevent alterations by outside parties. The patients are responsible for starting a smart contract and sharing private keys. The hash of the data and the transaction information are stored in the blockchain and can be used to access the data and check its integrity. This document does not handle cloud file activities like updating and deleting files.

By adopting a permissioned blockchain, the authors of [6] suggest a system for exchanging electronic medical records in which only authorized individuals are able to join. Users of the system have access to shared health data from different healthcare providers as well as the ability to add their data to the cloud repository that stores all of the data. The requests users make to access or modify data are regarded as transactions, and users can make these requests by giving their private key. The consensus nodes then confirm these transactions.

### 3.2.2 InterPlanetary File System

InterPlanetary File System is a content-address, peer-to-peer storage and hypermedia sharing method in a distributed file system. In location-based addressing, the exact location of a resources is specified i.e. IP address or domain name. IPFS uses content-based addressing. Instead of saying where to find the resource, here we tell what it is that we want. Every file has a unique hash. To download a file, we ask the network who has a file with this hash.

Ayesha et. al. [7] discuss the use of blockchain to design a system for secure Electronic Health Record (EHR) sharing. This solution aims to solve the scalability problem of blockchain as it is not designed to store huge amounts of data. IPFS has been used as a means of off-chain storage for the health records.

Blockchain-as-a-service was used as a basis for a medical record storage solution by Buzachis et. al. [8]. This solution, called BaaS-HIE, uses a private blockchain and various smart contracts to manage access to data. For the secure storage of health data, IPFS has been used. The problems of security and interoperability among different healthcare providers can be overcome by the use of blockchain.

### 3.2.3 Existing database

The authors [9] have devised a system that deploys smart contracts using the Ethereum-based distributed ledger and keeps track of the interactions between patients and their doctors and hospitals. With the appropriate permissions, users can access the saved medical records. The suggested system can be integrated with the provider's current data storage system. To protect the data against unauthorized changes, an encrypted copy of the data is kept on the blockchain. It is recommended for researchers and other healthcare professionals to join the system as miners to record transactions on the blockchain. When a block makes it to the chain, a particular function in the contract compensates miners with anonymous medical data.

The authors [10] have built a private blockchain using which smart devices can make calls to smart contracts and write data using the Ethereum protocol. This system's sensors assist in real-time patient monitoring. Due to regulatory constraints, critical healthcare data will not be stored on the blockchain but rather on secure storage systems. Only transactions that can be authenticated by linking them to such databases are included in the blockchain.

The authors [11] here suggest a framework known as "Ancile" that strengthens access control and implements data obfuscation through the use of sophisticated encryption technologies and smart contracts. Numerous smart contracts in Ancile are in charge of tasks like registration of users, categorizing nodes, upkeep of node relationships, defining level of access, etc. Using smart contracts, patients may control who is granted access to their personal information. Ancile regulates access to the permissioned blockchain by validating user details before approval.

In order to protect recipients' privacy, Lee et al. created the health information exchange framework MEXchange [12], which masks both the sender and the recipient's addresses. This framework includes numerous smart contracts and procedures that protect user privacy by avoiding interference issues through the usage of ring signature and stealth address. MEXchange employs the PoW (Proof-of-Work) consensus technique and is built on the Ethereum private network.

### 3.2.4 Other off-chain solutions

Shan Jiang et al. have suggested BlocHIE [13], a blockchain-based network for exchanging health data. The two types of health data taken into consideration—personal health data and electronic health records—are stored on two loosely connected blockchains. Records that have been signed by the patient and the hospital are kept on the first blockchain. IoT hardware gathers and transmits patient data. The second chain contains this information. Instead of storing entire data, the blockchain stores only digitally signed hash values of records with time stamps. This guarantees that information cannot be accessed by the general public, protecting patient data privacy. By avoiding the storage of the actual records, the network's throughput is increased.

A PSN-based (Pervasive Social Network) healthcare system that enables wireless sensor devices to share medical data was proposed by Zhang et al. [14]. To put the concept into practice, the authors have created two protocols. One is to set up a safe channel of communication between the sensor nodes. To allow these devices to share data on the blockchain, the second protocol is used. Addresses are kept on the blockchain, and nodes can communicate with one another.

Purohit et. al. propose a blockchain-based HonestChain [15], a health information sharing system. The technology that is being exhibited interfaces with chatbot support and uses consortium blockchain. This promotes reputation building and compliance with data access rules. The benefits of using a permissioned blockchain during deployment include a shorter deployment time and fewer resource use. On the other hand, public blockchains are open to all participants and have no entry requirements. The paper is to be credited for its addressing of issues relating to reduced Loss of value/opportunity. The suggested system's test bed and assessment are implemented using Hyperledger Composer. Results demonstrate that the system performs better on measures for service time and request resubmission rate.

## 3.3 Summary

In the survey, various papers that talk about the importance of blockchain technology in the healthcare sector are discussed. Some of these papers have been summarized in *Table 3.1*. These papers discuss the use of blockchain in storing Electronic Medical Records (EMRs) of patients and propose secure decentralized systems and architectures for the same. Various consensus mechanisms, incentives, encryption techniques are also presented. The use of these systems will bring about a great difference in the healthcare sector by giving better service to patients.

Most of the papers do not include access control for patients and it is essential for patients to have control over their data in terms of who can access it. Medical records of patients should be made accessible to only those participants who the patient trusts. In this way misuse of personal data of patients can be avoided to an extent.

| Authors | Year | Blockchain Type | Consensus Mechanism | Implementation | Performance Analysis |
|---|---|---|---|---|---|
| Liu et.al.[16] | 2019 | Private Blockchain | Improved Delegated Proof of Stake | ✓ | ✓ |
| Jiang et.al.[13] | 2018 | Two loosely-coupled Blockchain | Proof of Work (PoW) | ✓ | ✓ |
| Azaria et.at.[9] | 2016 | Ethereum-based blockchain | Proof of Work (PoW) | ✓ | ✗ |
| Griggs et.at[10] | 2018 | Private Blockchain | Practical Byzantine Fault Tolerance (PBFT) | ✓ | ✗ |
| Dagher et.al.[11] | 2018 | Permissioned Ethereum Blockchain | QuorumChain Consensus Algorithm | ✓ | ✓ |
| Han et.al.[2] | 2018 | Consortium Blockchain and Fully Private Blockchain | Proof of Work (PoW) | ✗ | ✗ |
| Purohit et.al.[15] | 2021 | Consortium Blockchain | Proof of Authorization | ✓ | ✓ |
| Zhuang et.al.[17] | 2018 | Private Blockchain | Proof of Stake (PoS) | ✓ | ✗ |
| Buzachis et.al.[8] | 2019 | Private Blockchain | Clique-Proof-Of-Authority | ✓ | ✓ |
| Zhang et.al.[3] | 2018 | Private Blockchain and Consortium Blockchain | Proof of Conformance | ✓ | ✓ |

Table 3.1: Literature Survey

Existing works focus more on storing and sharing of medical records. Very few of them have explored the scope of blockchain in providing various other services like dispensing medicines and appointment systems. All the services of the existing healthcare system can be provided by blockchain based systems and can thus help in giving a much better service to patients.

Medical records can include scan results, reports and other documents that are usually larger in size and hence storing of such documents on the chain will lead to burden on the network. Some of the existing works use an on-chain storage mechanism without taking this into consideration.

This paper proposes a system that takes into account all the above mentioned limitations in the existing work. The proposed system provides a secure storage for medical records of patients where they have control over it. The system uses IPFS to store files thus reducing the burden on the network. The system also provides major services from making an appointment to dispensing of medicines using blockchain technology.

# Chapter 4

# Design and Methodology

The proposed system consists of four participants - *Admin, Patient, Doctor and Pharmacist*. The proposed solution is split into 5 modules. These modules cover the entire medical experience for patients, at the same time letting them control access to their data.

