# PATIENT HEALTH RECORD MANAGEMENT USING BLOCKCHAIN

A PROJECT REPORT

submitted By

**ARAVIND KRISHNA A V**
**TVE21MCA2020**

**to**

the APJ Abdul Kalam Technological University
in partial fullfilment of the requirements for the award of the degree

**of**

Master of Computer Applications

**Department of Computer Applications**
College of Engineering
Trivandrum-695016

NOVEMBER 2022

# Declaration

I undersigned hereby declare that the project report titled **"Patient Health Record Management Using Blockchain"** submitted for partial fulfillment of the requirements for the award of degree of Master of Computer Applications of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by me under supervision of Sri. Shine S, Asso.Professor. This submission represents my ideas in my words and where ideas or words of others have been included. I have adequately and accurately cited and referenced the original sources. I also declare that I have adhered to ethics of academic honesty and integrity as directed in the ethics policy of the college and have not misrepresented or fabricated any data or idea or fact or source in my submission. I understand that any violation of the above will be a cause for disciplinary action by the Institute and/or University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title.

Place : Trivandrum **Aravind Krishna A V**

Date : 25/11/2022

**DEPARTMENT OF COMPUTER APPLICATIONS**

**COLLEGE OF ENGINEERING**
**TRIVANDRUM**

## CERTIFICATE

This is to certify that the report entitled **Patient Health Record Management Using Blockchain** submitted by **Aravind Krishna A V** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Master of Computer Applications is a bonafide record of the project work carried out by him under my guidance and supervision. This report in any form has not been submitted to any University or Institute for any purpose.

Guide                                                                                                    Supervisor

Head of the Dept

# Acknowledgement

First and for most I thank **GOD** almighty and to my parents for the success of this project. I owe a sincere gratitude and heart full thanks to everyone who shared their precious time and knowledge for the successful completion of my project.

I am extremely thankful to **Dr. Suresh Babu V**, Principal, College of Engineering Trivandrum for providing me with the best facilities and atmosphere which was necessary for the successful completion of this project.

I am extremely grateful to **Dr. Deepa S S**, HOD, Dept of Computer Applications, for providing me with best facilities and atmosphere for the creative work guidance and encouragement.

I express our sincere thanks to **Sri. Shine S**, Asso. Professor, Department of Computer Applications, College of Engineering Trivandrum for his valuable guidance, support and advice that aided in the successful completion of my project.

I profusely thank other Asst. Professors in the department and all other staffs of CET, for their guidance and inspirations throughout my course of study.

I owe my thanks to my friends and all others who have directly or indirectly helped me in the successful completion of this project. No words can express my humble gratitude to my beloved parents and relatives who have been guiding me in all walks of my journey.

**Aravind Krishna A V**

# Abstract

The need for maintaining an accurate and infallible record of an individual's medical records and bills can't be understated. Reproducing these documents is essential to ensure that the insurance claim process goes about smoothly and without hinderance. Conventional methods of record keeping often prove to be inefficient and vulnerable to data leakage.This Blockchain based Patient Data Management System has been designed to eliminate any scope of fraud or manipulation that could take place with respect to the processing of medical bills and the insurance claim. This system consists of the three entities: Hospital Department, Medical Department, Insurance Company. The Hospital Department needs to first add the patient and create their id. Once the patient id is created, the medical department of the hospital can start adding the bills. The insurance company can search for patients using their id and recover all the bills uploaded by the medical department. After the bills have been recovered from the hospital's side, the insurance company can cross check them against the bills submitted by the patient. In this proposed work, the Data of patient mostly the finance related data is being added here. It's difficult to understand or keep a track of the bills for any user. Since there are a lot of scams going with respect to hospital and insurance companies when the final settlement is done. Blockchain technology kills scope of manipulation and tampering of the data, here the insurance company has access to the bills added by the company plus it can added the bills which the patient has to cross verify if there has been any kind of manipulation by the hospital end.

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Introduction

Blockchain has been a buzzword in Information and Communication Technology industry in recent years. The rise of this new technology has greater potentials to solve data privacy, security, and integrity issues. The word blockchain came in the front line after the publication of the Bitcoin white paper by Satoshi Nakamoto in 2008.The fundamental mechanism behind Bitcoin is to make financial transactions possible without the intervention of a trusted third party. The technology is mainly considered a distributed Peer to Peer(P2P) network where digital data may publicly or privately be allocated to all users on the web in a secure and verifiable way. In traditional financial transactions, both sender and receiver need to depend on a Trusted Third Party (TTP), e.g., bank. It involves a few security issues and operational difficulties. For instance, a TTP gets access to a user's financial data, which indicates the lack of user privacy. Moreover, the time involved in a TTP transaction is lengthy as there are many steps in between the operation. Furthermore, users need to pay the TTP for their service. Bitcoin solves the above limi- tations and makes the TTP vanish for a successful transaction between two users.

Many surveys have been published on the application of blockchain in various areas. Among these papers, many were systematic reviews on the application of blockchain in healthcare sectors. Researchers discussed blockchain technology's limitations, possible applications, and future directions in healthcare, government, supply chain, and many other fields. We have proposed a comprehensive SLR on the application of blockchain to manage EHRs.

# Chapter 2

# Problem Defnition and Motivation

The proposed system makes use of blockchain and RFID by utilising the capabilities of a certain sort of smart contract that was created using a special structure. This offers encryption and therefore safe data transfer. The blockchain records and verifies transactions, which cannot be reversed, hacked, or erased.

