TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

PULCHOWK CAMPUS

A

PROJECT REPORT

ON

ELECTRONIC MEDICAL RECORD STORAGE AND MANAGEMENT SYSTEM USING BLOCKCHAIN

SUBMITTED BY:

PRABHAT KIRAN KABDAR (PUL075BCT059)

PRIYA THAKUR (075BCT062)

ROHAN KARKI (075BCT067)

SHREEM ARJYAL (075BCT084)

SUBMITTED TO:

DEPARTMENT OF ELECTRONICS & COMPUTER ENGINEERING

May, 2022

Page of Approval

TRIBHUVAN UNIVERSIY
INSTITUTE OF ENGINEERING
PULCHOWK CAMPUS
DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

The undersigned certifies that they have read and recommended to the Institute of Engineering for acceptance of a project report entitled **"ELECTRONIC MEDICAL RECORD STORAGE AND MANAGEMENT SYSTEM USING BLOCKCHAIN"** submitted by **Prabhat Kiran Kabdar**, **Priya Thakur**, **Rohan Karki**, **Shreem Arjyal** in partial fulfillment of the requirements for the Bachelor's degree in Electronics & Computer Engineering.

.....
Supervisor
Anand Kumar Sah
Assistant Professor
Department of Electronics and Computer Engineering,
Pulchowk Campus, IOE, TU.

.....
Internal examiner
Assistant Professor
Department of Electronics and Computer Engineering,
Pulchowk Campus, IOE, TU.

.....
External examiner
"Mr. Deeepen Chapagain"
LogPoint
deepen.chapagain@logpoint.comg,

Date of approval:

Copyright

Acknowledgments

This project is now in its completed state as a result of the coordinated efforts of numerous people and organizations. The following people have contributed significantly, and we would like to sincerely thank them: First and foremost, we would like to express our sincere gratitude and debt of gratitude to Prof. Anand Kumar Shah, who served as our supervisor, for his essential encouragement, advice, and support beginning at the early stages of our project and for giving me wonderful experiences throughout the process. Above all, his invaluable and rigorous oversight at every stage of the job encouraged us in countless ways.

We would especially want to thank him for his guidance, oversight, and crucial assistance during this project when needed. His interest in creativity has sparked and fostered our intellectual development, which will be useful to us for a very long time. We are honored to say that we got the chance to collaborate with a professor with such a wealth of knowledge. We are also appreciative to our teachers who provided insightful criticism and recommendations that significantly raised the project's level of quality. Their assistance was crucial in ensuring that the project met the strict criteria established by the organization.

We also like to thank our students for their help with the project's technical aspects and for their support and cooperation. Their cooperation, effort, and dedication were essential to the project's success. They made a priceless and deeply valued contribution.In closing, we would want to thank everyone who helped this engineering project succeed by acknowledging their contributions, whether they were directly or indirectly involved. We would like to express our sincere appreciation to each and every one of them for their tremendous assistance and collaboration.

Abstract

Above all else, a person's health is the most important thing, so any personnel's medical records are unquestionably a very sensitive and priceless resource.If this knowledge is given to the wrong people, they may misuse it in unfathomable ways. The conventional form of paper file storage looks to be the most dangerous method of storage, although being used today. Additionally, computerized folder systems for storing records are not very trustworthy and may allow the relevant authority to abuse them. However, handling such data would have been made much simpler if the patient had been given complete control over who should have access to these sensitive information by cutting out the middleman. The blockchain concept is presented at this point since it has proven to be a great technology for decentralized data storage. Data security is best ensured by blockchain decentralized apps that link several entities, including as patients, doctors, and laboratories.

Keywords: *Healthcare, centralization, decentralization,Blockchain, data security*

Contents

List of Figures

List of Tables

List of Abbreviations

EHRs	Electronic Healthcare Records
P2P	Peer to peer
SCs	Smart Contract
IPFS	Inter Planetary File Service
JSON	JavaScript Object Notation
RPC	Remote Procedure Call
PHR	Personal health record
DNS	Domain Name Service
API	Application Program Interface
DPoS	Delegated Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
M2M	Machine to Machine
FPGA	Field programmable gate array
SHA	Secure Hash Algorithm
IoT	Internet of Things

1. Introduction

Several parties are involved in the medical record storage industry, including doctors, patients, labs, pharmacies, insurance companies, and researchers. Since sharing these sensitive and important details with anyone would be inappropriate. Modern digital storage methods are incredibly trustworthy, safe, and dependable since they only allow secure patient data to be submitted when necessary. Utilizing a blockchain limits data modification after a block is created. A user must also have authorization on the Blockchain network in order to access part of the data. As a result, blockchain technology is used in our project to store and manage electronic medical records in order to protect sensitive data.

1.1 Background

Traditional methods of storing diagnosis reports on manual paper files are quite laborious and not safe. Even though most health sectors now use digital systems, the relevant authorities still have to go through those drab-looking folders that hold a lot of documents relating to a single patient.The authority must sort the files in that specific folder using the oldest file first format and examine each file dating back to the patient's initial diagnosis report in order to learn about any patient's diagnosis history report. To think that this circumstance is too challenging and then attempt it every day can eventually result in mistakes. Additionally, related authorities occasionally misuse patient records for their own gain. As a result, Blockchain technology offers a practical answer to all of these issues by storing data in a decentralized manner with complete patient control.Decentralization, authenticity, immutability, and transparency are among Blockchain's key properties. Traditional methods manage medical data through a centralized authority, which leaves data vulnerable to destruction, corruption, obscurity, and exploitation through bribery of the person in charge. Records lack immutability and transparency, and therefore are not secure. When traditional approaches struggle to apply prerequisites on health care data, blockchain aims to restore confidence in contemporary medical records.

The management and storage of electronic medical records using blockchain technology is a viable method for strengthening the confidentiality and privacy of sensitive patient data. With blockchain, medical records can be kept in a distributed, decentralized database that cannot be changed without the agreement of all network members. This decreases the risk of unwanted access, data breaches, and data tampering and eliminates the requirement for a centralized authority to control and manage the data.

Patients can pick who can access their medical data and have full control over it by adopting a blockchain-based system. Only the information required by doctors, labs, pharmacies, and other organizations can be securely accessed, with the patient's proper authorization and consent. This facilitates quicker and more accurate research as well as more effective and precise diagnosis and treatment.A blockchain-based system can also increase accountability and transparency because every transaction and change is recorded and can be tracked back to its origin. This can enhance overall healthcare quality and outcomes while assisting in the prevention of fraud, mistakes, and misuse.Implementing a blockchain-based medical record system, however, necessitates careful consideration of a number of technological, legal, and ethical challenges, including data protection, confidentiality, permission, ownership, responsibility, interoperability, and others.The system must be developed and put into use in a way that satisfies the unique needs and specifications of many stakeholders while upholding the strictest privacy and security regulations.The manner that medical records are stored, handled, and exchanged could be completely changed by blockchain technology. Blockchain can improve healthcare results and give individuals more control over their personal health data by offering a transparent and secure platform for data exchange.

Greater security and privacy are two important advantages of using a blockchain-based system for EMR storage and management. Data breaches and hacker attacks are substantially less likely because there is no single point of failure or control because the data is stored in a decentralized database. Every transaction on the blockchain is also protected by encryption and authentication, guaranteeing that only people with the proper permissions can access the data.Greater transparency and accountability are two advantages of using blockchain technology for EMR storage and management. It is simple to spot any illegal alterations or questionable activity because every transaction on the blockchain is logged and can be tracked back to its source. As a result, fraud, mistakes, and abuse can be imrpoved overall healthcare quality and outcomes.

In conclusion, blockchain technology has the potential to revolutionize the way that medical records are maintained, exchanged, and stored by enhancing their security, privacy, accountability, and transparency. To make sure that a blockchain-based system for EMR storage and management is effective, efficient, and fair for all stakeholders, it is crucial to thoroughly analyze the technical, legal, and ethical problems involved.

1.2 Problem statements

The conventional record-keeping system's main flaws were its lack of security, dependability, and centralization of storage, all of which made it easy to alter data in a variety of ways. Although there are some platforms for cloud storage of medical records, they are not very

dependable. Security hazards, privacy concerns, accessibility issues, data fragmentation, and a lack of patient control are just a few issues that centralized medical record storage systems can bring about for patients and healthcare professionals. Blockchain-based decentralized solutions may provide a safer, more private, and more easily accessible option for managing and storing medical records.

The major problems associated can be listed below :

I.Security risks: Systems for centrally storing medical records are susceptible to security lapses and cyber-attacks, which may result in the theft or unauthorized access of sensitive patient data. This is due to the fact that all the data is kept in one place, making it a prime target for hackers and other bad guys.

II.Limited accessibility: Some healthcare professionals may not have access to centralized medical record storage systems, particularly those who practice in remote or rural areas or for various healthcare organizations. As centralized system requires the permission to be granted by the central authority rather than the patient. So, for the entities who aren't granted access by the central authority who records the medical data it may be problematic to access such medical data. This may result in treatment delays and a breakdown in provider coordination.

III.Data Fragmentation Patient information is frequently scattered among several systems and databases in centralized medical record storage systems. So, a patient records may be stored at different medical institutions databases rather than the single collective fashion. So, it may be hard to acquire the patient's medical data in the collective way as patient can be getting treatment from the several institutions. So, it makes challenging to distribute, record and access the patient's records across various healthcare providers.

IV.Lack of patient control Patients frequently have limited control over their own data when medical records are stored centrally. They could not have easy access to their medical records, or they might not be able to control who has access to their information and for what purposes. For an example, certain medical institutions may give access to any doctors, or any other entities without the consent of the patient. And patient may be unaware who have access for what purpose, for how much period and over which data.

1.3 Proposed Solution

A blockchain is a distributed, decentralized database that keeps information in blocks that are linked to one another in a chain, with each block having a hash of the one before it. This makes it nearly impossible to change any block without also changing all succeeding blocks and getting agreement from all network users.Medical records are managed and stored using this technology. On the blockchain, each medical record would be kept in its own block, which would also contain a timestamp and a distinct hash. Any modifications to the record would necessitate the creation of a new block, which would then be connected to the prior block to form a chain. Every medical transaction would have a permanent, unalterable record, thanks to this. This helps from the security risks posed by the central based system.