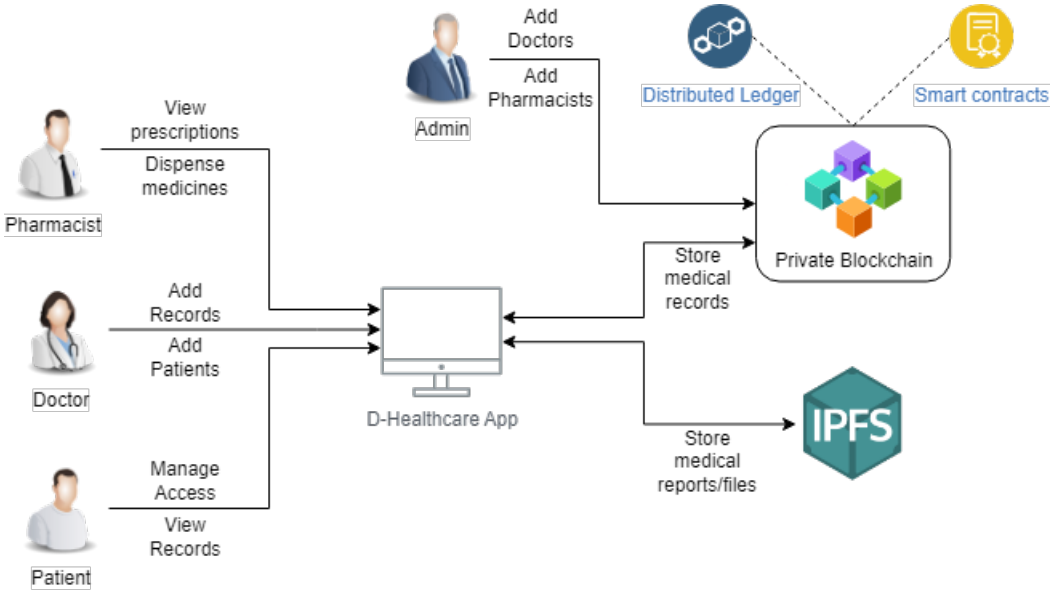


Figure 4.1: System Diagram

*Figure 4.1* shows the overall system diagram depicting the different participants use the application to carry out various functions in the system. Admin is the one responsible for adding doctors or pharmacists into the network. Doctors can then add new patients, and view records of patients to which he/she has access to.

Patients can manage access to their data by granting/revoking read access to doctors. The doctor can add patient records which will be stored on the blockchain. If these records contain any files, they are stored on IPFS. Patient can request for appointments from the medical provider, and doctors can view these requests, and confirm or reject them. Another participant in the network is the pharmacist who is responsible for dispensing medicines to patients based on doctor prescriptions.

*Figure 4.2* depicts the flow of data from and to various entities in the system. *Figure 4.3* is a use case diagram that shows the various actors in the system along with their use cases.

Users (Doctors, patients and pharmacists) can login to the application by providing a valid username and password. Users are logged in if the credentials are valid. After a doctor logs into the application he/she will have the option to register a new patient in the system. Patients can provide all their information to doctors and doctors can add new patients. Doctors must verify that the provided information is valid before registering them. Once the patient is registered all the necessary information to login to the application will be sent to the personal email address of the patient. Patients can use these details to login to the application. Patients can request an appointment to the doctor that they want to visit by providing the address of the doctor and date of appointment. Doctors can view all the appointment requests and can confirm a request by picking a time based on the availability.

Patients can visit the healthcare provider on the date of appointment and the doctor can provide treatment. Doctors can create a new medical record by providing the treatment details. They can also attach files like reports, scan images, etc. if a doctor wishes to know the medical history of a patient, then he/she can request the patient to provide access to view. Patients can manage access to their medical data through the application. They can grant or revoke access to a particular doctor by providing a valid address of the doctor. Only doctors who have access to view the medical records of a particular patient can view the records. The prescriptions that are suggested by the doctor can be viewed by the pharmacist. Pharmacists can login to the application and provide a valid address of the patient to view all the prescriptions that were suggested to the patient. No other personal data of the patient will be made available to pharmacists.