The motivation behind the project was the drawbacks of the existing system as well as the unexplored applications of blockchain technology. The existing system require huge amount of human resources and lot of hardware equipment is needed for surveillance and tracking. The quality of the hardware also can impact the data which is collected. Automobile tracking can tamper the privacy of the user and today no such system in place that can be both secure and effective. When the data is handled through blochain, the handled data is secure, immutable or hacked.

## 2.1 Existing System

In the existing system the records are stored and maintained under the organization. So that, the patient can't able to access these records for further references. When the particular server(database) gets crashed then all the records will be spoiled. To overcome these drawbacks the proposed system is developed. Electronic Records (EHRs) provide a convenient record storage service, which promotes traditional patient medical records on paper to be electronically accessible on the web. In the current situation, patients scatter their EHRs across the different areas during life events, causing the EHRs to move from one service provider database to another.

Therefore, the patient may lose control of the existing healthcare data, while the service provider usually maintains the primary stewardship. Patient access permissions to EHRs are very limited, and patients are typically unable to easily share these data with researchers or providers. Interoperability challenges between different providers, hospitals. The patient should have right to access his EHRs for managing and sharing them independently Institutions, etc.

This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved. Without coordinated data management and exchange, the records are fragmented instead of cohesive. If the patient has the capability of managing and sharing his EHRs securely and completely.

### 2.1.1 Limitation of Existing System

- Privacy and Cybersecurity Issues
- Inaccurate Data
- Lack of secure accessibility
- Lack of interoperability

## 2.2 Proposed System

In the proposed future system, the patient should have right to access his EHRs for managing and sharing them independently. The patient can be access his medical report directly and can use the digitalized report with anyone. By storing the data in the blockchain the user's data is encrypted and stored as blocks in the etherscan. The user stores data by two way authentication process such as getting secret key generated by the Metamask. Electronic Health Record Systems are proprietary that is centralized by design. This means that, there's a single supplier that controls the code base, database and the system outputs and supplies the monitoring tools at the same time. It is difficult for centralized systems to gain trust from patients and doctors and hospital management. Open source, independently verifiable systems solves this issue. This system was designed to allow patients to possess the control of generating, managing and sharing EHRs with family, friends, healthcare providers and other authorized data consumers. Moreover, provided that the healthcare researcher and providers of such service access these EHRs across-the aboard, the transition program of healthcare solution is expected to be achieved.

A blockchain is managed by a network of computers where there is no single computer is responsible for maintaining or storing the data, and any computers can enter or leave this network at any time Using Blockchain for records can make the whole process End to End verifiable and transparent. The stored data will be transactions, from which we can create a blockchain that will keep track of the database of the patient records. Using this approach, all the patients can make use of the records by themselves, and because of the blockchain they can use these records without any permission request from the organization directly by using the secret key given to them.

### 2.2.1 Advantages of Proposed System

- Can be implemented as an upgrade to existing toll booth and similar checkpoints.
- Hardware used is economical.
- Quality of hardware is not an issue.
- Collected data is secure with the help of blockchain.
- Passive RFID tags do not need power source also has no moving parts making the tags more effective in the tracking system. as it is attached to automobiles.
- Human resource needed is very low, with the touch of a button the automobile can be traced.

# Chapter 3

# Literature Review

Authors in [2] presented the MedRec system, a decentralized medical record management system based on blockchain technology. There are three types of Ethereum smart contracts to associate patients' medical data to allow third-party users to access the data. Yang et al. [3] further presented an attribute-based authentication mechanism on the MedRec system to enable the secure sharing of medical data. A high-level blockchain-based framework was designed in [4], where an identity-based authentication and key agreement protocol is applied to achieve user membership authentication. They also developed the MedShare [5] system to provide data provenance and control in cloud repositories among hospitals. Liang et al. [6] used the hyperledger fabric membership service and channel formation scheme to guarantee data privacy in a blockchain network for medical data sharing. The mobile application was also implemented to collect data from wearable devices for storage and sharing with healthcare providers. Patientory [7] is a peer-to-peer medical record data storage network. The software framework in [7] was presented to address the authentication, authorization, access control, data encryption interoperability enhancement and token management.

Authors in [8] proposed the MedChain system, where the timed-based smart contracts can interact with the various demands of health providers, patients and third parties. An incentive mechanism in [8] was also presented to leverage the degree of health providers about their efforts on maintaining medical records. In [9], an attribute-based signature scheme with multiple authorities was designed. There are multiple authorities without a centralized one to generate and deliver public/private keys of the patient, avoiding the escrow problem. Liu et al. [10] presented a healthcare insurance anti-fraud system based on blockchain. A hybrid architecture to facilitate access control of medical data was developed in [11]. A blockchain is used to manage identity and access control and acts as a tamper-proof log of access events. Hasavari et al. [12] introduced a combination of secure file transfer methods and blockchain techniques as a solution to record patient's emergency medical data such that ambulance crews can access and use it to provide high quality pre-hospital care.

# Chapter 4

# Requirement Analysis

## 4.1 Purpose

Blockchain can transform the way a patient's electronic health records are stored and shared. It can provide a safer, more transparent, and traceable underpinning system for health information exchange. The technology has the potential to connect multiple data management systems working in silos and provide what could be a connected and interoperable electronic health record system.