All the records of the patients are recorded collectively in the respective patient account. And the patient can access it anytime. And also any doctor or any other entity can access it as required without getting permission from any central authority and hence it has greater accessibility.

Since, all the records of the patient from any doctor or any medical institution is stored in the patient account. And all the records of the patient from the beginning is stored in the patient account the problem of the data fragmentation is solved. And all records of the patient from the beginning can be viewed easily.

In this system the patient decides whom to give access as well as revoke the access. Only that entity which get access can view the records or upload the records to the patient's account. Hence, the patient has full control over his/her records and account.

This can enhance the general quality and effectiveness of healthcare by preventing fraud, mistakes, and misuse.

1.4 Objectives

This blockchain-based decentralized storage platform was proposed in order to provide a platform for the storage and management of electronic medical records. This platform is more secure, dependable, and offers significant protection against data manipulation because it puts all power in the hands of the patient.
The major objectives of this project are :

I. A blockchain-based EMR system's better security of patient data is one of its main goals. Patient data can be kept in a decentralized, tamper-proof database using blockchain technology.

II. A blockchain-based EMR system's additional goal is to make medical records more accessible. Regardless of where they are situated, patients may readily exchange their medical information with healthcare professionals, which can raise the standard of treatment.

1.5 Scope

Long-term, this kind of technology may take the place of every other conventional method of information storage, improving data security. A blockchain-based EMR project's scope may be rather extensive because it is a decentralized system, covering a variety of topics like patient data administration, healthcare provider collaboration, patient privacy and consent, medical research, and health insurance and billing. The immutable, traceable, transparent, auditable, and secure storage of the medical records may be ensured by the decentralized architecture of blockchain.

2. Literature Review

2.1 Related work

Various scientists, researchers and authors have published articles Blockchain based electronic medical record management system and also EHR. MedRec [1] technology is built to provide decentralization, utilizing the properties of Blockchain technology. The patient centric API is designed to include interoperability for the aggregation of the databases. A cryptographic hash is used to ensure that the data is not manipulated. Smart contracts in the Ethereum network are used for data collection and access permission. Proof of identity, a DNS-like model, is used to connect a unique Ethereum address to a particular patient ID. A syncing algorithm enables the management of off-chain data sharing between the supplier and the patient's database. To prevent a common point of failure, MedRec depends on several participants. The system offers convenient access to immutable and robust medical information resources through care providers and services. However, the model does not have scalability and encryption over smarts contracts. MedBlock proposed a Blockchain-based data management framework that improves the hybrid-consensus platform to resolve network latency and high energy consumption problems where DPoS and PBFT are not sufficient. The consensus process functions like a committee voting, where one node is elected as the influencer to operate on behalf of several other nodes inside a network. To demonstrate strong and reliable identity, MedBlock incorporates symmetric cryptography with custom access control. The system enables quick data transfer to prevent network overload by executing several tasks in a single period for the patient. Compared to other methods, the Bread Crumb mechanism provides less access time and continuous data transfer at various intervals, which addresses the issue of exchanging information and data storage in broad networks. But EHRs are held in hospital servers, they lack the idea of Blockchain decentralization to prevent being exploited by malicious hackers. Peterson et al. [2] proposed a medical information sharing system that has a community based network design. This study suggested a framework where data can only be viewed on a given node if the community members accept and support the semantics. Ultimately, patient monitors the protected data exchange and their enforcement. But the biggest downside is the direct storage of personal data. SMEAD [3] is a modern healthcare model built for patients with diabetes in a safe end-to-end network. The suggested model involves three wearable tools (neckband, shoes, and wristband) to track the status of the patient and anticipate the condition. They also

introduced MEDIBOX (an auto-served and shared network) to act as a tool for patients to warn and recall. Using smart contracts, Blockchain provides encryption and access control of data to trusted parties. The proposed framework is built together with medication, IoT, wearable devices, and cloud storage. The use of public-key cryptography preserves the data authentication. Through protecting transactions, smart contracts are being used to resolve the privacy problem. This system focuses primarily on the constant supervision of patients and alerts people if something is unusual. However, the feature does not define security for the mobile application controlled by the number of parties concerned. Salahuddin et al. [4] proposed a Machine-to-Machine (M2M) data management framework by an innovative protocol-based beacon. The proposed architecture allows the use of IoT sensors based on Field-Programmable Gate Array (FPGA) for tracking medical data. Heterogeneous groups including authorities, retailers, staff, doctors, insurance providers, and hospitals may handle the deployed systems. Blockchain and IoT-based cloud gateway is used to restrict data manipulation, where data fusion, and decision fusion is applied. Conceicaoet al. addressed a solution regarding transparency and protection using Ethereum based smart contracts. The information is only held by the patient. Smart contracts monitor health transactions, store EHR, and store public-private key pairs of users. Wallets are used as a tool to accelerate the information search. Three categories of transactions are defined: New Record, Notification, and Request Access. If a user misplaced their private key, they will not be able to access their wallet anymore. Data is not maintained in a secured database so data recovery mechanisms would be a problem. Lee et al. [5] propose an intelligent service model for healthcare on top of data measurement and storage functionality provided by IoT health devices. To obtain data from personal health devices, an application level collaboration protocol is proposed in which receives bio-signals information from the IoT-enabled devices. Rajput et al.propose an IoT based architecture to obtain health-related data from sensors and upload it to the cloud database for sharing with clinicians. Zgheib et al. [6] present a new IoT architecture for healthcare applications with a focus on the principles of weak coupling and of semantic data exchange. Siyal et al. discuss the application of blockchain technology in medicine and healthcare domain. The article claims that blockchain technology has a potential to help in personalized, authentic, and secure healthcare by merging the entire real-time clinical data of a patient's health and presenting it in an up-to-date secure healthcare setup. However, they mentioned issues relating to data emanating from diverse sources and pointed out the interoperability issues between blockchains from various service providers.

2.2 Related theory

2.2.1 Blockchain Technology

In 2008, Satoshi Nakamoto first proposed the idea of Bitcoin cryptocurrency as a decentralized P2P public system. Blockchain technology has been the foundation behind Bitcoin that functions as a transactional ledger. Blockchain technology is a digital innovation that has the potential to significantly impact trusted computing activists. Blockchain provides transparency. The features of the Blockchain technology attracted many researchers to explore the architecture and find out potential use cases. The diversity of Blockchain technology in the application domain has faced rapid growth. The type of application is not restricted to financial transactions only. Blockchain is a linked list that is distributed, consistently maintained by consensus, cryptographically linked, and cryptographically assures the integrity of data [20]. A linked list is a set of blocks that are connected by some link. In Blockchain for linking the tamper-resistant blocks cryptographic hashing is used. So, it is called hash linking. Blockchain commonly uses the Secure Hash Algorithm (SHA) 256 for hash linking.

Blockchain works by using cryptography to secure transactions and create an unalterable record of them. Each block in the chain contains a unique digital signature, or hash, that links it to the previous block, creating an unbroken chain of data. This makes it virtually impossible to tamper with the data or alter it in any way, as doing so would require changing all subsequent blocks in the chain

The technology behind blockchain is based on cryptography, which is the practice of using mathematical algorithms to secure communications and data. A blockchain is a decentralized, distributed database that is used to record transactions securely and transparently. It consists of a series of blocks that are linked together in a chain, with each block containing a unique digital signature, or hash, that links it to the previous block. This creates an unbroken chain of data that is virtually tamper-proof, as altering any block in the chain would require changing all subsequent blocks as well.

There are two types of blockchain technology: public and private. Public blockchains, such as the Bitcoin blockchain, are open to anyone and are used to record transactions that anyone can see. Private blockchains, on the other hand, are restricted to a specific group of users and are used to record transactions that are not visible to the public.

One of the most notable applications of blockchain technology is cryptocurrency. Cryptocurrencies like Bitcoin and Ethereum use blockchain to create a decentralized digital currency that can be sent and received without the need for a centralized intermediary, such as a bank. Transactions are recorded on the blockchain and verified by a network of users, making the system secure and transparent.Blockchain technology has many other potential appli-

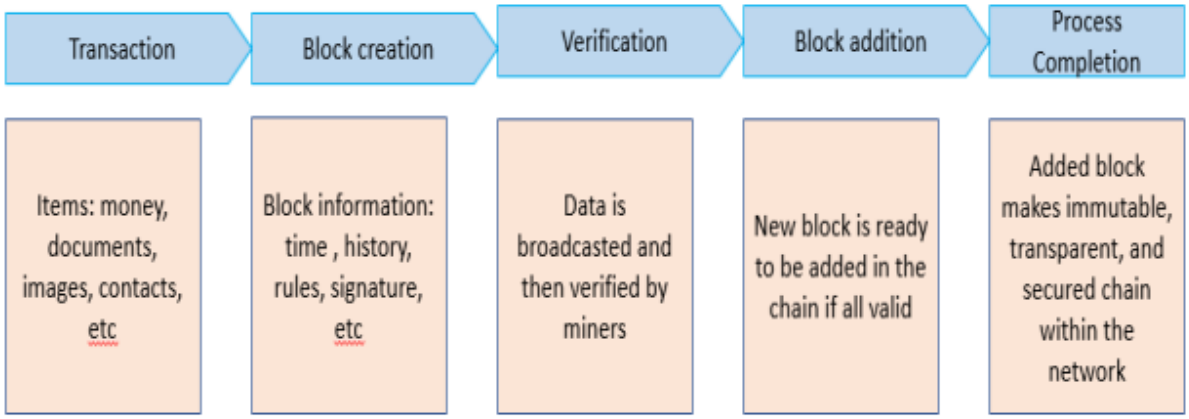

Figure 2.1: Basic working principle of Blockchain

cations beyond cryptocurrency. For example, it can be used to create secure supply chain networks, track the ownership and transfer of assets, and facilitate secure voting systems. The potential uses of blockchain are virtually limitless, and as the technology continues to evolve, it is likely to become an increasingly important tool for businesses and organizations around the world.

2.2.2 Blockchain Consensus Algorithms

The idea of consensus was formulated based on the Byzantine general problem. Byzantine generals commanded an empire over a single town during the battle. The Byzantine General Problem appears when certain generals must decide to launch an assault or not. Blockchain introduced distributed consensus algorithms to improve data accuracy and durability [20]. A consensus algorithm is a mechanism where all peers agree on a common state of the distributed ledger. The consistency of the data is maintained by mining (nodes validating transactions and creating blocks) after having the consensus. The consensus means that most of the peers agree on the data that is going in the block. The consensus protocols widely used are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), PBFT, Ripple, etc.