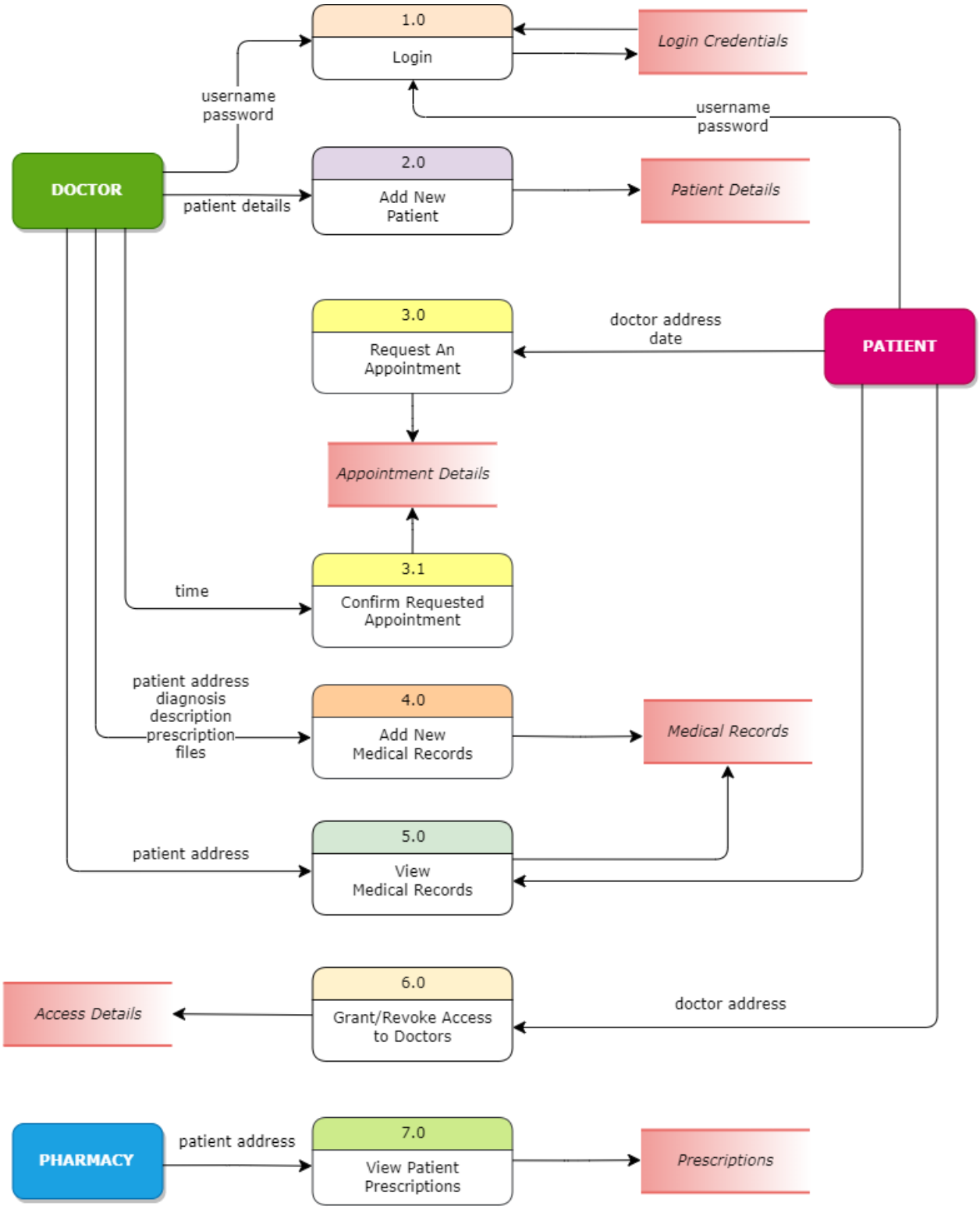


Figure 4.2: Data Flow Diagram

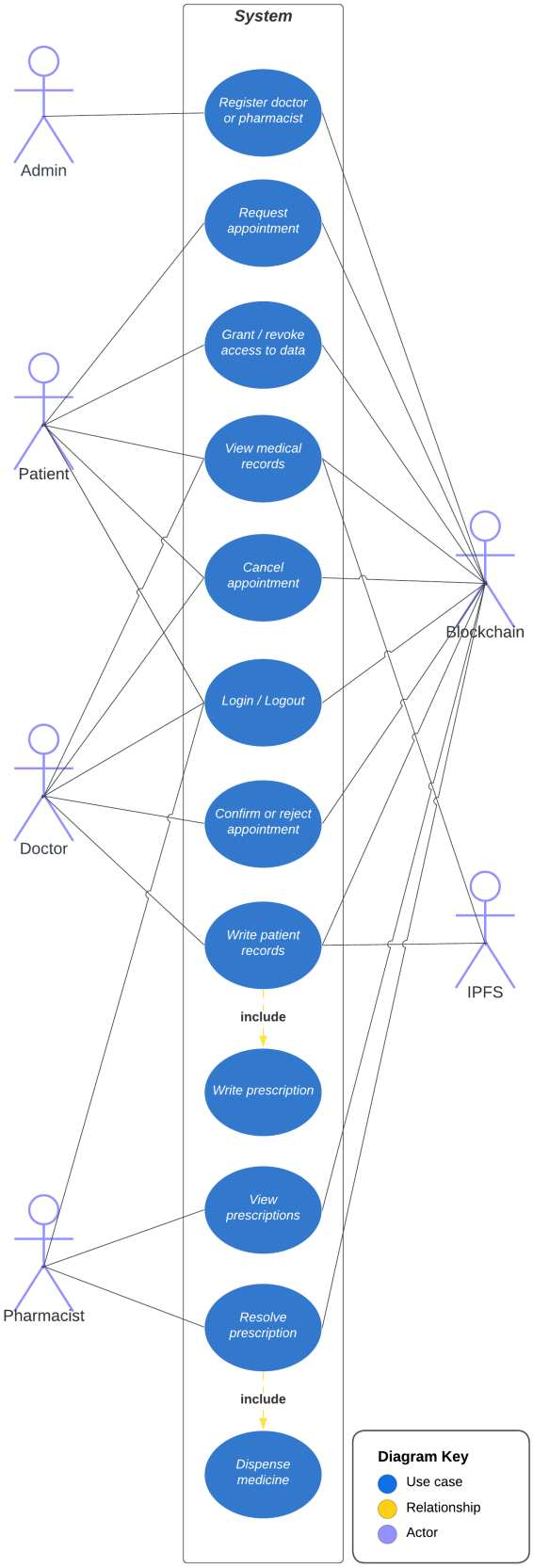


Figure 4.3: Use Case Diagram

## 4.1 Authentication

This module is responsible for allowing users into the network. Doctors and pharmacists will be registered by the administrator. Patients will be registered by the doctor using the web application that is provided. On registration, the patient will receive the private key and password for his account, using which he/she can login and perform their activities.

This module ensures that a user cannot login with an address that has not been registered yet. A user cannot login to an address that is not his/her own. Password entered must match with password corresponding to that address. While the doctor is registering patients, a patient cannot be registered twice. *Figure 4.4* shows the sequence diagram of this module.

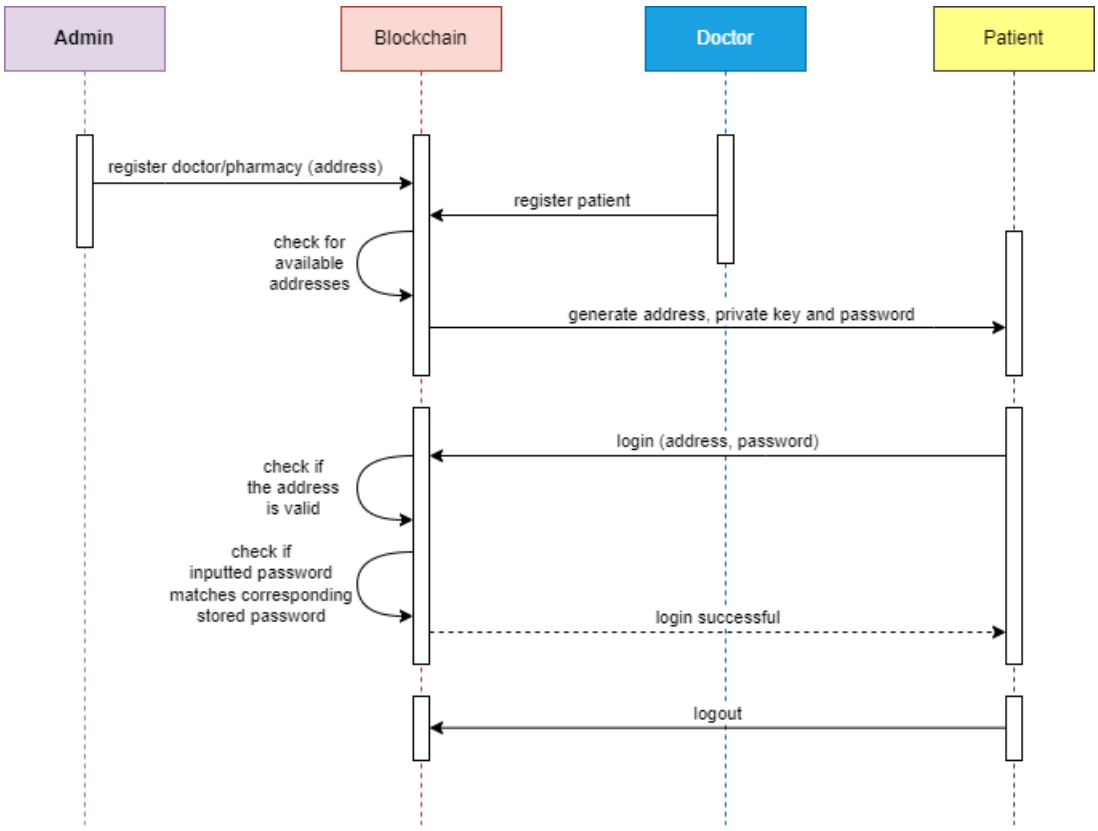


Figure 4.4: Authentication Sequence Diagram

## 4.2 Appointments

Patients can request for appointments at the desired doctor offices for the desired dates. Doctors can view these requests, and can either confirm or reject them. If they confirm, they specify a time for the patient to visit. A patient can delete a pending appointment request or even cancel an appointment that has been confirmed by the doctor. The doctor also has identical capabilities. Once an appointment is complete i.e the patient has visited the doctor during the scheduled time, the doctor can mark the appointment as complete.

This module makes sure that no patient can make an appointment request with an address that has not been registered yet. A patient cannot make an appointment request to an address that does not belong to a registered doctor. *Figure 4.5* depicts the sequence of events involved in the appointment module.

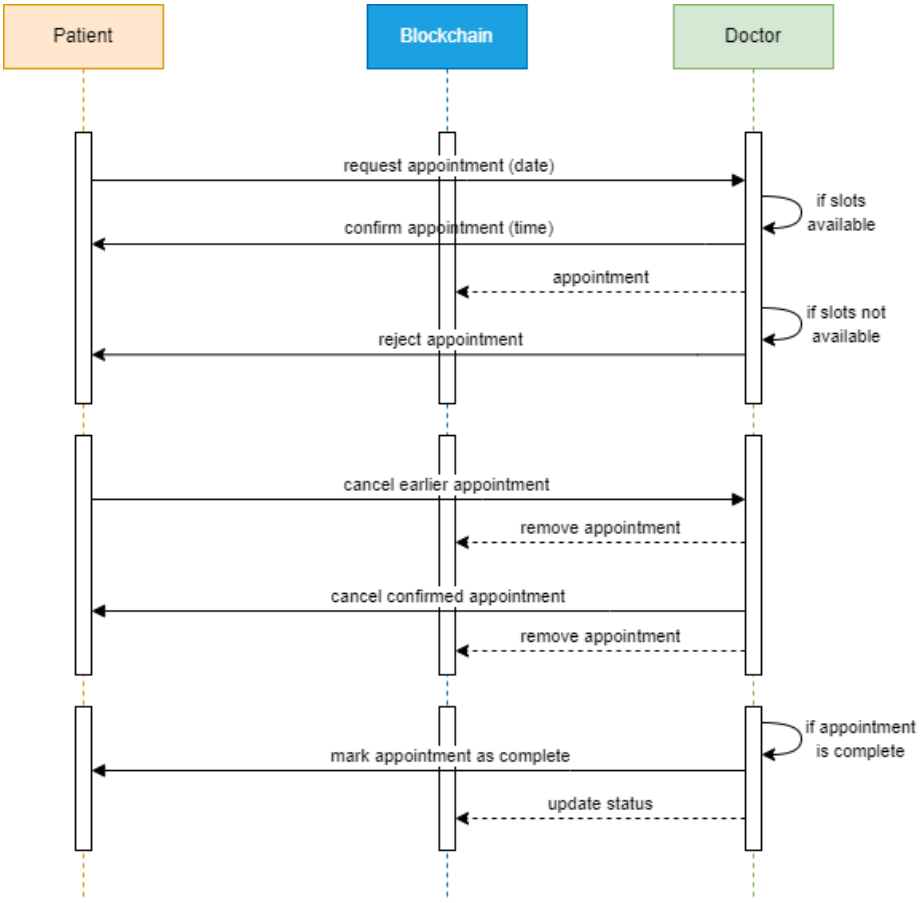


Figure 4.5: Appointment Sequence Diagram

## 4.3 Record Storage and Retrieval

This module allows the doctor to create patient records. Given a valid patient address, doctors can add new records for the patient. These records can contain various fields such as

- Diagnosis
- Description
- Prescription
- Files (if any)

Blockchain is not very good at storing files or large quantities of data. Thus, IPFS (InterPlanetary File System) is used to store the files in the records. IPFS stores the files and returns their hashes which is stored on the blockchain.These new records will be stored on the blockchain and can be retrieved when valid users request them. Valid users here refer to the patients themselves and the doctors who have been given access by the patients. *Figure 4.6* shows the sequence diagram for the storing records and retrieving them.