## 4.2 Overall Description

At checkpoints, RFID-tagged vehicles are scanned with an RFID reader. Each RFID tag has a unique identifier that is uploaded to the blockchain network, forming a chain of checkpoints that the vehicle travelled through and allowing the vehicle's path to be tracked.

### 4.2.1 Hardware Requirements

- Processor : Intel Core i3
- Storage : 512 GB Hard Disk space
- Memory : 4 GB RAM

### 4.2.2 Software Requirements

- Operating System : Linux/Windows
- Back-end : Nodejs, PHP, Solidity, Ganache
- Smart contract IDE : Remix IDE
- Cryptocurrency wallet : Metamask

## 4.3 Functional Requirements

All of the actions or processes that the proposed system should accomplish are included in the functional requirements. It consists of

### 4.3.1 NodeJs

Nodejs is a cross-platform runtime environment for creating server-side and networking applications that is open source. Nodejs apps are written in JavaScript and run on OS X, Microsoft Windows, and Linux using the Node.js runtime. Node.js also comes with a large library of JavaScript modules, which greatly facilitates the creation of web applications with it.

### 4.3.2 Web3.js

Web3.js is a group of libraries that allow you to interface with an ethereum node over an HTTP or IPC connection. By developing smart contract code that reads and publishes data from the blockchain, Web3.js allows you to create blockchain-aware websites or clients. Clients for interacting with the Ethereum Blockchain are being created. It's a collection of libraries that, among other things, allow you to send Ether from one account to another, read and write data from smart contracts, and create smart contracts.

### 4.3.3 Ethereum Blockchain

The Ethereum blockchain resembles the bitcoin network in many ways. Ethereum is entirely decentralised, similar to the bitcoin network. The fact that Ethereum is programmable is one of the features that sets it apart from bitcoin. Each block in the blockchain contains a code snippet known as smart contracts, in addition to the transactions. The Merkle tree is a crucial data structure employed by Ethereum. A hash value is assigned to each transaction in Ethereum. Merkle tree is a tree constructed using transaction hash values. Two transactions are coupled within a block to generate a single hash. Then two paired transactions are combined to generate a new hash. This procedure continues until the root hash is a single hash. The root of a Merkle tree is the result of all transactions in that block.

### 4.3.4 Smart Contract

Smart contracts are critical components that reside in the form of snippets of code within the blocks of blockchain. The smart contract programming language Solidity is the most widely used. The javascript code and Solidity is fairly similar. Smart contracts are a collection of rules and conditions that must be obeyed when conducting business. Smart contracts are crucial because they eliminate the requirement for third-party verification.

### 4.3.5 Ganache

Ganache is used to emulate blockchain. Ganache is a personal Ethereum blockchain that can be used to deploy contracts, create apps, and conduct tests. It comes as a desktop program and a command-line tool. It allows you to do whatever you could on the main chain for free. This is how many developers test their smart contracts while they're still in development. It has useful features like enhanced mining controls and a built-in block explorer.

### 4.3.6 IPFS

IPFS is a distributed data storage technology with a peer-to-peer network. Because IPFS data is safe from alteration and assures secure data storage, any attempt to alter data saved on IPFS can only be performed by changing the identifier. Hence, it provides a cryptographic identity to protect data from manipulation. Every data file stored on IPFS contains a cryptographically generated hash value. It only has one value and is used to identify data files stored on IPFS. The IPFS protocol makes use of a peer-to-peer (P2P) connection that includes an IPFS object, which contains data and linkages. The data is an array of disorganized binary values, while the link is a disorderly binary value.

## 4.4 Non Functional Requirements

### 4.4.1 Performance Requirements

- Unique ID : Each tag contains unique id.
- Cost Effective : Implementing the suggested system is fairly inexpensive.
- Less human resources needed :Compared to the current system, there is less human engagement.
- Secure : Security properties of blockchain is achieved in this project.
- User Friendly : UI is built with simplicity in mind. The working of the system can be handled by the user with ease.

# Chapter 5

# Design And Implementation

## 5.1 Overall Design

The proposed system has client server architecture. The system has both a client and a server component. The web browser inputs the data from the user and transfers the data to the server via the client portion. PHP is used on the server side, whereas react js and HTML are used on the client side. The output is made visible to the user via a client side made using HTML and react js, Through web3 injection smart contract is deployed.

## 5.2 System Design

The system is web based. The input is taken from the user and is passed to the php program running in the server side. The server side program sends the data to the blockchain network with the help of smart contract. The records are added with the transaction address from the ganache to the ipfs.