A consensus algorithm is a set of rules that govern how transactions are validated and added to a blockchain. There are several different consensus algorithms used in blockchain technology, each with its own strengths and weaknesses. Here are some of the most common consensus algorithms:

I.Proof of Work (PoW): This is the consensus algorithm used by Bitcoin and many other cryptocurrencies. In PoW, miners compete to solve complex mathematical problems, with

the first miner to find a solution being rewarded with a new block and the associated transaction fees. This algorithm is resource-intensive and can consume a lot of energy, but it is considered to be very secure.

II.Proof of Stake (PoS): In this algorithm, validators are selected to validate transactions based on the amount of cryptocurrency they hold. Validators are chosen at random, and the more cryptocurrency they hold, the more likely they are to be chosen. This algorithm is less resource-intensive than PoW, but some argue that it is less secure.

III.Delegated Proof of Stake (DPoS): This algorithm is similar to PoS, but instead of validators being chosen at random, they are voted in by the community. The community elects a group of delegates who are responsible for validating transactions on the blockchain. This algorithm is faster than PoW and PoS, but some argue that it is more centralized.

IV.Byzantine Fault Tolerance (BFT): This algorithm is designed for use in permissioned blockchains, where the nodes on the network are known and trusted. In BFT, a group of nodes is selected to validate transactions, and they must come to a consensus before the transaction can be added to the blockchain. This algorithm is considered to be very secure, but it is less decentralized than PoW or PoS.

2.2.3 Features of Blockchain

Blockchain is a less complex approach for encrypting ledger-based transactions across networks. The technology interacts with hosts having various processing capabilities. Ranging from a few to several network nodes, the technology has incredibly efficient computation speed. Figure 3 defines the fundamental operating stages of a Blockchain. First, people perform a transaction or share a query. A network of nodes affiliated with certain roles, validates the transactions. After successful hashing and agreement for the consensus algorithm 5 from each group concerned, a single block is officially announced. The block is eventually added to the current Blockchain.

Blockchain includes multiple techniques and have some properties like:

a) Integrity: Integrity of the data is maintained because of the cryptographic hash link.
b) Immutable: Tamper-proof log of data with limited access.
c) Distributed: Blockchain is a distributed system with replicated copies, in contrast to

the traditional systems for data management which requires records to be updated on the central server.

d) Authenticity: Complete information including data history can be searched on the decentralized network only if the user is authenticated.

e) Cryptographically hashed: Uses hash (SHA 256) linking. Hash algorithms provide functions like one-way cryptography, faster deterministic calculation, avalanche effect, and collision resistance. There is a public-private key pair under which the private key used for block signature and the public key is used to test the signature's validity.

f) Smart contracts: The codes are time-framed and generated on a distributed ledger framework where all the entities are required to follow the same set of rules. Mining: Miners use nonce in the blocks to calculate desired hash-values. This requires a high speed of calculation (and computational power) to obtain the reward for block mining.

g) Consensus: The consistency of the connected ledger is maintained through this mechanism. Every party should go through some stages of verification under the thumb rule of certain protocols. This is the backbone of the algorithm for making the technology secure.

g) Decentralization: One of the key features of blockchain technology is its decentralized nature. Instead of being controlled by a central authority, a blockchain network is maintained by a distributed group of users.

h) Interoperability: Blockchain technology can be used across different systems and networks, making it an ideal tool for creating interoperable systems and improving data sharing between different organizations.

These properties make blockchain technology a powerful tool for a wide range of applications, from cryptocurrency to supply chain management to voting systems and beyond. As the technology continues to evolve, it is likely that we will see many new and innovative uses for blockchain in the years to come.

2.2.4 Classification of Blockchain

The deployment of blockchain can be public or private.Everyone can participate in a public Blockchain i.e.available to all. Participants in private blockchain are known to each other. Bitcoin is the most famous example of public Blockchain. The private blockchain network operates by limiting the membership. An example of a private blockchain would be grant licences to a registrar for network participation. Consortium (or federated) Blockchain is a sort of network where the infrastructure is operated by several organizations. In Table 2.2.4, a short Blockchain classification has been presented for better understanding.

Public Blockchain	Private Blockchain	Consortium Blockchain
Public	Private	Public or Private
Decentralized	Partially decentralized	Almost centralized
High security	Medium security	medium security
High cost	Medium cost	Low cost
Anonymous user identity	Identified user	Identified user
Eg: Ethereum, bitcoin	Eg: company internal	Eg: Hyperledger

Table 2.1: **Types of Blockchain**

2.2.5 Blockchain as Database

A blockchain is a distributed database that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format.The innovation with a blockchain is that it guarantees the fidelity and security of a record of data and generates trust without the need for a trusted third party. A blockchain collects information together in groups, known as blocks, that hold sets of information. Blocks have certain storage capacities and, when filled, are closed and linked to the previously filled block, forming a chain of data known as the blockchain.

Firstly, blockchain is a distributed database, meaning that it is not controlled by any central authority or organization. Instead, the data is stored across a network of nodes, each of which has a copy of the ledger. Secondly, blockchain databases are immutable, meaning that once data is added to the ledger, it cannot be changed or deleted. This is because the data is stored in blocks, which are linked together in a chain using cryptographic algorithms. Each block contains a hash of the previous block, creating a continuous and unbroken chain of data. This immutability makes the blockchain ideal for use cases where data integrity is paramount, such as financial transactions, supply chain management, and voting systems.Finally, blockchain databases use consensus algorithms to validate transactions and maintain the integrity of the ledger. In a traditional database, transactions are validated by a central authority, such as a bank or government agency. In a blockchain database, however, transactions are validated by a network of nodes, each of which must agree on the validity of the transaction before it is added to the ledger. This consensus mechanism makes the blockchain more secure and trustworthy, as it is not subject to the whims of any one central authority.

2.2.6 Blockchain as decentralized network

What a blockchain does is to allow the data held in that database to be spread out among several network nodes at various locations. This not only creates redundancy but also maintains the fidelity of the data stored there. If somebody tries to alter a record at one instance of the database, the other nodes would not be altered and thus would prevent a bad actor from doing so.Blockchain is often referred to as a decentralized network because it operates without a central authority or middleman. Instead, it is composed of a network of nodes, each of which has a copy of the ledger and participates in validating transactions.

In a traditional centralized network, such as a bank, all transactions are processed and validated by a single authority. This can lead to issues such as censorship, single point of failure, and lack of transparency. In contrast, the decentralized nature of blockchain ensures that no single entity has control over the network, making it more secure and resistant to censorship and attacks.

Each node in a blockchain network has a copy of the entire ledger, ensuring that the data is always available and tamper-proof. Transactions are validated by consensus, meaning that a majority of nodes must agree on the validity of a transaction before it is added to the blockchain. This ensures that the ledger is accurate and transparent.Overall, the decentralized nature of blockchain allows for a more secure, transparent, and innovative network, free from the limitations of centralized authority.

2.2.7 Transparency in Blockchain

Because of the decentralized nature of blockchain, all transactions can be transparently viewed by either having a personal node or using blockchain explorers that allow anyone to see transactions occurring live. Each node has its own copy of the chain that gets updated as fresh blocks are confirmed and added.In a blockchain network, all transactions and data are publicly visible and recorded on the ledger, which is distributed across the network of nodes.This transparency ensures that anyone can view and verify the information stored on the blockchain, promoting trust and accountability.

Blockchain technology also allows for the creation of auditable records, which can be used to track the history of a particular asset or transaction. This is particularly useful in industries such as supply chain management, where transparency and traceability are important for ensuring the safety and quality of products.Overall, the transparency of blockchain technology provides a level of trust and accountability that is often lacking in traditional centralized systems. By allowing for public visibility and verifiability of data, blockchain promotes greater transparency and honesty in a wide range of applications and industries.

3. Methodology

3.1 Recognition of problem

Currently, available traditional method of medical record storage is not much efficient since it is centralized which may lead to data tampering and also the storage method either using paper file or let it be the digitized folder on the computer is quite tedious. And hence we addressed this problem through our application. Traditional method of storage of diagnosed report using manual paper file is really tedious and not secured way of storing data. Despite there are digitized system in most of the health sectors nowadays but still the related authorities have to go through those monotonous looking folders which contains large amount of files related to the single patient.To learn about any patient's diagnosis history report, the authority has to sort the files within that particular folder according to the oldest file first format and open each and every file since the patient's first diagnosis report. Also all the data of the patient may not be available in the single system or in single place. Or the medical records of the patient from the beginning may be fragmented or distributed at various places or institutions in the centralized based system rather than linked to the single account of the patient.

3.1.1 Functional Requirements

Functional requirements describe the functionality that the system must perform. These capture the intended behavior of the system. This software system requires the following functionalities:

1. Decentralized system
2. Signup for user
3. Login and entry for verified users
4. Limited time access for entities
5. Access authority by Patient

3.1.2 Non-Functional Requirements

The non-functional requirements of the project can be described as below :

a) Security: The EMR system shall be highly secure to protect patient data from unauthorized access, tampering, or loss. This could include measures such as data encryption,

access control, and backup and recovery procedures.

b) Scalability: The system shall be able to handle a large volume of data and users as it grows over time.

c) Performance: The system shall be fast and responsive, with minimal latency or downtime, to ensure that patient data can be accessed and updated quickly and reliably.

d) Interoperability: The system shall be able to integrate with other healthcare systems and technologies, such as electronic health records (EHRs) and medical devices, to ensure seamless data exchange and interoperability.

e) Compliance: The system shall comply with relevant legal and regulatory requirements, such as data privacy and security regulations, as well as industry standards and best practices.

f) Usability: The system shall be easy to use and navigate for healthcare professionals, patients, and other stakeholders, with a user-friendly interface and clear instructions for data input and retrieval.

g) Reliability: The system shall be reliable and available at all times, with a high level of uptime and minimal system failures or errors.