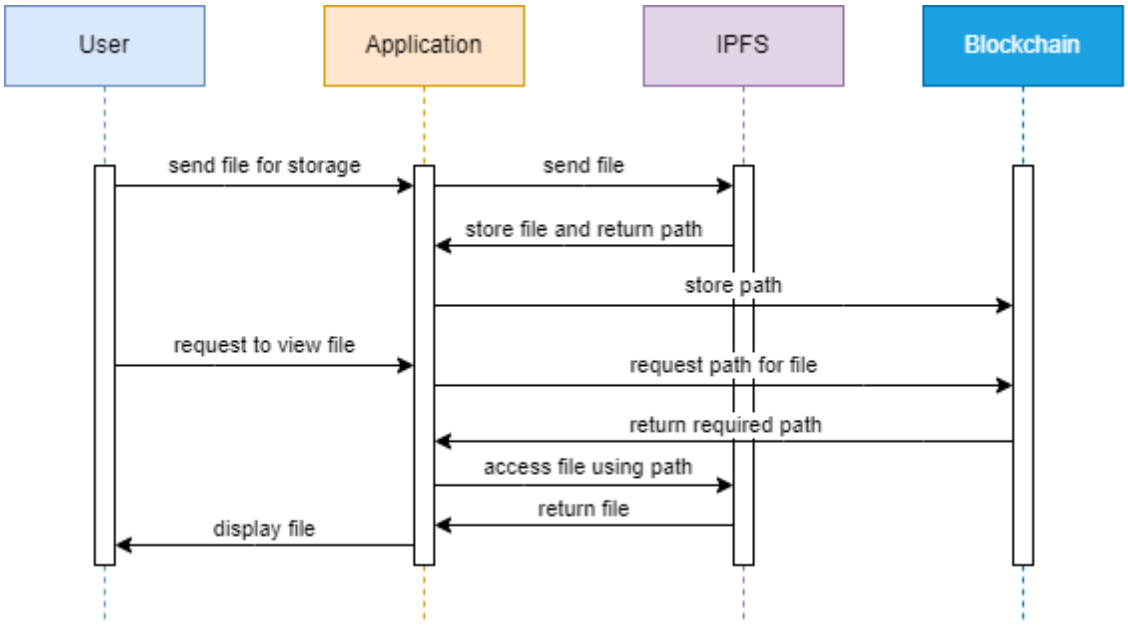


Figure 4.6: Record Storage and Retrieval Sequence Diagram

## 4.4 Access Management

The main objective of this project is to bring control into the hands of the patient over his/her data. This module enables us to meet this objective. The patient can grant/revoke access to read his/her data.

This module ensures that any patient can grant/revoke read access over his/her data to doctors of his/her choice. A doctor who has been granted access to a patient's data can read them as well as write new records for that patient. A doctor not granted access to a patient's data cannot read the patient records, but can write new records. *Figure 4.7* shows the sequence of events responsible for access management.

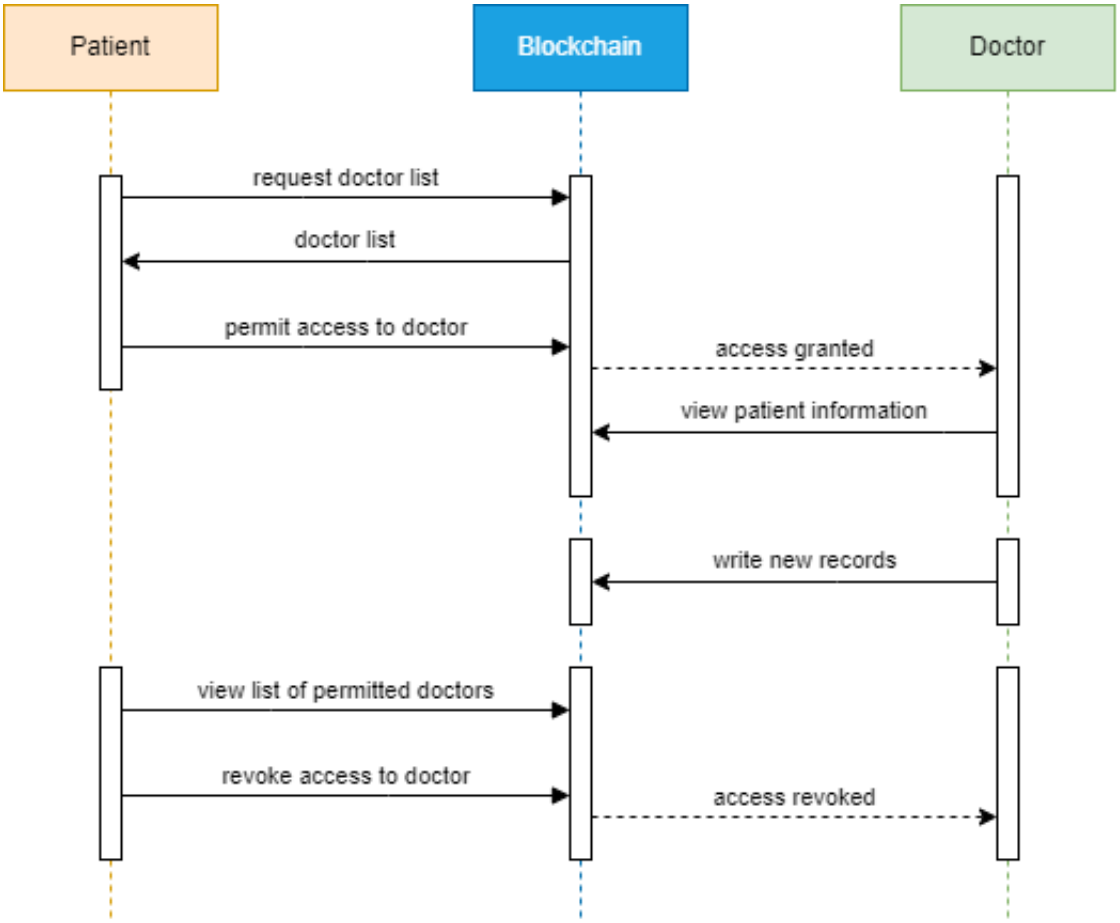


Figure 4.7: Access Management Sequence Diagram

## 4.5 Pharmacy

This module is responsible for the collection of patient prescriptions and the dispensing of medicines at the patient's request. Whenever a doctor creates a patient record, the system checks if the prescription field is blank. If not, the prescription will be sent to the pharmacy. When the patient visits the pharmacy to obtain medicines, he just has to give this address. The pharmacist can use this address to get the list of pending prescriptions, and dispense medicines accordingly. *Figure 4.8* depicts the pharmacy module sequence diagram.