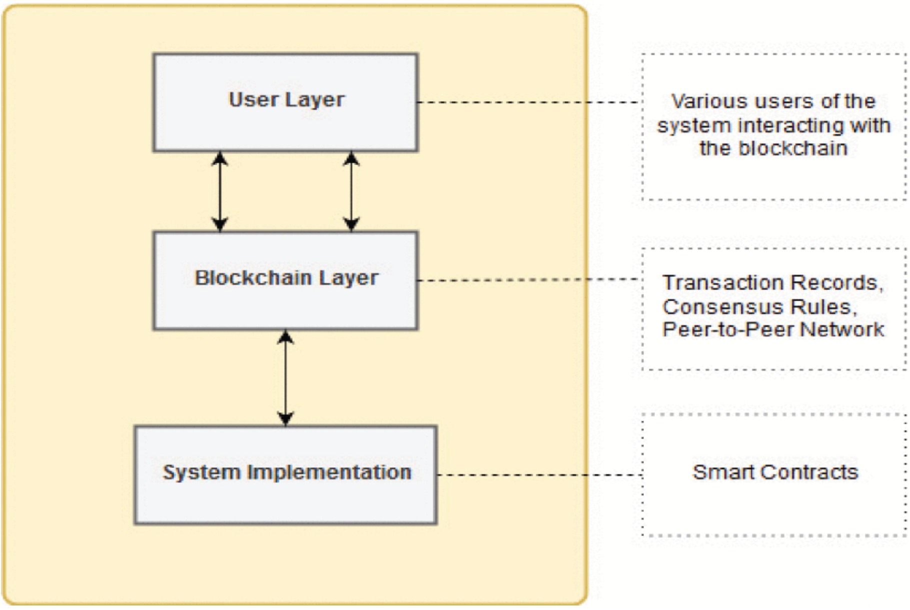


Figure 5.1: Architecture of the proposed system

## 5.3 Methodology

### 5.3.1 Use Case Diagram

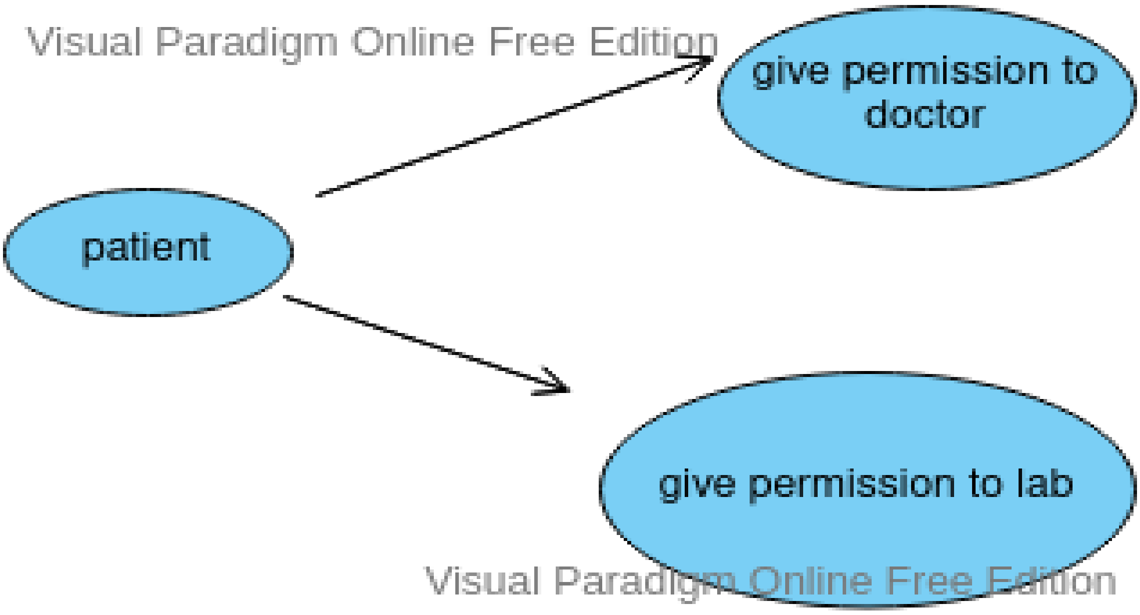


Figure 5.2: use case diagram of patient

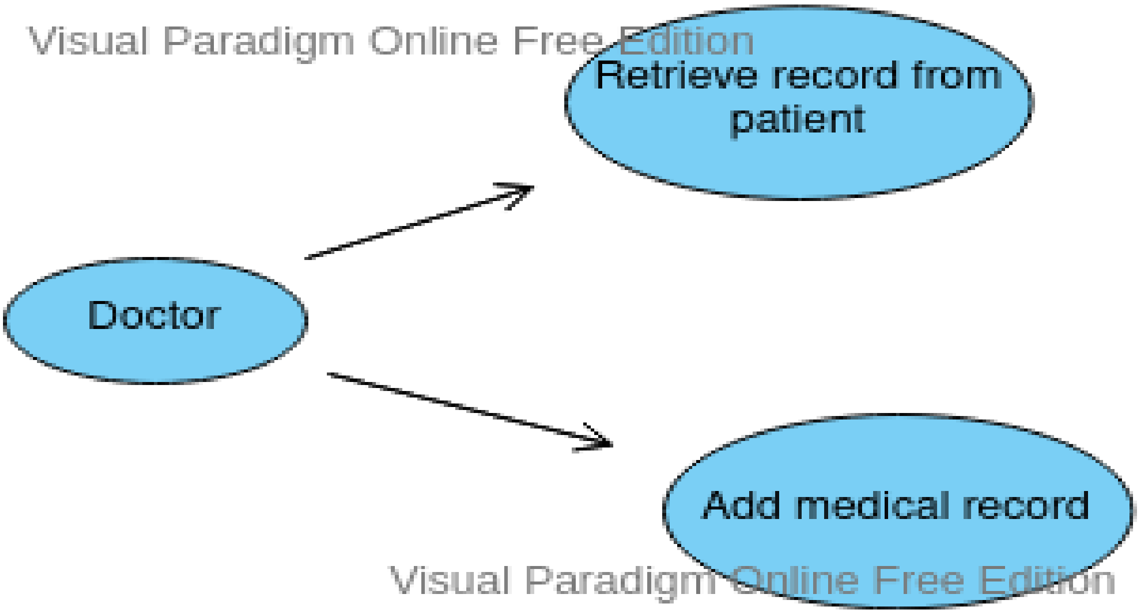


Figure 5.3: use case diagram of doctor

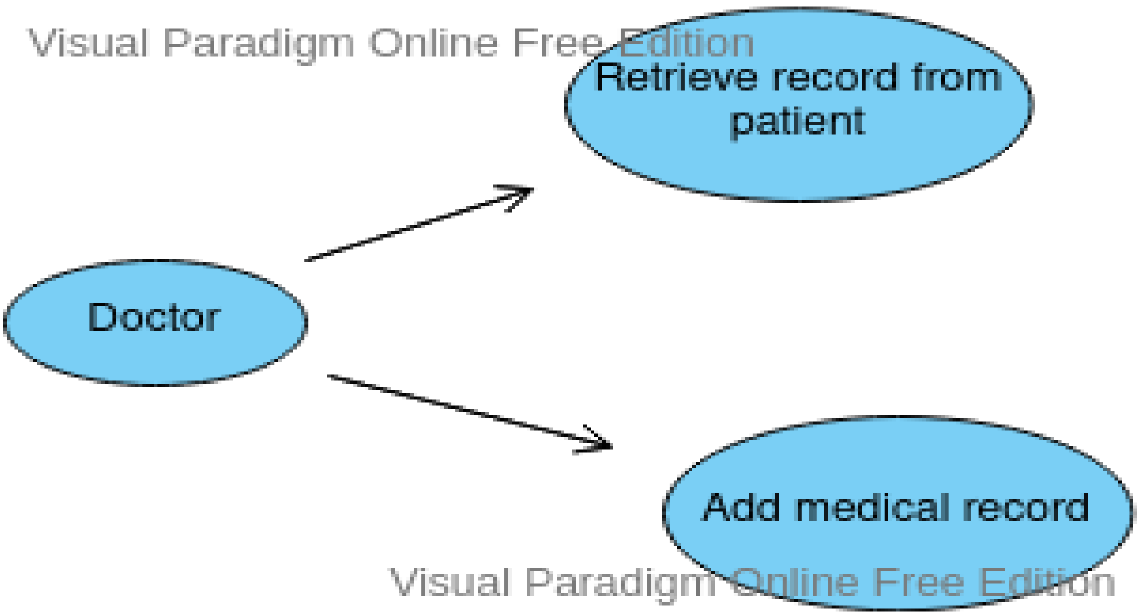


Figure 5.4: use case diagram of lab

## 5.4 Data Flow Diagram

DFD is a graphical representation approach that is used in a project to demonstrate the data flow through a project. DFD assists us in gaining an understanding of the input, output, and process involved.

The fundamental data flow of the programme is demonstrated at level 0. It does not go much further into the data flow. It will be examined at the Data Flow Diagram's higher levels.