3.2 Proof of concept

Proof here refers to determining the feasibility of our idea and verify that the idea will function as envisioned. Since platforms for electronically storing medical records are already in the market, and our project is somehow based on the similar idea, hence this proves the idea to be feasible. Also the blockchain based app are rising along with the trend of cryptocurrency as it is decentralized and secured. And also we were already familiar with the tools and programming needed, and had done research on the relevant concepts. The further research in this project aspects helped us consider the relevance of the concept and prove its feasibility.

3.3 Selection of Blockchain

Since it is not feasible to start a blockchain from scratch due to time limitations, we decided to build our application over the most popular blockchain for Dapps, Ethereum. Since Ethereum is the blockchain with many resources and researches in place, it was a great help for us. Ethereum is a decentralized, open-source blockchain platform that enables the creation of decentralized applications (dApps) and smart contracts. It was first proposed in 2013 by a programmer named Vitalik Buterin and launched in 2015.The Ethereum network is powered by its native cryptocurrency, Ether (ETH), which is used to pay for transaction fees and incentivize network participants. Ethereum uses a proof-of-work (PoW) consensus

algorithm, similar to Bitcoin, but has plans to transition to a proof-of-stake (PoS) algorithm in the future, which would be more energy-efficient.

Ethereum's open-source nature has led to the development of a vibrant ecosystem of developers and dApp creators, with thousands of decentralized applications built on the platform. Ethereum also supports the creation of new tokens and cryptocurrencies through its ERC-20 token standard, which has enabled the creation of many new blockchain-based assets.Overall, Ethereum is a powerful and innovative blockchain platform that has enabled the creation of many groundbreaking applications and use cases, and continues to evolve and improve over time.

3.4 Smart Contract Development

The real development of our application started with the designing the smart contract in Solidity. It is the most important part of the Dapps. We designed it considering all the possibility of failure and with the exception handling in such a way that it avoids gas costly pattern.Smart contracts are computer programs that execute automatically when certain conditions are met. They are self-executing, meaning that they don't require human intervention to carry out their intended functions. Smart contracts can be used for a variety of purposes, such as financial transactions, supply chain management, voting systems, and more.Smart contracts are written using programming languages such as Solidity (used for Ethereum), and typically contain a set of rules and conditions that define the terms of an agreement.

So, we wrote the function in the Solidity for our app. The contract consists of the functions like registering the entities like patient, doctor etc and recording their data in the blockchain. Also the Login function to authenticate the users with their public key and data stored during the register process. Similarly, the records patient function helps to store the records of the patient by the certain entity to whom the access is given. And there is also the function to view the records of the patient by the entity. Also the revoke access function is there to ensure the patient can revoke the access of the entity at any time as per requirement.

All these functions are implemented in the smart contract and the functions are implemented only when the certain conditions are met.

Once a smart contract is deployed on a blockchain network, it becomes part of the network's permanent ledger, and can be executed automatically whenever the specified conditions are met. One of the key benefits of smart contracts is that they enable trustless transactions, meaning that parties can interact with each other without the need for intermediaries or trusted third parties. This can significantly reduce transaction costs and

increase efficiency, while also increasing transparency and reducing the risk of fraud.

3.5 Frontend development

The frontend development phase started simultaneously with smart contract development. It involved designing the easy and user-friendly user interface. We used React as it helps to build a rich user interface, is easy to maintain and is flexible due to its modular structure.

The specific requirements of the user interface, such as the layout, navigation, forms, and data visualization were determined.The necessary tools and dependencies for React.js development, such as Node.js, npm, and a code editor were installed and configured.The project structure, including the directory structure and configuration files was setup. React.js was used to develop the user interface components, such as forms, tables, charts, and menus and user interactivity.Use of state management library, such as Redux , to manage the application state and ensured that the user interface components are updated in response to changes in the state.

While developing the frontend we first developed the base UI which is the home page showing the logo of medical storage, login and register options for the various entities. So, they can choose the options from there to register or to login into their account.

Similarly the account page for each of the entity were build where they can see their details, see records of patient after putting the public address of the patient. And can upload the records into the specific patient address. On the other hand the patient account consists of viewing records of the patient, as well as granting and revoking access to the specific entity by putting the address of the patient.

We used the ethers.js to connect to the smart contract on the blockchain network and retrieve data from it.

3.6 Integration:web3.js

Using an Ethereum Blockchain is complicated but ethers.js, a decentralized library of node.js,comes as a saviour to integrate the frontend and the smart contract. After the complete development of frontend and smart contract, the integration part included a call to the functions of smart contract through web app. That is provided by ethers.js through JSON RPC protocol.

First, ethers.js was installed in the project.An instance of the ethers class was created and connected to the Ethereum network using the ethers constructor.The URL of the network that the smart contract is deployed on was specified and in our case it was deployed on a local network Ganache.In order to interact with the smart contract,we need to retrieve its ABI (Application Binary Interface) and its address. The ABI is a JSON file that describes the functions and variables of the smart contract, while the address is the unique identifier

of the contract on the Ethereum network.Once we have the smart contract instance, we can call its functions using the contract.methods property. We pass arguments to the functions and specify the gas price and gas limit for the transaction.

Finally, we integrated the smart contract functions with the user interface components, such as buttons, forms, and input fields. We used event listeners and callbacks to handle user actions and trigger the smart contract functions.

So, the functions we wrote in the smart contract were called using the ethers.js to execute using the frontend UI. Where specific user can call the functions using their address. Like patient can call the access or revoke function of the smart contract using the UI which will be executed for that particular patient's address.

4. System design

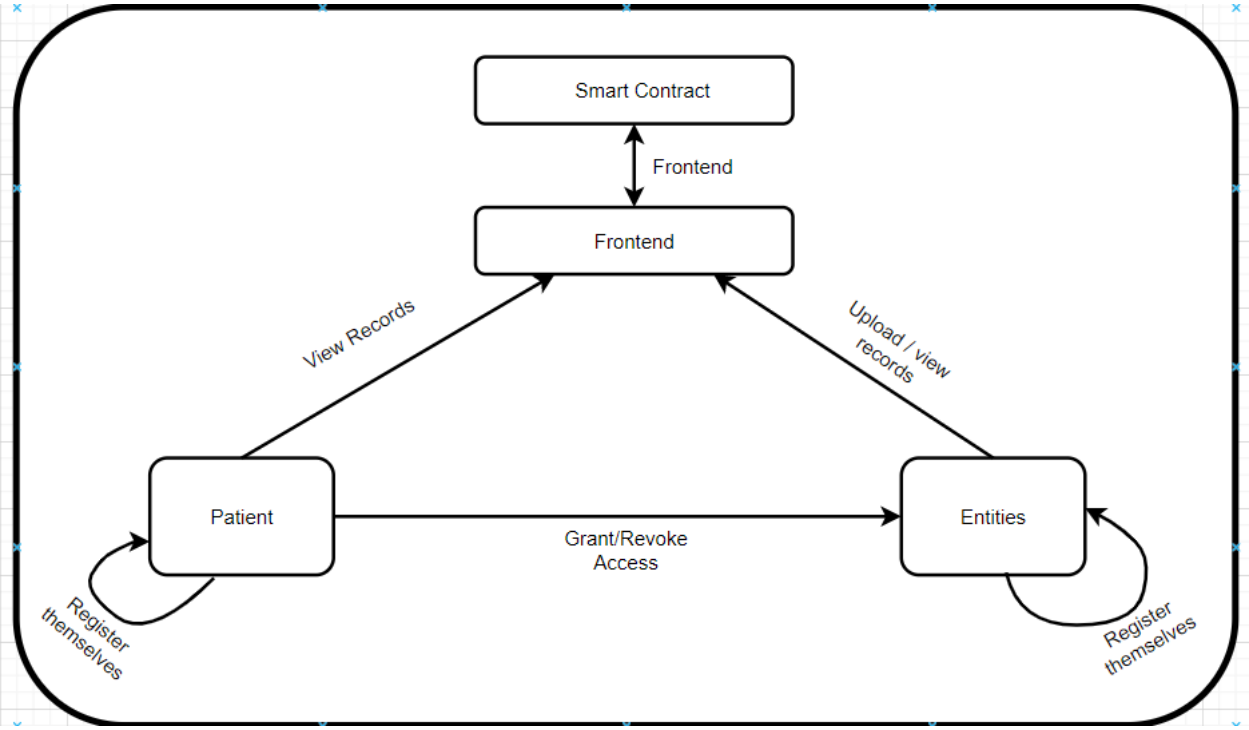

Figure 4.1: System Design

4.1 Description of Working principle

The system workflow involves various steps as follows:-

A. Patient has all the right handling the accesses regarding the whole system .Patient first registers themselves into the system and then decides whom the access can be granted and whom not. Decides on whether the entity trying to get access is registered or not. Patient also decides to revoke the access after the entity is done with the usage of the records.

B.The entities connected in the system queries the available medical record files. Once the entity registers themselves through this application and needs to log into the system for accessing the system utilizations and the patient authorizes them through their available etheruem-address .Entities involved here are doctor, laboratory, pharmacy, researchers and insurance company.

C. After the entities gets authorization , the entities can further access data and also upload record depending upon the conditions occurred. (Generally , uploading is done by entities only). Once the entities get registered , they log in in to the system. Each and every entities have their own ethereum addresses which they need to connect to prior any register or login.

D. For any entities to access the records , first the patient need to grant access to particular entity using its ethereum address. Once the access is granted , only then the particular entity can access any records of the patient who granted access to.

E. In the entity dashboard, we can their see details , upload records and access records . If any entity tries to access record without having permission to their request is discarded.

F. In the patient dashboard, we can see their details, access record that has been uploaded by all the entities and grant revoke accesses.

4.2 Use Case Diagram

The interactions between a system and its external actors or users are modeled and visualized using use case diagrams, a form of UML diagram. It demonstrates the various use cases the system is capable of carrying out and how these use cases relate to the actors involved.
The actors are shown as stick figures in a use case diagram, while the use cases are shown as ovals. The relationships between the actors and the use cases are depicted by the lines. For instance, a user might utilize the system to carry out a particular use case, such logging in, looking for information, or placing an order.
Use case diagrams can be employed to explain a system's requirements and functioning. The use case diagram offers a high-level overview of the system's behavior and aids in capturing the functional needs of the system. Additionally, it can be used as a communication tool between various stakeholders, including developers, testers, and business analysts, and to help identify any gaps or ambiguities in the requirements.