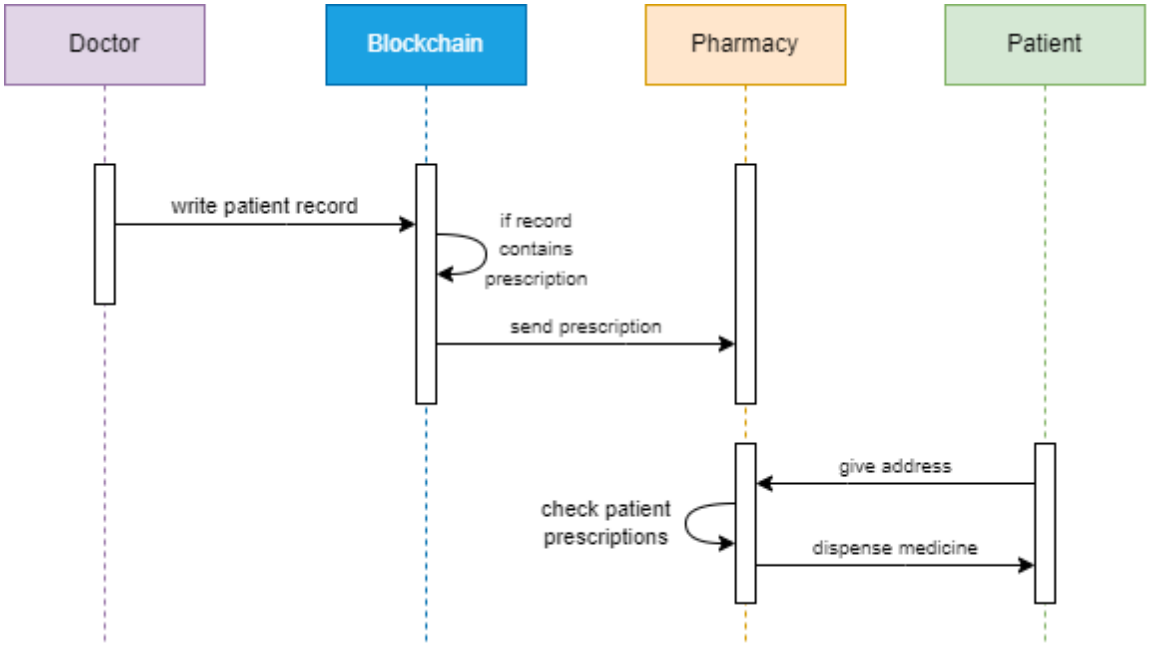


Figure 4.8: Pharmacy Sequence Diagram

# Chapter 5

# Implementation

## 5.1 System Requirements

### 5.1.1 Hardware Requirements

- Processor: Intel Core i5 or Ryzen 5
- RAM: 8 GB
- Hard-disk: 500 GB

### 5.1.2 Software Requirements

- Node v18
- Truffle v5.8.1
- Ganache v7.7.7
- Solidity v0.8.0
- web3.js v1.8
- ReactJS v18.2

## 5.2 Technologies Used

The proposed system architecture/design is implemented using tools like Truffle, Ganache, Solidity, IPFS, ReactJS, web3 js and Metamask.

- **Truffle** is a framework used for building blockchain based applications. It eases the process of writing and deploying smart contracts. It also provides other tools that can be used to develop, deploy and test smart contracts for blockchain apps. It provides the necessary migration code that is required to deploy the smart contracts and users can focus on smart contracts without the need to worry about how to deploy them.

- **Ganache** is a tool, part of the truffle suite, that creates a private ethereum based blockchain on a local system and can be used for testing contracts and development purposes. A workspace can be created for a project by linking the configuration file of the truffle project. By default it creates 10 accounts with 100 ETH each and these accounts can be used to make transactions on the blockchain network.

- **Solidity** is the language that is used to write smart contracts. This language is similar to other high-level languages and supports some of the object-oriented features. It allows users to define their own data types according to the needs of the application it is being used for.

- **IPFS (InterPlanetary File System)** is a peer-to-peer network that is used for distributed storage and sharing of medical records. It uses a decentralized system and stores the files on various nodes in the network. It returns a hash for every file that is stored on the system and this hash can be used to access the files from the network.

- **ReactJS** is a JavaScript library that is used for building user interfaces. It is one of the famous frontend frameworks for developing single page applications. Components can be built and reused whenever required. It is also considered to be fast and easy for development.

- **Web3.js** is another JavaScript library that is used to communicate with the local ethereum node. It has various tools that are required to run a blockchain application like making transactions, fetching data, etc.

- **Metamask** is a browser extension that is used to manage crypto wallets and helps browsers connect to blockchain. It allows users to interact with decentralized applications. It supports various tokens and ethereum networks.

## 5.3 Phases in Implementation

### 5.3.1 Installation & Setup

The first phase in implementation is the installation of required tools and frameworks. Truffle was installed and a sample project was unboxed. The sample project comes with few contracts written in solidity and migration files that are required to deploy those contracts. Then ganache was installed and a workspace was created by linking it with the created truffle project. All the necessary network configurations like host, port number and network id were made in the configurations file of the truffle project. Version of the solidity compiler was also configured according to the need. A react app was created to build the user interface for this application and dependencies were added according to requirement. MetaMask extension was added to the browser and accounts were imported from ganache by providing the private keys. In addition, a dedicated IPFS gateway was created to upload and store files.

### 5.3.2 Smart Contract Development & Deployment

Smart contracts were written in solidity to support all the required functionalities of the system. Various smart contracts were written for patients, doctors and pharmacists. The developed smart contracts were migrated, which compiles the smart contracts written, deploys them into the blockchain network created by ganache and generates JSON files for the deployed contracts. This file contains ABI which can be used in react to call smart contracts. Some of the smart contract functions have been discussed in *Section 5.4*.

### 5.3.3 Frontend Development

*React* was used to create the user interfaces of doctor, patient and pharmacist. Various pages were created for different users based on their roles and functionalities. *Web3 js* library was installed on the react app and imported in the code. The JSON (JavaScript Object Notation) files that were previously created when smart contracts were deployed were also imported into the code. Using this library and ABI, an instance of the deployed smart contracts were created. These instances were then used to call the functions in the smart contracts, whenever required, by passing valid parameters to them. Code was written to store files on the *IPFS* by calling the API for the created gateway and only the hash of the file was stored on the blockchain.

## 5.4 Smart Contracts

Various smart contracts are used to secure patient data, control access, allot appointments and even dispense medicines. Let us take a look at some of the functions that are available to the different participants in the system.

**Algorithm:** Patient Functions

**Function**: permit_access (*addr*)
 **if** *addr is a valid doctor address* **then**
  **if** *doctor does not already have access* **then**
   add *addr* to the permitted list;
  **else**
   display a message that the doctor already has access;
  **end**
**end**

**Function**: revoke_access (*addr*)
 **if** *addr is a valid doctor address* **then**
  **if** *doctor does have access* **then**
   remove *addr* from the permitted list;
  **else**
   display a message that the doctor does not have access;
  **end**
**end**

**Function**: request_appointment (*addr, date*)
 **if** *addr is a valid doctor address* **then**
  create an appointment request at the *addr* doctor's office for the *date*;
**end**

**Function**: view_records ()
 **if** *msg.sender is a valid patient* **then**
  return the patient records;
**end**

**Algorithm:** Doctor Functions

**Function**: add_patient (*aadhaar, name, age, email*)

**if** *aadhaar has not already been registered* **then**

create a patient with the given parameters;

generate a private key and address;

generate a random password;

send an email to the patient with the generated details;

**end**

**Function**: confirm_appointment (*addr, date, time*)

**if** *addr is a valid patient address* **then**

**if** *there exists an appointment request from the patient on date* **then**

change the status of the appointment to *confirmed* at *time*;

**end**

**end**

**Function**: view_records (*addr*)

**if** *addr is a valid patient address* **then**

**if** *doctor has access to records of patient with address addr* **then**

view records of patient with address *addr*

**else**

notify patient about doctor trying to access records

**end**

**end**

**Function**: create_patient_record (*addr, diagnosis, description, prescription, files[]*)

**if** *addr is a valid patient address* **then**

**if** *files[] is not empty* **then**

stores the files in IPFS and get their hashes;

**end**

create a 'record' object with the specified parameters and include these hashes;

**end**

**Algorithm:** Pharmacy Functions

**Function**: view_prescriptions (*addr*)

**if** *addr is a valid patient address* **then**

return the list of prescriptions of patient *addr* where the status is *pending*;

**end**

**Function**: dispense_medicines (*addr, prescription*)

**if** *addr is a valid patient address* **then**

**if** *status of prescription is pending* **then**

change the status of *prescription* to *resolved*;

**end**

**end**

# Chapter 6

# Results

The results of the implementation are given below.