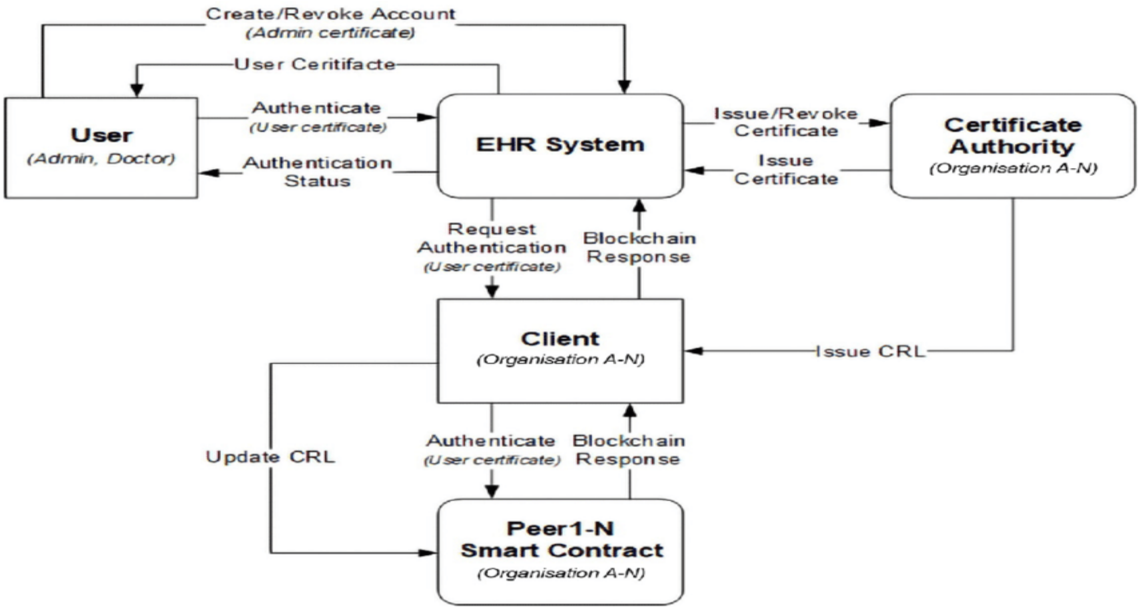


Figure 5.5: Level 0 DFD

## 5.5 Screenshots of user interface

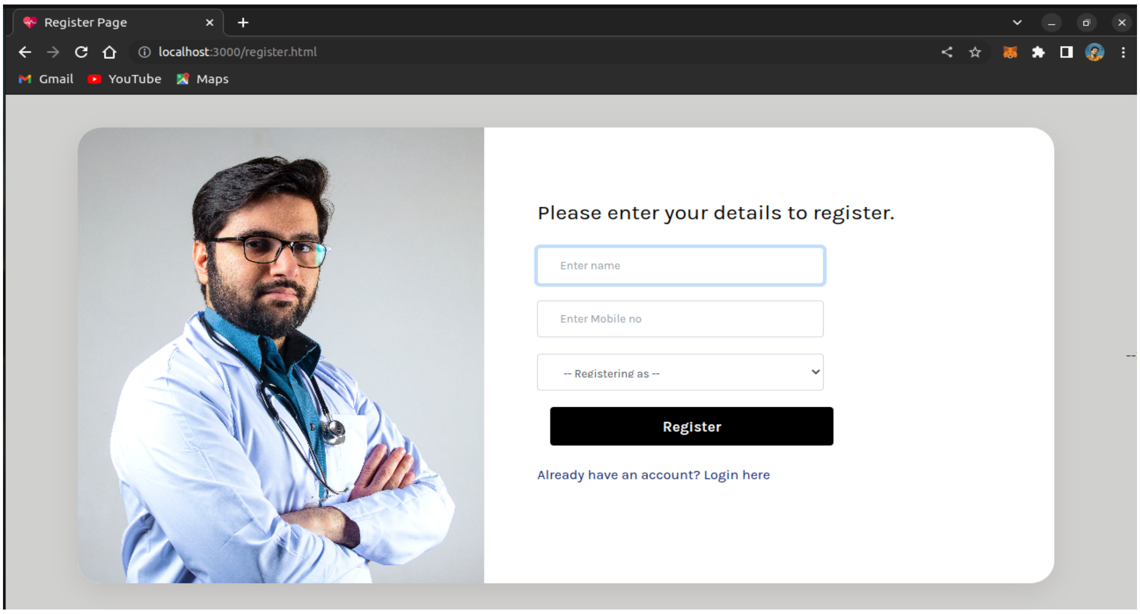


Figure 5.6: Registration

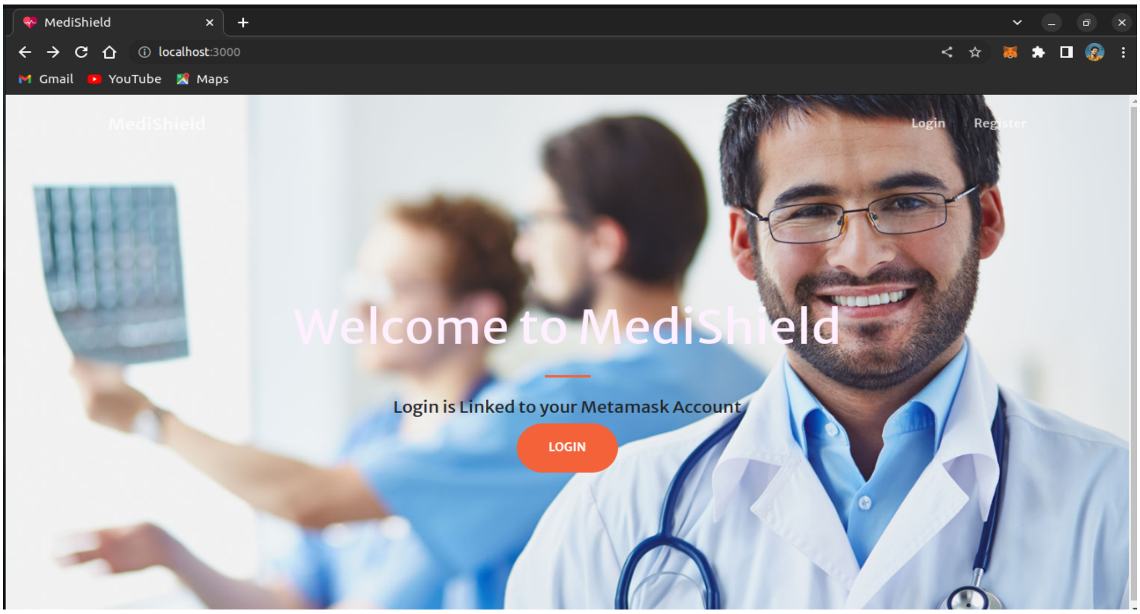


Figure 5.7: Login

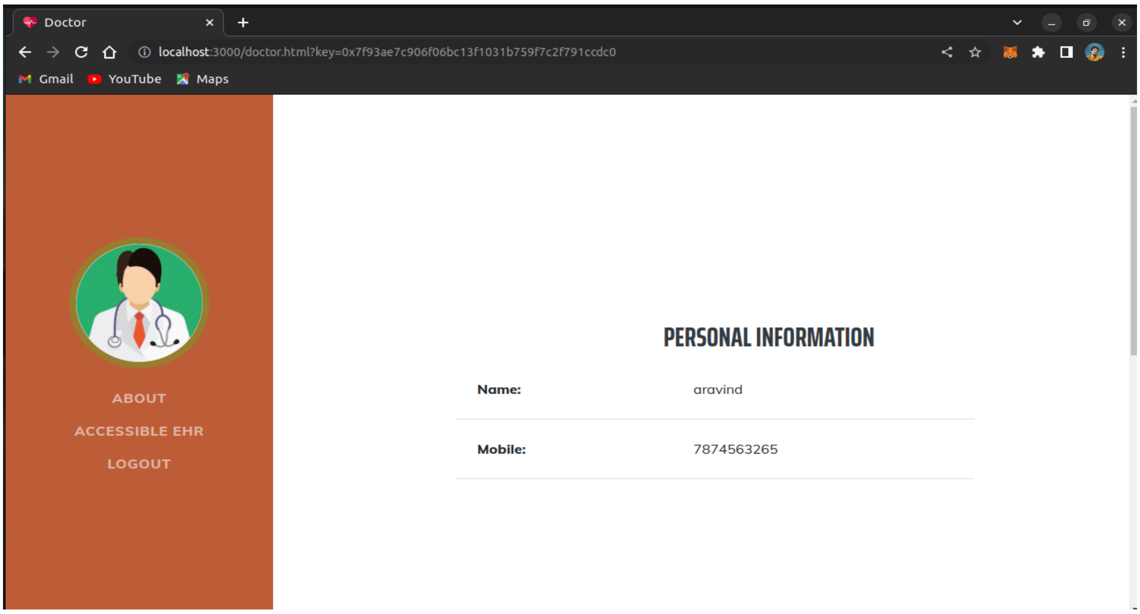


Figure 5.8: Doctor

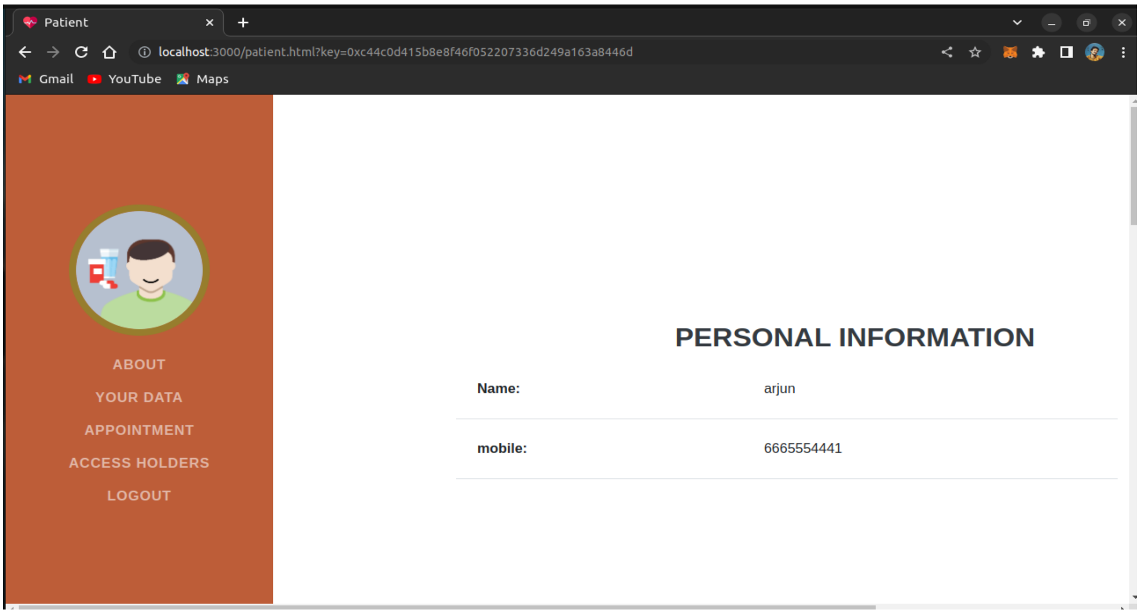


Figure 5.9: Patient

# Chapter 6

# Coding

**Algorithm 1** Proof-of-Work

Start.
Initialise index writer
Configure the analyser for the index writer
Initialise a matrix M for bitmap index
for each EHR do
Breakdown the text field into tokens
Extract and index the token
Attach keyword w to the matrix row
Attach file hash hj to the matrix column
if wi  EHRj then
cell cij in M = 1
else cell cij in M = 0
return M
Stop.

Next, Algorithm 1 initialises a two-dimensional array as a matrix for storing the information about the EHR's index. The encrypted keywords are attached to the first column of the matrix; while the hash value of the EHR returned by the Interplanetary File System (IPFS) storage is attached to the column of the matrix, representing the column identifier. Lastly, the algorithm will check the presence of each keyword in the particular EHR and fill the cells with "1" if the keyword is present in the file;otherwise, it will remain "0".

# Chapter 7

# Testing and Implementation

## 7.1 Testing and various types of testing used.

System testing is the step of implementation that ensures the system functions correctly and efficiently before it goes live. Testing is the process of running a program to look for mistakes and missing operations, as well as comprehensive verification to see whether the goals are reached and the user requirements are met.

A test plan is carried out on each module, using comprehensive testing methodologies. The unit, integration, and system testing approaches are all defined in the test plan. The following items are covered by the test: One of the key goals of application testing is to ensure that the system fulfils all functional and quality criteria (Non-functional requirements).

The user should find that the project has met or surpassed all of their criteria at the end of the project development cycle. Any modifications, additions, or deletions to the requirements document, functional specification, or design specification shall be documented and tested to the greatest quality possible given the project's remaining time frame and the test team's capabilities. The secondary goal of application system testing is to find and disclose any flaws and hazards, and to ensure that all known issues are fixed before release.