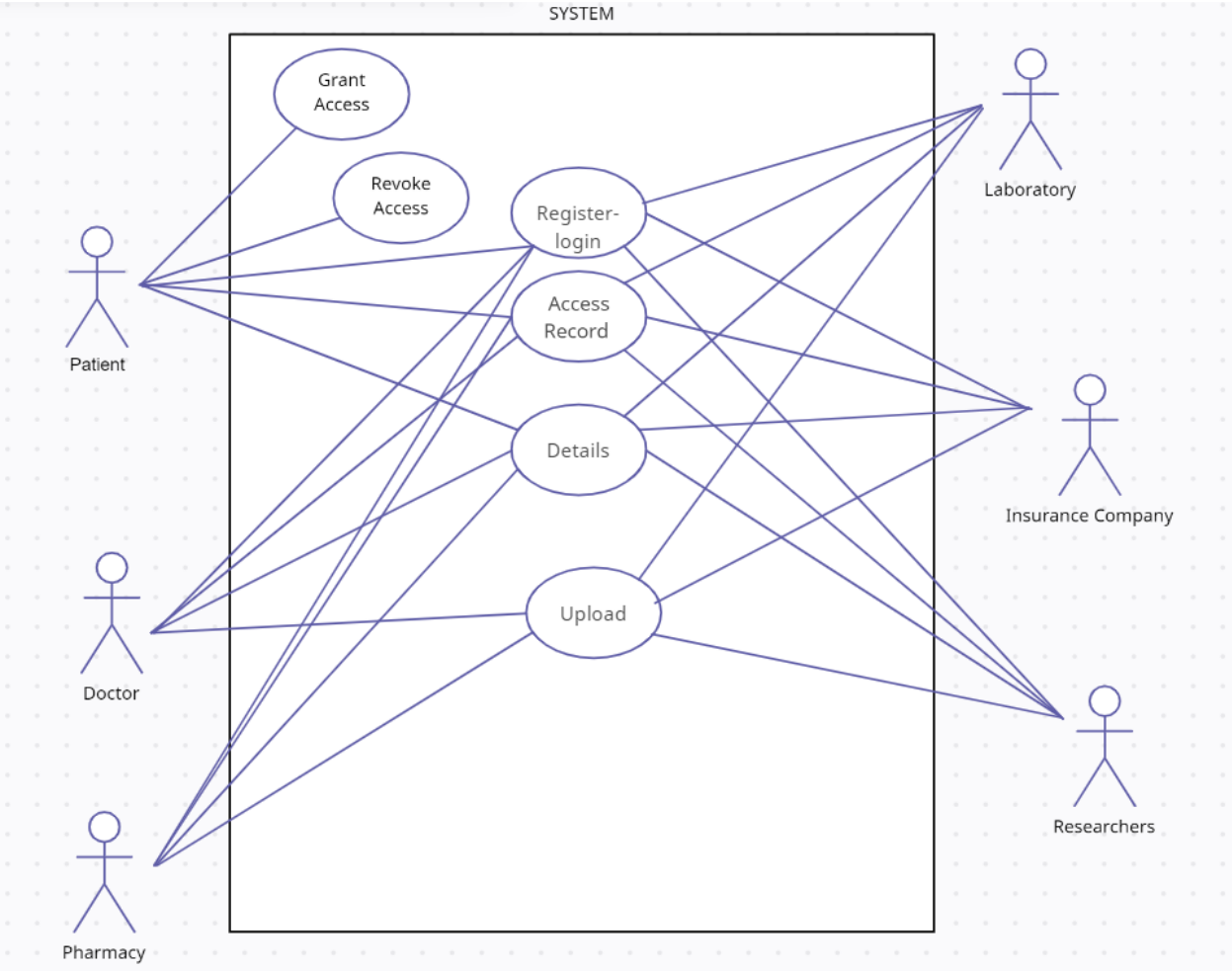

Figure 4.2: Use Case Diagram

4.3 Activity Diagram

A UML behavior diagram that illustrates a system's logic is called an activity diagram. Instead of focusing on the actual implementation, try to picture how the system's controls flow.

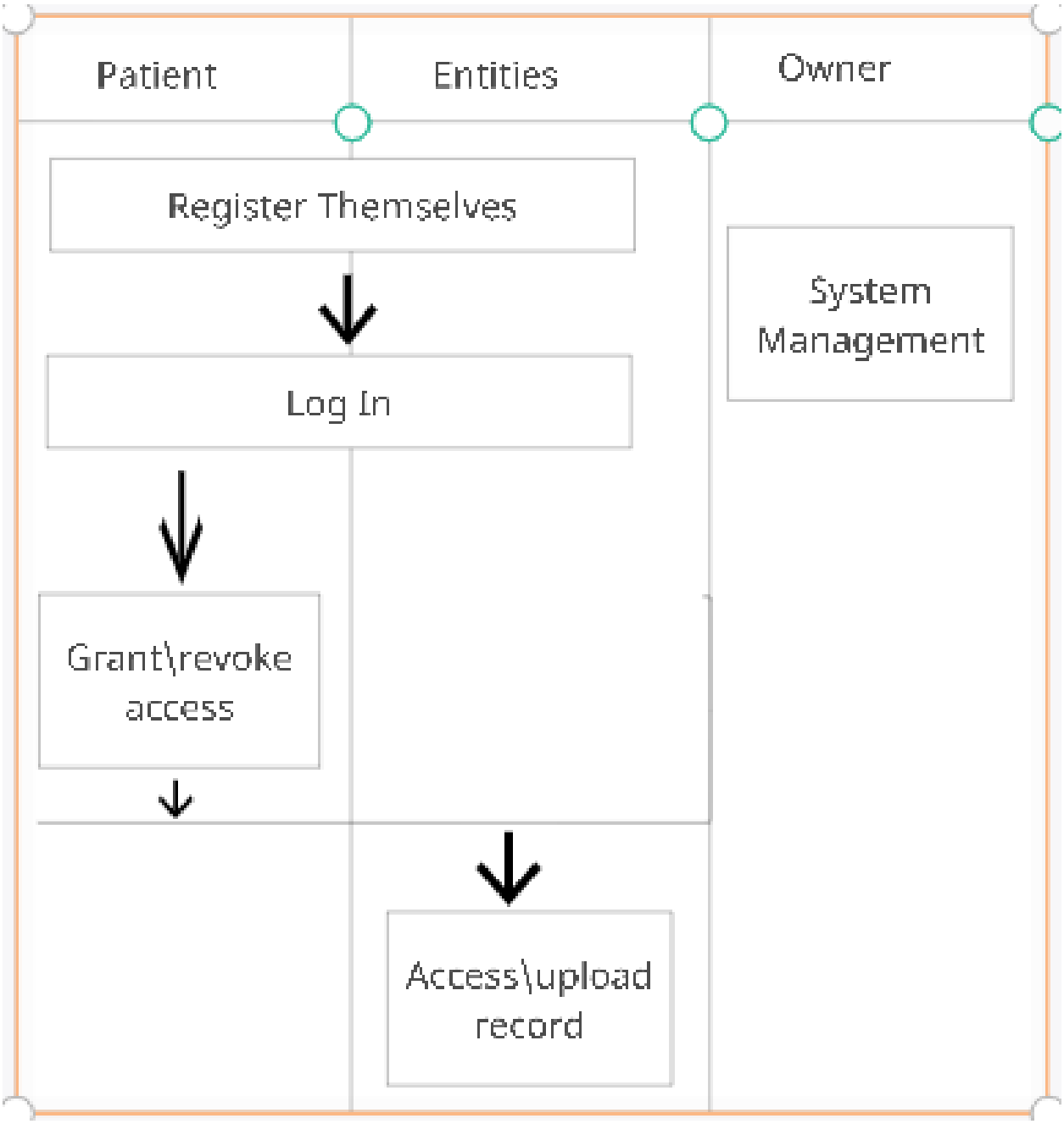

Figure 4.3: Activity Diagram

5. Tools and Technologies

5.1 Frontend

5.1.1 Javascript

Although JavaScript is typically run in web browsers, it can also be utilized by servers and other environments by using a variety of platforms and frameworks. It is a multi-paradigm language that supports both functional and object-oriented programming.Form validation, dynamic content changes, and animations are just a few of the interactive features that JavaScript is frequently used to provide to web pages. More complicated programs, including web games and mobile apps, can also be made using it.Javascript is used as the core scripting language for the frontend development.

5.1.2 React

Component-based architecture, which is the foundation of React, divides UI elements into manageable, reusable units known as components. It is simple to handle complicated UIs because each component can have its own state and behavior. In addition, React makes use of a virtual DOM (Document Object Model) to quickly update the user interface in reaction to state changes.When creating native mobile applications, React is frequently combined with other frameworks and libraries, such as Redux for state management and React Native. It boasts a sizable and vibrant community with a wealth of learning and development resources.

5.1.3 Hooks

Previously only available in class components, state and other React features can now be used in functional components thanks to hooks in React.Since their introduction in React 16.8, hooks have become a crucial component of React development. They make it simpler to reuse functionality between components and enable developers to build cleaner, more succinct code. Developers can design unique hooks to reuse logic across several components by using hooks. JavaScript functions that employ one or more of the built-in hooks are known as custom hooks.For creating scalable, maintainable React apps, hooks are an effective tool. They make managing state and side effects in functional components simpler and more manageable for programmers.

5.2 Backend

A decentralized digital ledger called a blockchain enables secure and open record-keeping. Blockchain technology can give electronic medical records (EMRs) a safe and unchangeable means to store patient data. On the other hand, smart contracts are self-executing contracts in which the contents of the parties' agreement are explicitly encoded into code. Smart contracts can be used in the context of EMRs to automate the management of patient data.Patient data can be securely and openly preserved by using a blockchain and smart contract as the backend for a decentralized EMR system. On the blockchain, each patient would have a unique digital identity that would house all of their medical data. Access control could be handled through smart contracts.

Data is kept in a centralized database under one authority's control in the conventional client-server architecture. Due to the possibility of the database being hacked or otherwise infiltrated by bad actors, this presents a single point of failure. Users must also have faith in the central authority to handle and safeguard their data.

On the other hand, a blockchain is a network of nodes that manages a decentralized, distributed database. The data on the blockchain is accurate and impenetrable because each node keeps a copy of it and verifies any new transactions. There is no single point of failure because the data is spread over numerous nodes, and the system is secure from attacks and hacking. As a backend, a blockchain is used.

The high level of security that blockchain offers is one of the key benefits of adopting it as a backend. It is difficult for hackers to alter or modify the data because it is stored across a network of nodes. Blockchain technology also employs cryptography to secure the data, making hacking almost difficult.

Transparency is another benefit of utilizing blockchain as a backend. Every transaction is documented on the blockchain, making it easy to track a transaction's full history. This makes it simple to audit and validate data, which can be crucial in applications like voting systems or supply chain management.

The use of blockchain as a backend is not without its difficulties, though.

6. Results

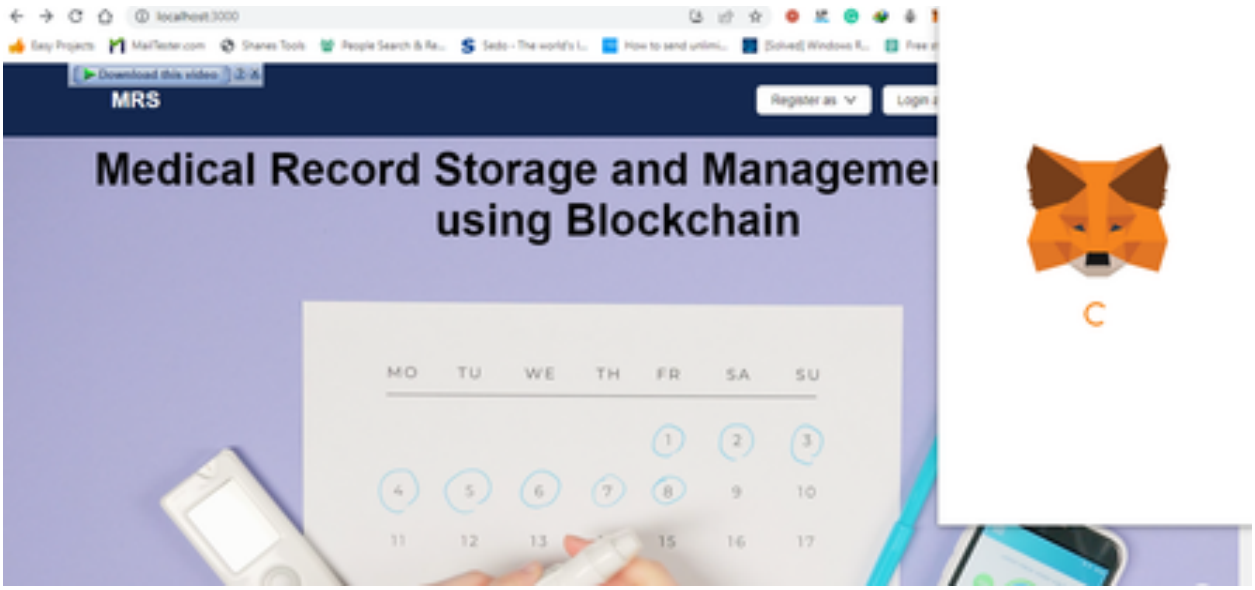

Figure 6.1: Result 01

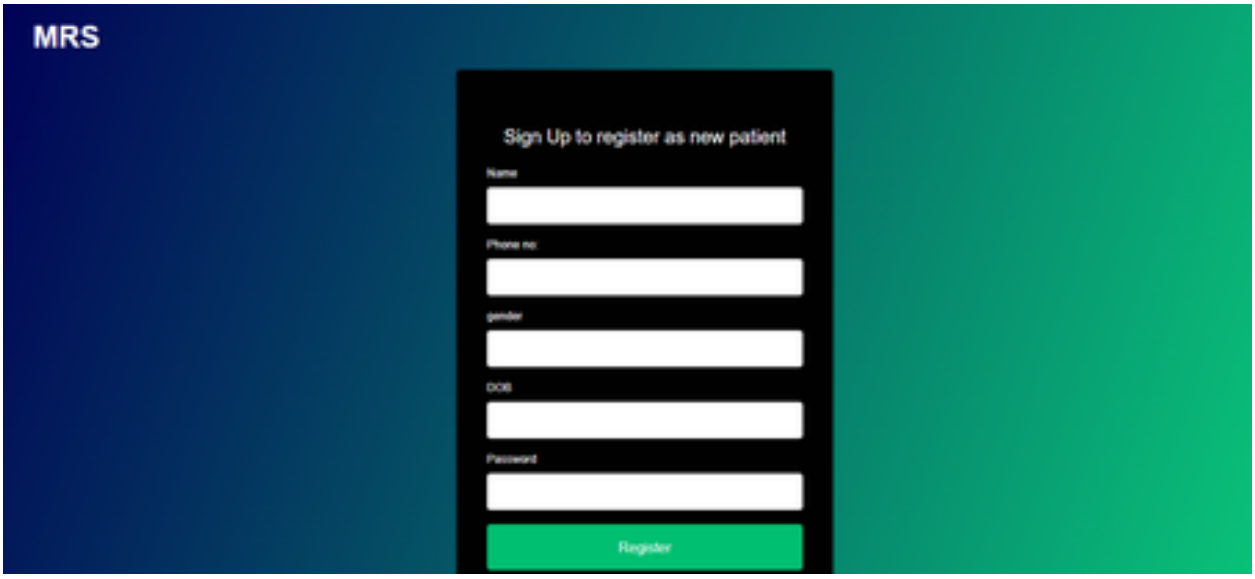

Figure 6.2: Result 02

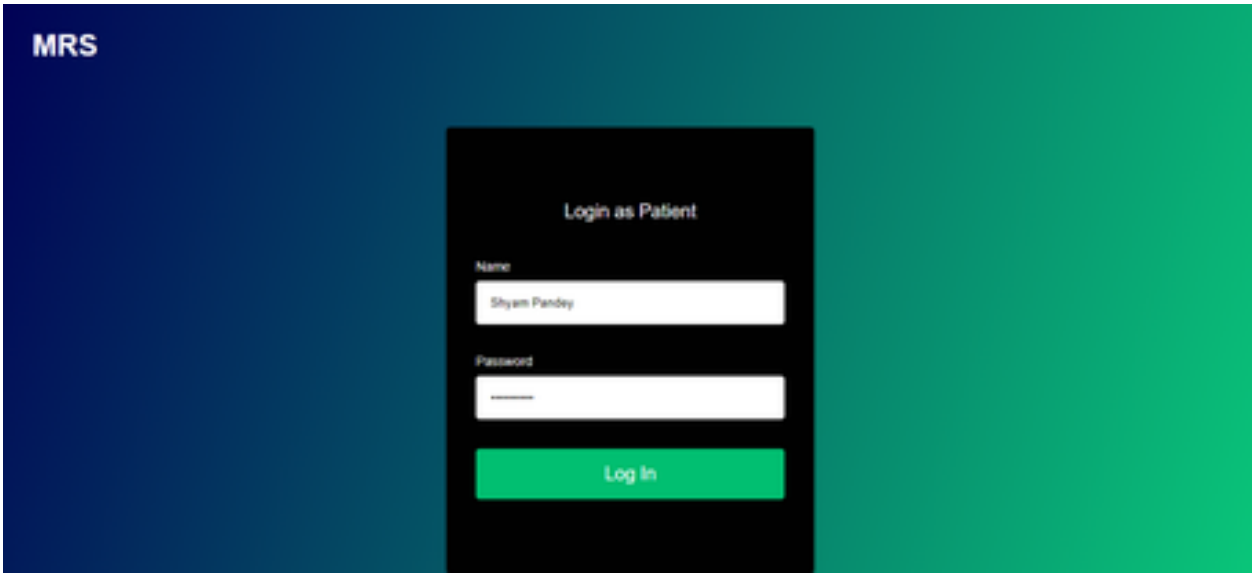

Figure 6.3: Result 03

Figure 6.4: Result 04

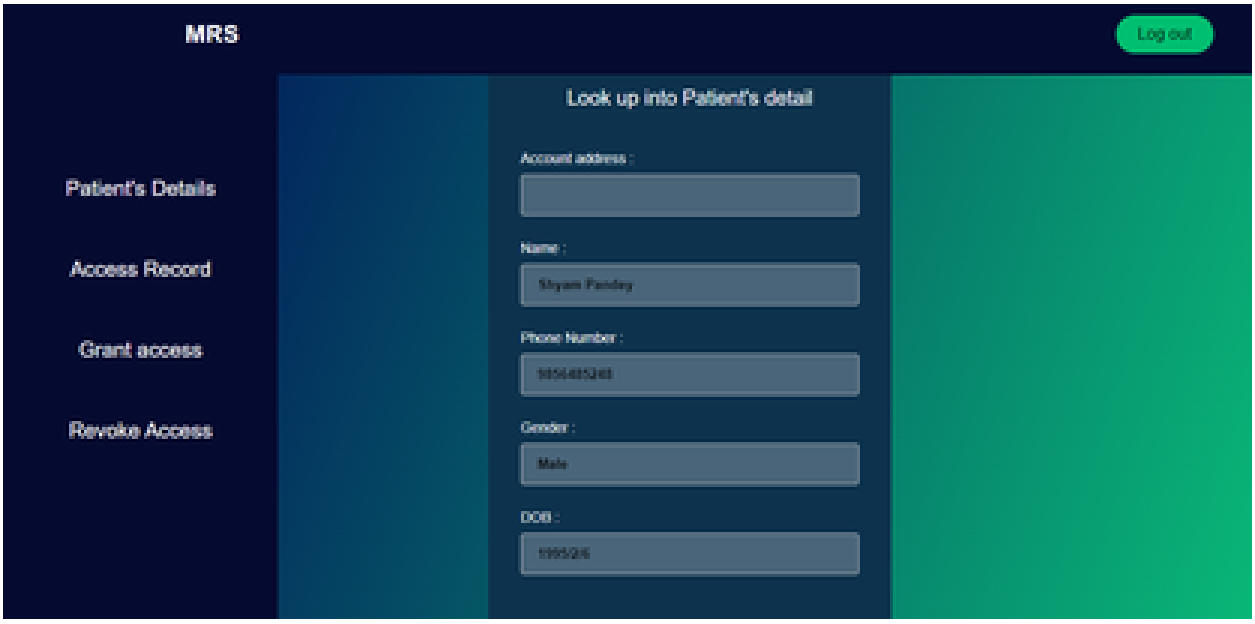

Figure 6.5: Result 05

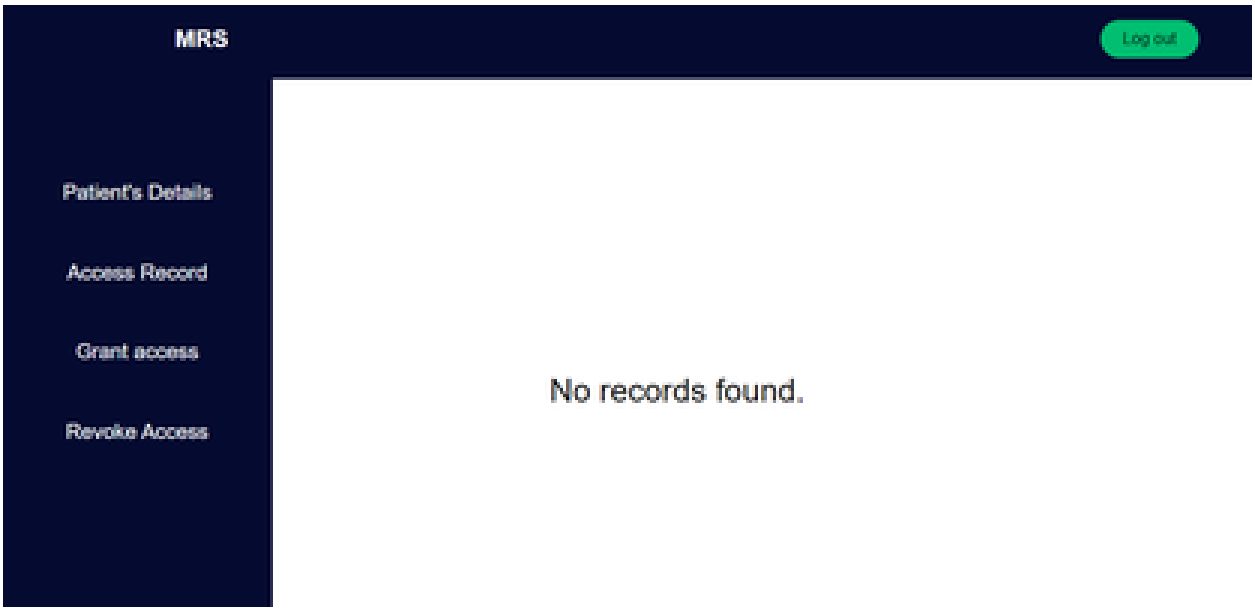

Figure 6.6: Result 06

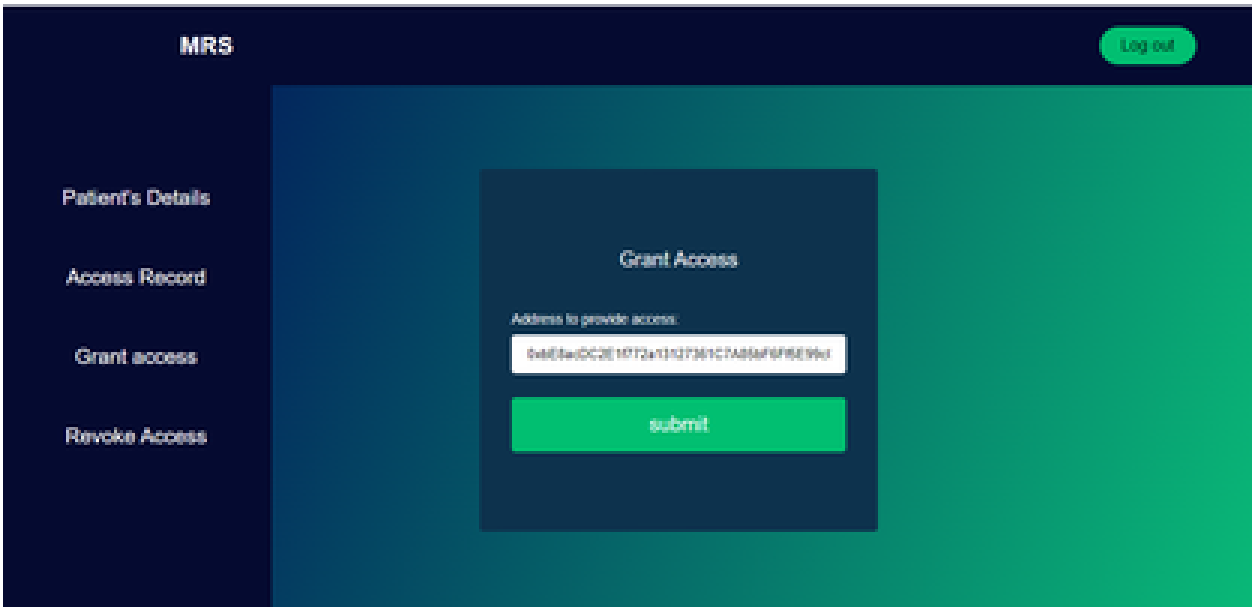

Figure 6.7: Result 07

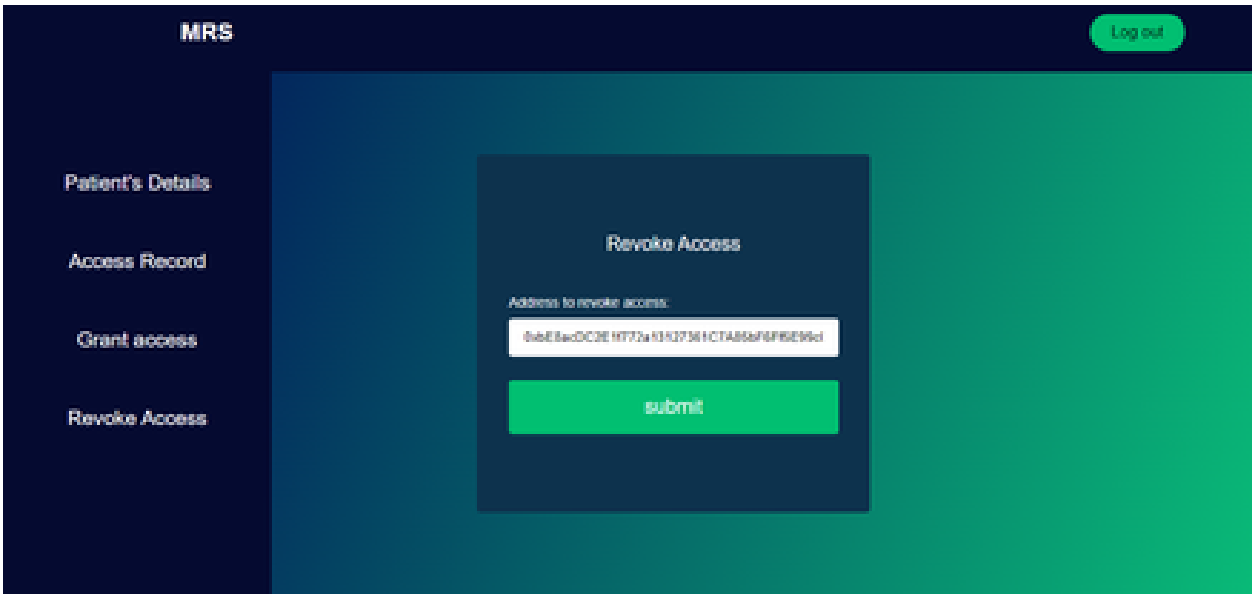

Figure 6.8: Result 08

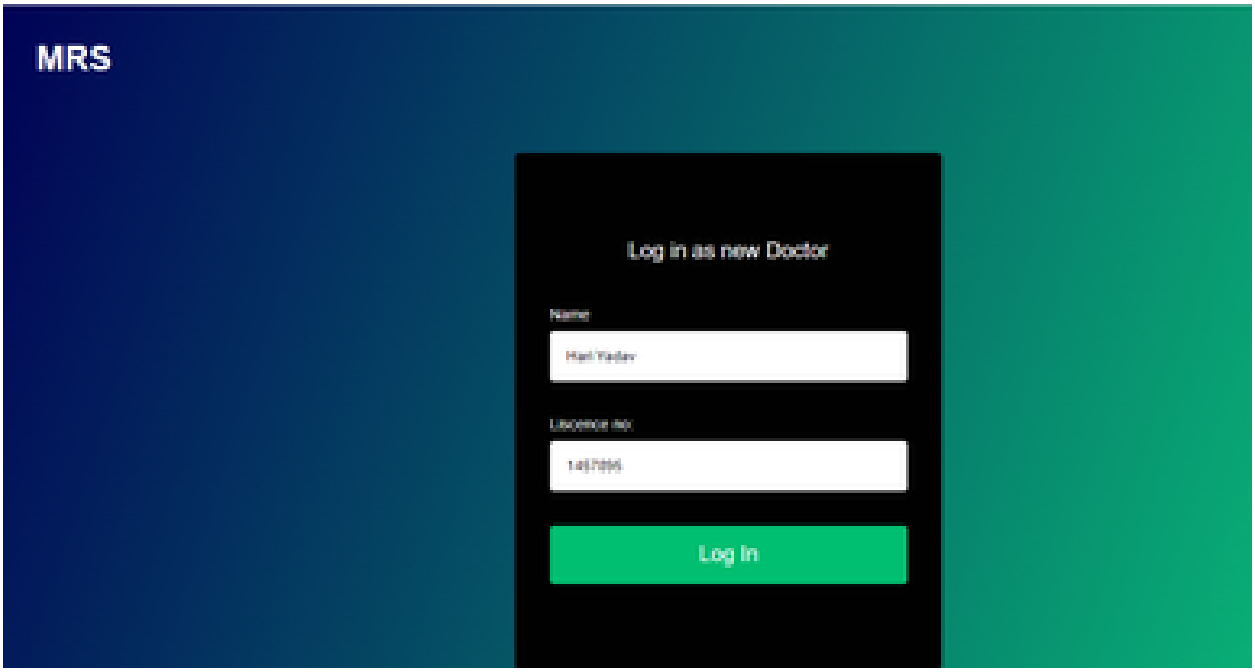

Figure 6.9: Result 09

Figure 6.10: Result 10

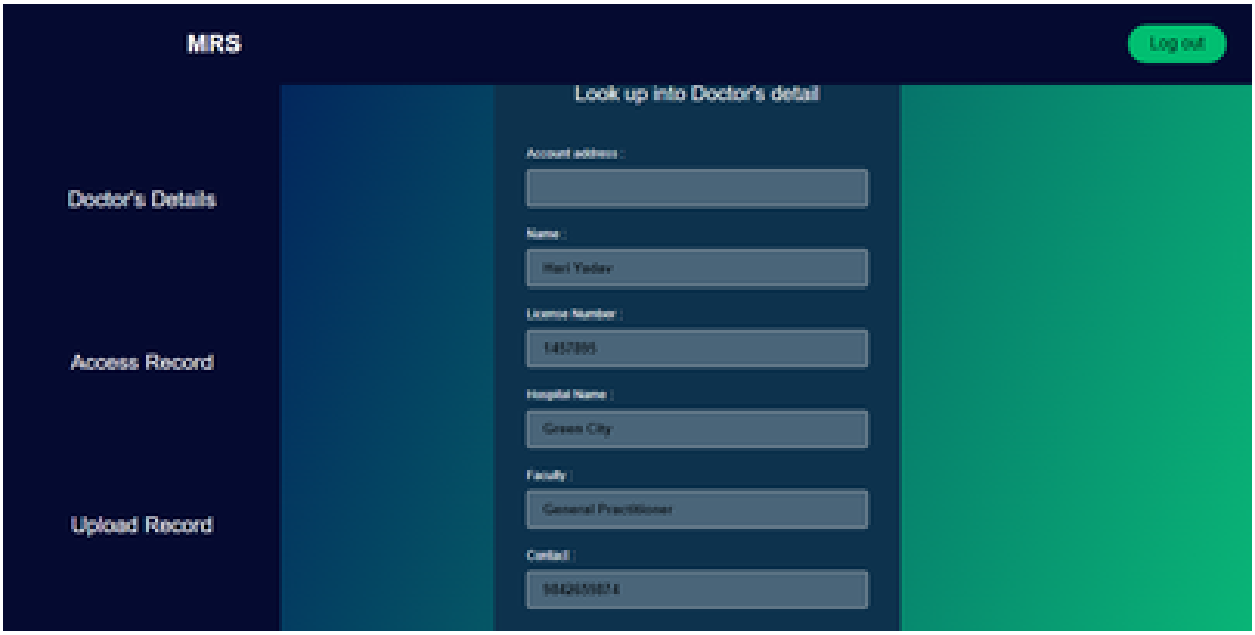

Figure 6.11: Result 11

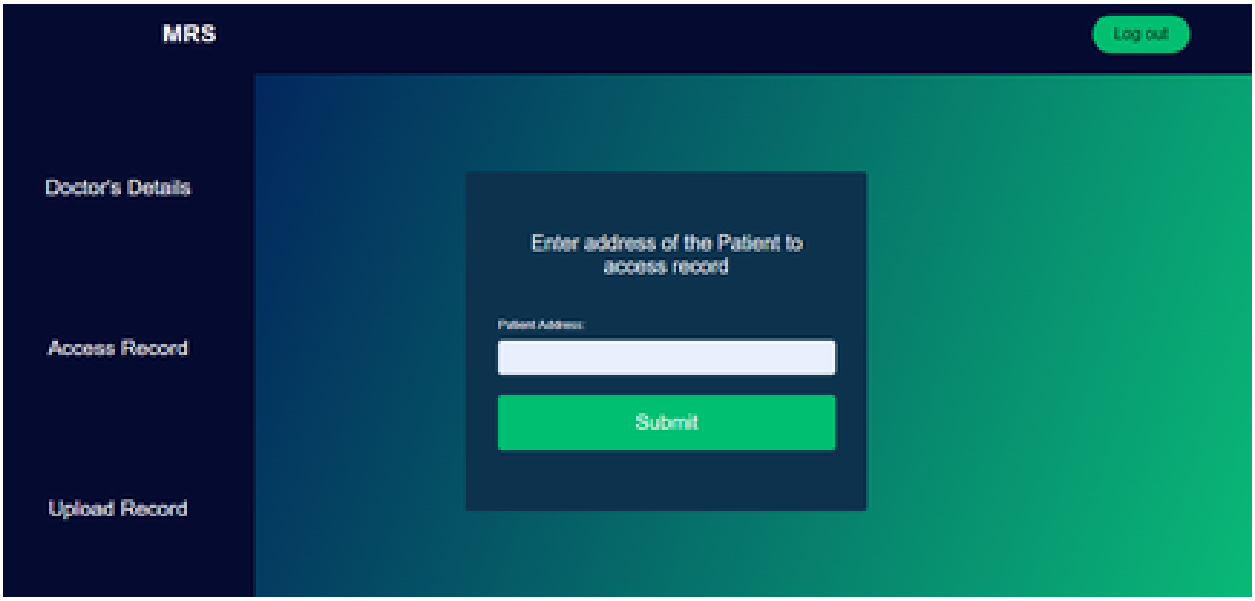

Figure 6.12: Result 12

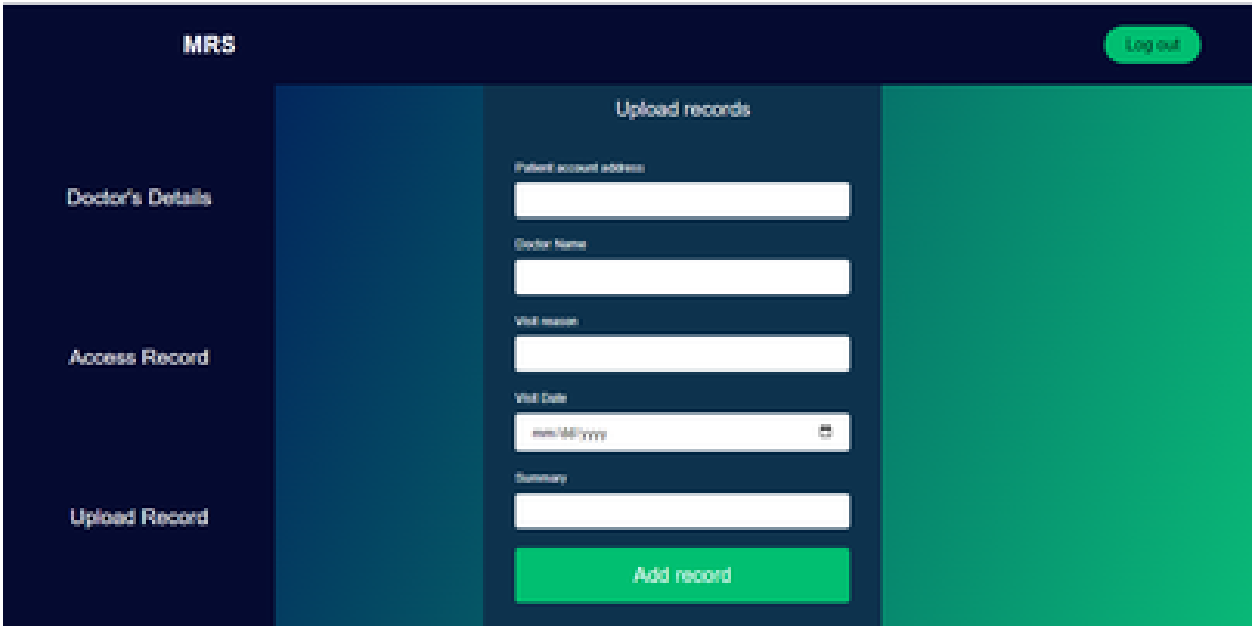

Figure 6.13: Result 13

7. Conclusion

To sum up the project, the Electronic Medical Record Storage and Management System may be the most important and necessary tool for many users who do not want to maintain their records centrally located at a medical facility.Due to the decentralized nature of the system, patients are able to keep track of who should have access to their records.

This system appears to provide a comprehensive storage and administration with a high level of security, dependability, and authority by leveraging multiple resources and incorporating numerous metrics. Additionally, the system seems to have a high level of security, dependability, and authority, all of which are crucial when handling sensitive patient data. By utilizing cutting-edge encryption techniques and decentralized storage, which can stop illegal access and tampering, blockchain technology can help safeguard the security and privacy of patient data.

Additionally, using a variety of resources and metrics can help guarantee the accuracy and dependability of the system. Incorporating various metrics can help monitor system performance and spot potential problems before they become serious, while using multiple nodes or servers, for instance, can help prevent downtime or data loss.

8. Limitations and Future Enhancement

Some of the limitations are enlisted below and how this project shall be enhanced for future use is also described below:

1. The application is identified as the web app. Hence , this application shall be extended to mobile applications as well.
2. This application really needs the actual database for the storage of the record , which hasnot been yet implemented.

References

[1] A. Azaria A. Halamka J.D. Ekblaw and A Lippman. A case study for blockchain in healthcare: "medrec" prototype for electronic health records and medical research data. *Proceedings of IEEE open big data conference*, 13(13):47–55, 2016.

[2] S. Gupta S.K. Khan M.S Gupta and S Mondal. Blockchain based secure architecture for electronic healthcare record management. 16, 2012.

[3] Liyana Shuib Dimitrios Xanthidis Ourania Koutzampasopoulou, X. and D. Nicholas. Electronic medical records in greece and oman: A professional's evaluation of structure and value. *International Journal of Environmental Research and Public Health*, 15(6), 2018.

[4] P. Parolia N. Shinde S. Edoh Thierry O. Pawar and M. Singh. ehealthchain—a blockchain based personal health information management system. 77(22), 2022.

[5] Aishwarya V Natarajan and K Balaji. Medical data management using blockchain. *Journal of ISMAC*, 2:222–231, 2012.

[6] IbrarYaqoob KhaledSalah R.Jayaraman Y.Al-Hammadi S. Pesic M.Madine, AmmarBattah and S. Ellahham. Blockchain for giving patients control over their medical records. *IEEE Access,*, 01:193102–193115, 2020.

[1] [2] [3] [4] [5] [6]