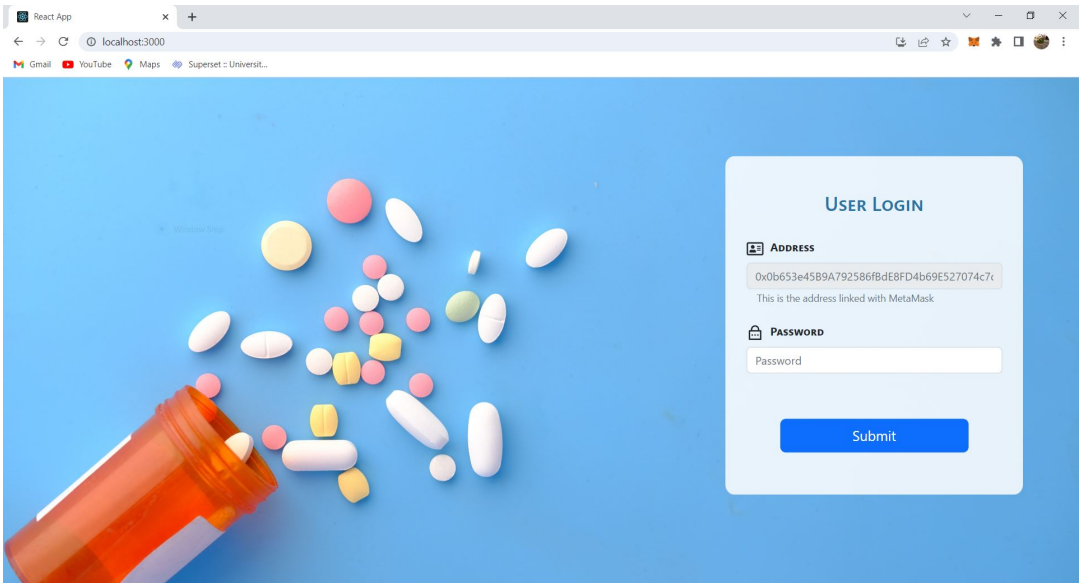


Figure 6.1: Login Page

*Figure 6.1* shows the user interface of the LOGIN page. All the users (Doctor, Patient and Pharmacist) will have a common login page. The credentials that are required to login are 'Address' and 'Password'. The 'Address' field is disabled and the active *Metamask* account's address is automatically detected and filled. Users can just check if the 'Address' that is displayed is their own address and enter their 'Password'.

Users will be able to successfully login if the entered 'Password' matches with the password corresponding to that address, stored on the blockchain. If the 'Password' does not match then an error message is displayed to the user. After successful login, different users will be redirected to different pages based on their roles.

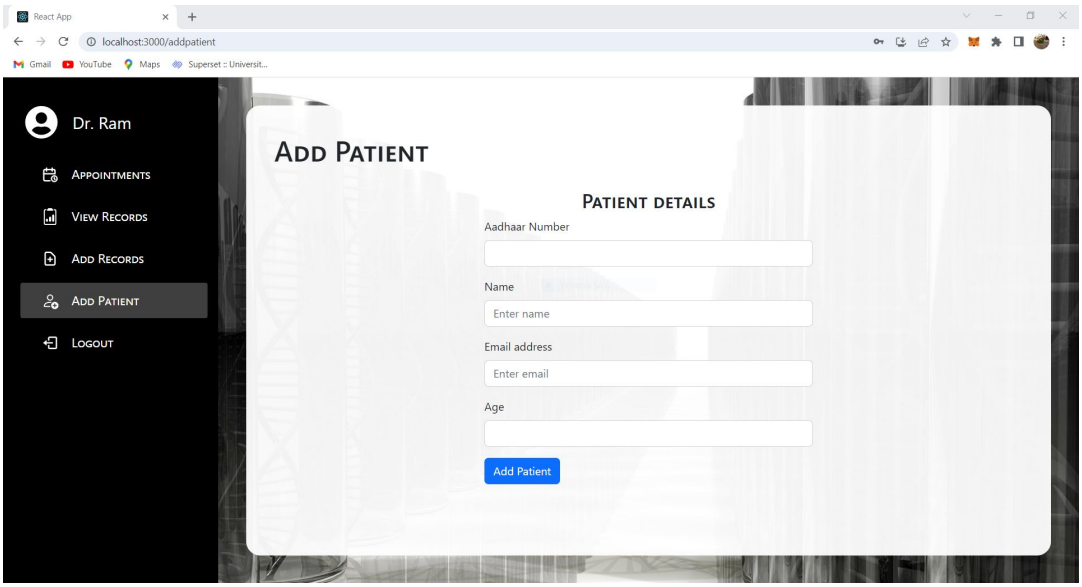


Figure 6.2: Add Patient

*Figure 6.2* shows the ADD PATIENT page. This page is only accessible by doctors. Doctors can add patients to the blockchain network by adding their basic details like Aadhaar number, name, age, email, etc. All the details entered must be valid. To ensure there is no duplication of patient registration, aadhaar number is used to verify that the user is not already present in the network. If the entered aadhaar number already exists in the network, an appropriate error message is displayed. After entering all the basic details the patient will be added to the blockchain network and an 'Address' and 'Private Key' will be assigned to the patient. The 'Address' and 'Private key' along with the login credentials will be sent to the email of the patient that was used during the registration. Patient can use these details to login to his/her account.

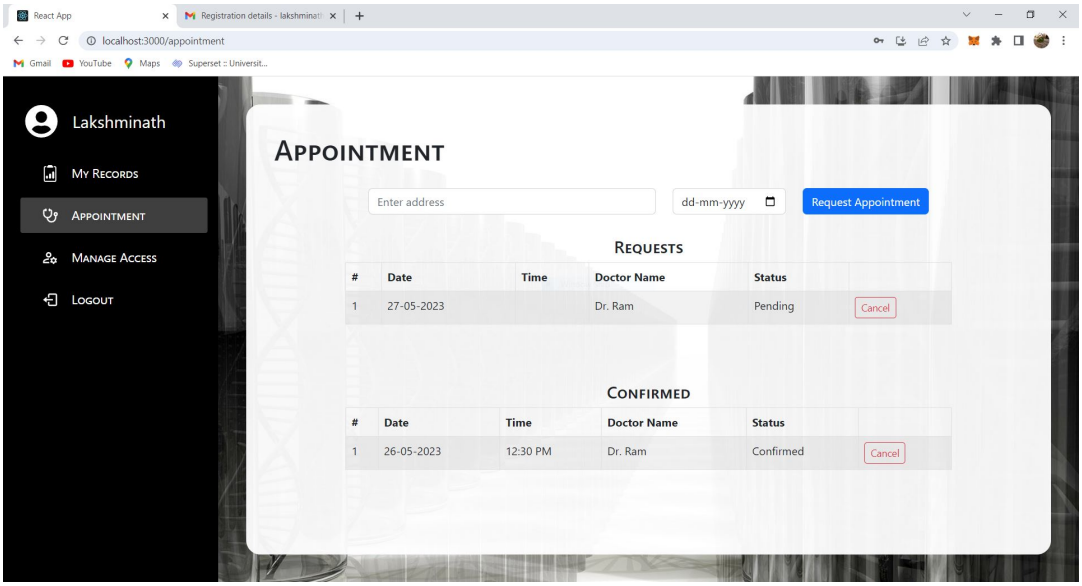


Figure 6.3: Appointment Page for Patient

*Figure 6.3* shows the APPOINTMENT page for patients. Patients can request an appointment to a doctor by entering the address of the doctor and selecting the date. Once the request is made, the status of the appointment is marked as pending and is displayed in the requests table. Patients will also have an option to cancel their appointment request by clicking on the cancel button corresponding to the appointment that is to be cancelled. Once the doctor accepts this request, the status of the appointment is changed to confirmed and is displayed in the confirmed appointment table. Patients can also cancel the confirmed appointment using the *cancel* button.

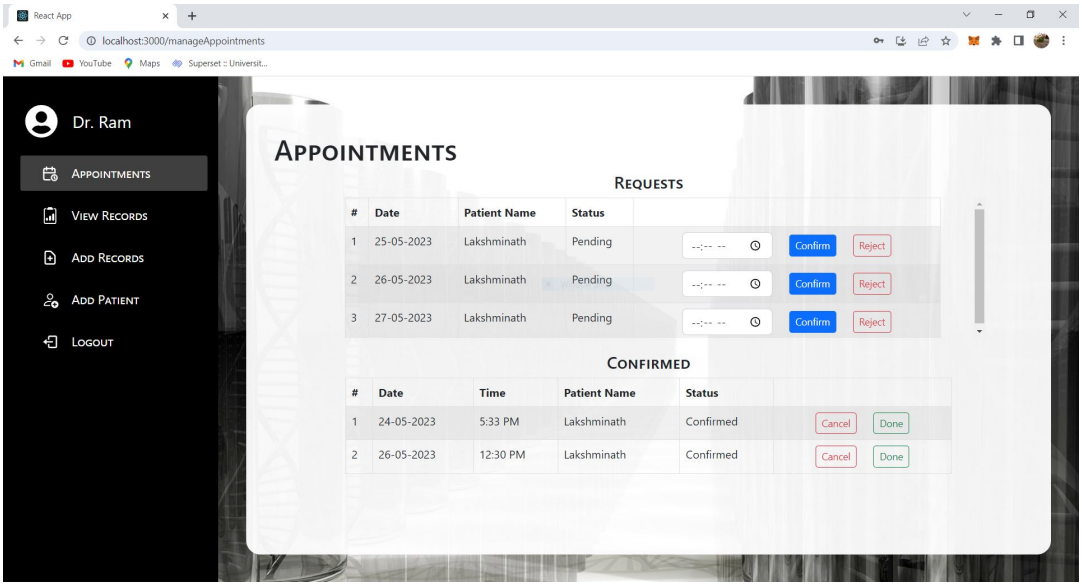


Figure 6.4: Appointment Page for Doctor

*Figure 6.4* shows the APPOINTMENTS page for doctors. Only doctors will be able to view this page. The appointment requests that are made by patients are displayed to the doctor in the requests table with the name of the patient and the date. Doctor can check his/her availability on that particular date and confirm the appointment by selecting the time. Once the appointment is confirmed by the doctor, a notification is sent to the patient through email about appointment confirmation with the time. Doctors can also cancel the requests made by patients by stating the reason and the same will be conveyed to the patient via email. Once the appointment is confirmed, its status is changed to confirmed and moved to the confirmed appointments table. Doctors will also have an option to cancel the confirmed appointments similar to cancellation of requests.

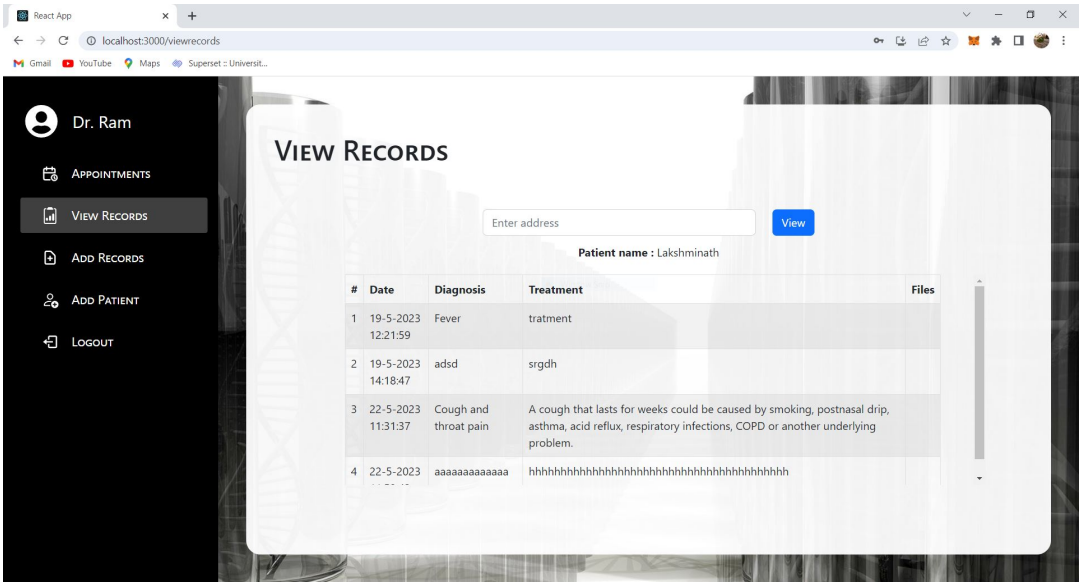


Figure 6.5: View Records Page for Doctor

*Figure 6.5* shows the VIEW RECORDS page for doctors. Doctors can view the previous medical records of the patient by entering the address of the patient, only if the patient has granted access to his/her medical records. Previous medical records details include date of treatment, doctor name, treatment, prescriptions, medical reports, etc. If a doctor does not have access to medical records of a patient, an appropriate message is displayed and also a notification is sent to the patient that the doctor is trying to access the records. The patient can decide whether or not to grant access to that particular doctor.

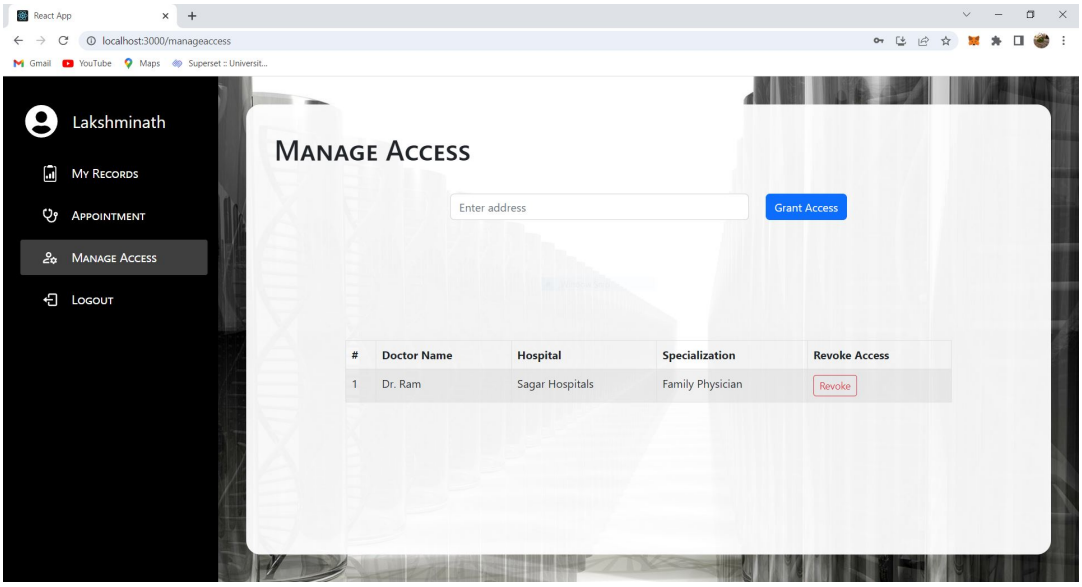


Figure 6.6: Manage Access Page for Patient

*Figure 6.6* shows the MANAGE ACCESS page for patients. Patients can grant or revoke access to doctors to view their medical records. To grant access, a patient must enter the address of the doctor to whom the medical records have to be shared. After entering the address, the patient can click on the grant access button which fetches the details of the doctor corresponding to that entered address. The details include doctor name, hospital name, specialization, etc. After verifying the details of the doctor, the patient can confirm to grant access to that doctor. Once the access is granted the details are shown in a table. This table shows the details of all the doctors that have access to patients' records. Patients can manage access through this table. If the access has to be revoked, the patient can click on the revoke access button and the access for that doctor will be revoked.

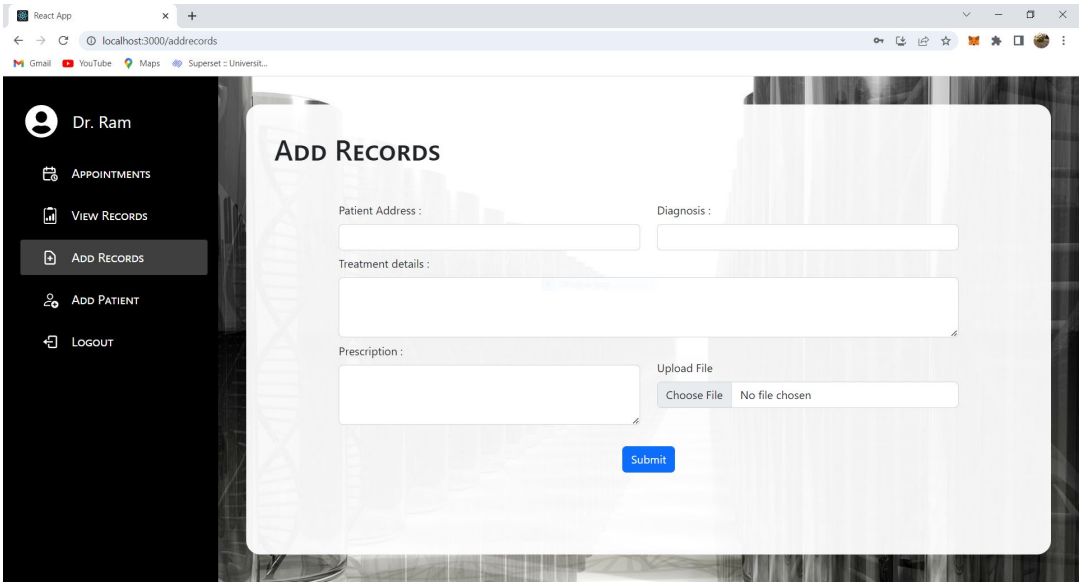


Figure 6.7: Add Record Page for Doctor

*Figure 6.7* shows the ADD RECORDS page for doctors. This page allows doctors to add new medical records for patients and only doctors will have access to this page. Doctors can add new medical records by entering the details like patient address, diagnosis, treatment details, prescriptions, medical reports, etc. The entered address must be valid for adding a new medical record. Once the doctor enters all the details and clicks on submit, the report files are stored on the IPFS which returns a hash for the file. The other medical record details along with the hash of the file are stored on the blockchain.


Figure 6.8: My Records Page for Patient

*Figure 6.8* shows the MY RECORDS page for patients. Patients can view their medical records through this page. This page displays all the medical records belonging to that particular patient with just one click. All the details of the records are displayed like treatment date, diagnosis, treatment, doctor name, etc. These details also include files like x-ray images, scan reports, etc. Patients can view these files by clicking on the links provided under the files column and the files will be displayed to the patient from IPFS.

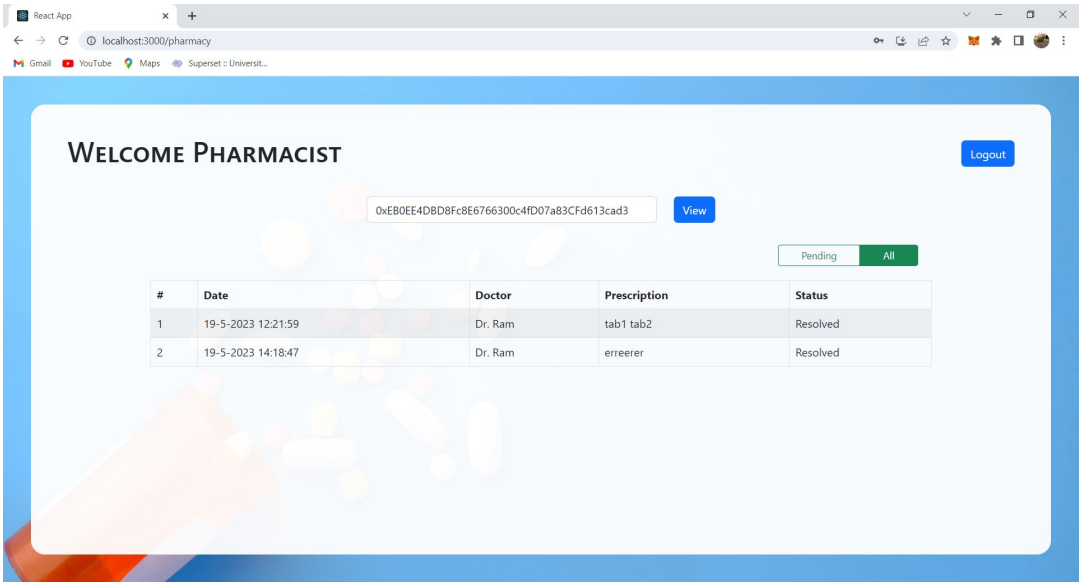


Figure 6.9: View Prescriptions Page for Pharmacy

*Figure 6.9* shows the VIEW PRESCRIPTIONS page for pharmacists. Pharmacists can get all the prescriptions that are suggested to the patient through this page. To get the prescriptions for a particular patient, pharmacists must enter the address of the patient and click the view button. This will show all the prescriptions of the patient that are not dispensed. The status of these prescriptions will be pending and pharmacists can click on the resolve button to change the status to resolved after the medicines are dispensed. This will remove the prescription from the pending list. Pharmacists can also view the resolved prescriptions by going to the all prescriptions tab. A toggle button is provided to view all and pending prescriptions. If there are no prescriptions found for the entered address, an appropriate message is displayed.

# Chapter 7

# Conclusion and Future Work

This system represents a promising blockchain-based health solution designed to address the challenges faced by governments in managing scattered health data and projecting accurate healthcare needs. By leveraging the advantages of blockchain technology and smart contracts, the system offers a secure, reliable, and decentralized system for managing health-related information. This enables governments to create a synchronized environment where health data can be effectively utilized for planning and decision-making.

The integration of smart contracts automates various processes, reducing administrative burdens and improving efficiency. Users can initiate requests and inquiries regarding appointments, medical tests, medications, and procedures through a user-friendly graphical interface. The system provides autonomy and transparency, promoting collaboration among stakeholders while maintaining data privacy.

A separate application can be built for Admin for managing doctors and pharmacists. Granular access to medical records can be provided. This will allow patients to manage who will have access to individual records of patient. Pharmacy module can further be developed to manage availability of medicines. Further, lab technicians can also be added into the system that will allow in them adding the reports or scan results of patients directly.

It is important to recognize that the implementation of this system would require careful consideration of various factors, including regulatory compliance, data standardization, scalability, and user adoption. Further research, development, and collaboration among stakeholders are necessary to refine the system and ensure its successful deployment in real-world healthcare settings.

# References

[1] S. Tanwar, K. Parekh, and R. Evans, "Blockchain-based Electronic Healthcare Record System for healthcare 4.0 applications," Journal of Information Security and Applications, vol. 50, p. 102407, 2020. doi:10.1016/j.jisa.2019.102407

[2] H. Han, M. Huang, Y. Zhang, and U. A. Bhatti, "An architecture of secure health information storage system based on Blockchain technology," Cloud Computing and Security, pp. 578–588, 2018. doi:10.1007/978-3-030-00009-752

[3] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," Journal of Medical Systems, vol. 42, no. 8, 2018. doi:10.1007/s10916-018-0995-5

[4] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, "Blockchain-based personal health data sharing system using cloud storage," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018. doi:10.1109/healthcom.2018.8531125

[5] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-based personal health records sharing scheme with data integrity verifiable," IEEE Access, vol. 7, pp. 102887–102901, 2019. doi:10.1109/access.2019.2931531

[6] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in Cloud Environments,” Information, vol. 8, no. 2, p. 44, 2017. doi:10.3390/info8020044

[7] A. Shahnaz, U. Qamar, and A. Khalid, “Using blockchain for Electronic Health Records,” IEEE Access, vol. 7, pp. 147782–147795, 2019. doi:10.1109/access.2019.2946373

[8] A. Buzachis, A. Celesti, M. Fazio, and M. Villari, “On the design of a blockchain-as-a-service-based health information exchange (BaaS-HIE) system for patient monitoring,” 2019 IEEE Symposium on Computers and Communications (ISCC), 2019. doi:10.1109/iscc47284.2019.8969718

[9] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “MedRec: Using blockchain for Medical Data Access and permission management,” 2016 2nd International Conference on Open and Big Data (OBD), 2016. doi:10.1109/obd.2016.11

[10] K. N. Griggs et al., “Healthcare blockchain system using smart contracts for secure Automated Remote Patient Monitoring,” Journal of Medical Systems, vol. 42, no. 7, 2018. doi:10.1007/s10916-018-0982-x

[11] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, “Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using Blockchain Technology,” Sustainable Cities and Society, vol. 39, pp. 283–297, 2018. doi:10.1016/j.scs.2018.02.014

[12] D. Lee and M. Song, “MEXchange: A privacy-preserving blockchain-based framework for health information exchange using ring signature and stealth address,” IEEE Access, vol. 9, pp. 158122–158139, 2021. doi:10.1109/access.2021.3130552

[13] S. Jiang et al., “Blochie: A blockchain-based platform for Healthcare Information Exchange,” 2018 IEEE International Conference on Smart Computing (SMARTCOMP), 2018. doi:10.1109/smartcomp.2018.00073

[14] J. Zhang, N. Xue, and X. Huang, “A secure system for pervasive social network-based healthcare,” IEEE Access, vol. 4, pp. 9239–9250, 2016. doi:10.1109/access.2016.2645904

[15] S. Purohit et al., “Honestchain: Consortium blockchain for Protected Data Sharing in Health Information Systems,” Peer-to-Peer Networking and Applications, vol. 14, no. 5, pp. 3012–3028, 2021. doi:10.1007/s12083-021-01153-y

[16] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A blockchain-based medical data sharing and protection scheme,” IEEE Access, vol. 7, pp. 118943–118953, 2019. doi:10.1109/access.2019.2937685

[17] Y. Zhuang, L. Sheets, Z. Shae, JJP. Tsai and CR. Shyu, ”Applying Blockchain Technology for Health Information Exchange and Persistent Monitoring for Clinical Trials,” AMIA Annu Symp Proc. 2018

[18] T. Space, “What is genesis block and why genesis block is needed?,” Medium, https://tecracoin.medium.com/what-is-genesis-block-and-why-genesis-block-is-needed-1b37d4b75e43 (accessed Jun. 7, 2023).