### 7.1.1 Unit Testing

| SLNO | PROCEDURE | EXPECTED RESULT | ACTUAL RESULT | PASS OR FAIL |
|---|---|---|---|---|
| 1 | Adding a patient | patient gets added and block gets created | Same as expected | pass |
| 4 | Addding o doctor | doctor gets added and block gets created | Same as expected | pass |
| 5 | output shown to user from blocks | searched data seen | Same as expected | pass |

Table 7.1: Unit test cases and results

### 7.1.2 Integration Testing

| SLNO | PROCEDURE | EXPECTED RESULT | ACTUAL RESULT | PASS OR FAIL |
|---|---|---|---|---|
| 1 | Record added | Block created | Same as expected | pass |
| 2 | Patients are able to update block | Blocks updated | Same as expected | pass |
| 3 | When record is searched | Output is seen by the user | Same as expected | pass |

Table 7.2: Integration cases and result

### 7.1.3 System Testing

| SLNO | PROCEDURE | EXPECTED RESULT | ACTUAL RESULT | PASS OR FAIL |
|---|---|---|---|---|
| 1 | Deploy contract | Contract Deployed on Blockchain | Same as expected | pass |
| 2 | Updating blocks | Block gets mined | Same as expected | pass |
| 3 | Data retrieved from blocks | output is obtained | Same as expected | pass |

Table 7.3: System test cases and results

# Chapter 8

# Results and Discussion

Based on the search results,the adoption of blockchain technology in the healthcare systems and challenges to EHR implementation of blockchain was analysed. From the synthesized research, the work was categorized and reported compelling factors of blockchain for EHR integration using current knowledge on blockchain research standardization and architectural challenges.

## 8.1 Advantages and Limitations

In the healthcare sector, transparent and immutable record-keeping transactions can also be important, such as purchase and shipping transactions in the supply chains of medical equipment and pharmaceuticals; as well as the tracking of permits and staff access to facilities, medical records, or other health data.

### 8.1.1 Advantages

- Better Health Records Exchange
- Increase Data Security and Privacy
- Validate the Correctness of Billing Management
- Empower the Medical Supply Chain

### 8.1.2 Limitations

There are several limitations of blockchain-based EHR solutions. Limitations include common standard, scalability in terms of storage, block creation time, data storage, user adaptation, and storing and maintaining EHR data costs. Most of the solutions are still in either a theoretical or prototype state. Blockchain technology is still in a developing state that lacks user-friendliness and has limitations regarding EHR privacy and security of EHR data. No solutions have been found to either delete fraud EHR data from the blockchain or for dead patients.

Besides, no acceptable solutions were found for the sce- nario where a patient is in a coma, unconscious, or illit- erate, and his EHRs need to be accessed by the doctors or physician. One possibility is that the patient has an ID card with a unique identification number, and the doctor can read the EHRs using it. Finally, aggregation of technolo- gies like ML, AI, and Edge Computing may help overcome problems like scalability, fraud EHRs detection, and many more

# Chapter 9

# Conclusion and Future Scope

This study answers the question of the current state of the art in blockchain-based EHR management research and future directions. We showed the distribution of blockchain types and platforms adopted by the reviewed articles. The potential benefits of blockchain to manage EHRs have met stakeholders' expectations in the healthcare sectors, while we also found that several challenges require further research. For instance, cross-border sharing of EHR data may be hampered by varying and often conflicting legislation. Besides, the privacy policies also vary based on the specific government regulation. Hence, further investigation on regulation, standardization, and cross-border accessibility of EHRs is crucial.

However, After thorough scrutiny of selected articles, we concluded that the most prominent blockchain platform for EHR management is Ethereum (private) and Hyperledger Fabric because these two platforms meet almost all the requirements. We also found that handling big EHR data on a large scale with blockchain has limitations such as limited storage capacity, computation cost, and communication cost. However, there are potential solutions to overcome these limitations, such as artificial intelligence, IoMT, and edge computing.

The study may serve as a reference for future research in this field. The accumulation of all related papers, their contributions, and limitations will help the potential researchers to design a new architecture or model. Moreover, future research directions to combine blockchain could help propose more exciting solutions for the existing problems.

# Bibliography


[1] H. Jin, Y. Luo, P. Li and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," in IEEE Access, vol. 7, pp. 61656-61669, 2019,doi:10.1109/ACCESS.2019.2916503

[2] 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), Vienna, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11

[3] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data", Proc. Norwegian Inf. Secur. Conf., pp. 1-12, 2017

[4] Q. Xia, E. B. 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, pp. 44, 2017

[5] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", IEEE Access, vol. 5, pp. 14757-14767, 2017

[6] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications", Proc. IEEE 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), pp. 1-5, Oct. 2017

[7] C. McFarlane, M. Beer, J. Brown and N. Prendergast, Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1, Addison, TX, USA:Entrust, 2017

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

[9] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," in IEEE Access, vol. 6, pp. 11676-11686, 2018, doi: 10.1109/ACCESS.2018.2801266

[10] W. Liu, Q. Yu, Z. Li, Z. Li, Y. Su and J. Zhou, "A Blockchain-Based System for Anti-Fraud of Healthcare Insurance," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1264-1268, doi: