Blockchain-based Mental Health Solution System

by

Faiyaz Masrur
18301213
Abir Hasan Akash
18301215

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
Bachelor of Science in Computer Science

Department of Computer Science and Engineering
Brac University
2024

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Faiyaz Masrur	Abir Hasan Akash
18301213	18301215

Approval

The project titled "Blockchain-based Mental Health Solution System" submitted by

1. Faiyaz Masrur (18301213)
2. Abir Hasan Akash (18301215)

Of Spring, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on May 27, 2024.

Examining Committee:

Supervisor:
(Member)

____

Arif Shakil (ARF)
Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:
(Member)

____

Md. Golam Rabiul Alam
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

____

Dr. Sadia Hamid Kazi
Associate Professor (Chairperson)
Department of Computer Science and Engineering
Brac University

Abstract

In recent years blockchain technology has evolved from finance to industrial usage, wellness to health, commerce to service sector. The convergence of blockchain technology and e-mental healthcare presents an evolutionary system which provides solutions to the challenges of the healthcare system. This report expresses how blockchain revolutionizes the accessibility, security, anonymity of patient data and quality of mental healthcare services. We build a system using Hyperledger Fabric blockchain that fulfill the gap of mental system which lack the tool to verify the credentials of medical professionals, identify the varified patients and access control one's medical data. In the system decentralised cloud system IPFS has been integrated for secure data sharing, storing patients' encrypted data and the hash value is stored in the blockchain. The system also offers users teletherapy treatment and access control over their data. To maintain quality treatment we also implement a review feature. By this project we are able to transform the mental healthcare service with more advancement. This is not just a mental healthcare project, by this project we can also understand how to develop other healthcare sectors.

Table of Contents

List of Figures

Chapter 1

Introduction

In an age of technological advancement the field of healthcare is advancing day by day. From the sectors of healthcare mental healthcare is a critical one as many people from different ages, young to old all are suffering from this illness. The challenges for participants in the mental healthcare involves competence, consent, confidentiality and competing interests.[1] During covid-19 mental disordered patients are moved to isolated wards. Patient's with mental disorder has higher chance for covid-19 infection.[2] Here electronic services and teletherapy plays a major rule for online counseling and mental health research.[3] In last decade visits to the psychiatrist or in the mental health institutes has significantly increased.[4]. Emotional, sexual and physical IPV are mental symptoms which associate with depression, suicidality, and PTSD. In recent study 36 percent people in relationship are victims of IPV from 569 participants.[5] For this increasing disease this field can undergo technological development. In this context blockchain technology emerges with revolution for mental health services, which offers solutions for many problems such as privacy, security, accessibility and transparency etc.

1.1 About Blockchain

Blockchain is a distributed network where each node holds identical data storage. Organization that runs on centralized database that are vulnerable to hackers whereas due to blockchain's decentralised technology stored data become temper proof. Blockchain architecture consist of three different layer where first layer is application layer followed by decentralized ledger and the last is peer-to-peer network. Application layer is a application layer like bitcoin wallet which stores public and private key of a user that controls the unspent bitcoins. Application layer gives a graphical interface from there users create transactions. Decentralised ledger makes blockchain consistent and temper-proof global ledger. Ledger consist of blocks which hold transactions created by users. These blocks are created by miners combining the transaction . The new block is added after the current block by saving the hash of that block which makes a chain of blocks. Blockchain uses consensus algorithm to decide adding and building blocks require most cumulative effort. Miners are peers who holds the full ledger. There also peers who do not share full ledger are light nodes. Only miners are responsible for creating and validating transactions and blocks from which they get incentives.[6] Blockchains' distributed database are

used to store and monitor any type of valuables like goods, resource information, property details, persons data. Almost anything can be tracked with low expenses. Some key components of blockchain, (i) Distributed ledger technology - as discussed the peers of blockchain are geographically isolated and shares identical transaction log, thus makes the ledger distributed, (ii) Immutable records - One transaction is added in the blockchain once, after that no transaction can be changed or altered. Not even the system administrative can remove a transaction. If an error transaction is added to a block then the error transaction is stored in the block. To mitigate this error, another transaction have to create. (iii) Smart contract - can support solidity which is a turing complete language. This code can be uploaded in the blockchain and invoked by a transaction. One has to pay as gas to execute smart contract code. (iv) Anonymity - can be achieve by pseudonymous addresses which is a string characters uses to identify users identity. This address is generated by cryptographic process and does not link to person's real world identity. And the nodes in the network do not know exactly which person is creating transaction or in general storing data.([7], [8]). Recent years blockchain has evolved into different types (i) Public Blockchain - In this type of blockchain anyone can join to the network because there is no single authority to regulate the network. Any user can read or write data in the ledger. (ii) Private blockchain - This is a permisioned blockchain means anyone need permission to become a peer in the network. The read, write access and other regulation are controlled by single authority. (iii) Hybride blockchain - this is a combination of public and private blockchain and also controlled by single authority. Write access is restricted but everyone can read data from the blockchain. (iv) Consortium blockchain - it is a private blockchain controlled by a set of private entities and read, write access, rules are controlled and set by them.[9] In this project we use Hyperledger fabric developed by Linux Foundation to build a private blockchain network. It supports different types of consensus algorithm and can be used which is best for the system . This is the first blockchain network which supports smart contract written by regular programming language and it does not need any gas to execute. Hyperledger fabric utilises identifiable participants, the network throughput performance is high, transaction confirmation time is low and maintains privacy and confidentiality. As a result this becomes a suitable for many enterprise use cases. The nodes that create blocks by ordering transaction are known as ordering service and they does not contain any block. It also provides membership service provider which is accountable for identifying the entities of the network.([10]-[11]) By storing the patients data in different nodes and granting them full control over their data we can create a temper proof system.
Furthermore, Blockchain-based mental health solution systems promote accessibility by overcoming traditional healthcare system barriers. We develop the system to verify patients and doctors which ensures trustful treatment environment. Patients can get remote therapy services from verified doctors. Decentralization of cloud storage system and transparency provided by the blockchain-based system offers benefits beyond data security and anonymity. As a result researchers and stakeholders can see anonymous patients data. This project provide individuals with control access over their medical records, treatment plan. Also the system construct a friendly domain where verified patient can give review to doctors. In conclusion this system represents a breakthrough approach to eliminate the challenges of mental health care by providing data security, privacy, transparency and accessibility features.

1.2 Problem Statement

The development in the mental health care sector is essential as growing the global burden in mental disorder and promoting overall well being. In this modern era urbanization is increasing all around the world. For this growing phenomenon mental health and services are facing many significant challenges like depression, lack of companions, joblessness, low income, excessive charging of mental healthcare services. Fast and unstructured developing countries like Bangladesh are enclosed by these challenges.[12]
There is a need to integrate mental healthcare into e-mental health platform to mitigate offline service providing problems which are barriers to get treatment, high cost, unstructured services system, mental healthcare related stigma. The process of integrating this service platform requires a customize approach. But there is a risk integrating an online approach that may lack some mental disorder. It's possible that already inadequate health services will be overworked, and there is insufficient data to support this expanding teletherapies.[13]
The importance to fill the mental healthcare service gap due to some specific barriers of availability, accessibility, acceptability and affordability. In this study, the primary service obstacle identified was cost. On the other hand, stigmatization or acceptability hurdles were rated lowest. Treatment for mental health issues is expensive, which suggests that individuals do not prioritize treating mental health issues or are unaware that treatments are available to anybody in need of them at no cost or with a few charges.[14]
The development of mental healthcare services is progressing slowly in middle and low income nations. The lack of finance from stakeholders, the difficulty of decentralizing the mental health platform, the difficulties of implementing it in primary-care settings, the low number of highly qualified service providers, and the recurrent shortage of leadership are some of the obstacles to this slow expansion.[15]
More than thirty-five percent of parents in a poll of 116 families stated that structural limitations, attitudes against mental health, and views of services are the key causes of obstacles to mental healthcare.[16]
One of the most critical challenges of mental healthcare is data privacy and security. As mental health care services are increasing in digital platforms, patients' data are more vulnerable to being leaked or unauthorized access. For this unauthorized access still in many places around the world, online access to health-care services is being held back. Compared to other areas of digital health, concerns about breaches of data privacy in the field of e-mental health seem to be much more significant. Furthermore, the majority of persons provide details regarding their addictive behaviors, recollections of abuse, thoughts of self-harm, traumas are the intimate data are exchanged throughout the e-mental system. These data are more susceptible to unwanted and illegal access due to conventional centralized data storage systems. Insufficient technological knowladge, encompassing a restricted comprehension of safety, secrecy, and anonymity is the primary impediment to using healthcare services.[17],[18]
Accessing mental care is a significant challenge in mental care service. People encounter difficulties getting mental health care in various nations, mostly due to a lack of resources and drugs. The World Health Organization (WHO) reports that for every 100,000 individuals, there are typically 0.1 mental health professionals and

0.3 psychiatric nurses in low earning nations.[19] Because there are limited mental health facilities and services available, there are few experts. Many people have significant obstacles when trying to receive mental health treatments, particularly those who live in distant or underserved locations, afraid of discrimination from their own society and inadequate knowledge about psychiatric services that are available.[20] High cost and insufficient insurance are also a barrier to accessing mental health care. As there are few amounts of mental care services the cost is high so for a poor family getting mental health care is a burden.[21],[22]

Access to mental healthcare is also hampered by limited alternatives and lengthy wait times. People must wait a very long period for in-person therapy, which makes them disinterested in mental health services. According to studies, 95.6 million American people, have experienced delays in receiving mental health treatments lasting more than a week. Furthermore, almost half Americans have either had to drive over an hour for medical attention or know someone who experienced.[23]

A further issue facing the mental health services is ignorance. Maximum patients desire to be healed but do not pursue medical attention. They feel that physically presenting a cure at a clinic is a burden, and they tend to be unaware of the facilities available for mental health care. An further obstacle to receiving treatment for mental illness is social stigma. Most individuals refuse therapy because of fear that others would discover they are mentally ill and that they have even lied. The stigma is holding back progress in the field of mental healthcare.[24]

Systems for mental health treatment are disjointed and lack communication between different organizations and providers. indicates that a large number of decision-makers within a mental health service or organization degrade the system by creating a lack of collaboration or a financial disagreement, which leads to an ineffective use of resources. And fragmentation has a negative effect on choice-making, value, price, and results. The disjointed structure makes it simple for the underprivileged to evade receiving care. Furthermore, patient data frequently vanishes while being altered in several facilities'. There is a lack of coordination and continuity in patient treatment when professionals are unable to access and communicate patient medical data between institutions.[25]

Another significant obstacle in the field of mental healthcare is the administrative load. Healthcare services are negatively impacted by administrative load because it prevents patients from receiving care. Professionals are frequently kept busy with administrative duties such as billing, scheduling and organizing appointments, maintaining accurate records, and document storage. These time-consuming duties take attention away from the patients. Consequently, the mental health system's effectiveness and quality decline.[26]

The issues confronting the mental health industry have grown in recent years, including those related to data privacy and security, access hurdles, the administrative load on healthcare professionals, stereotypes and disinformation, a lack of regulations, expense, waiting periods, and a lack of connection. To revolutionize mental healthcare, creative solutions are required in response to these growing issues. Blockchain technology, online software platforms, and medical instruments are examples of new technologies that have the potential to completely transform the mental health care industry.

1.3 Project Objective

The principal aim of this project is to devise, construct, and execute a framework that primarily accords precedence to security and privacy in the mental healthcare infrastructure. Utilizing blockchain distributed ledger technology to store only patients sensitive medical data that way we can block unauthorized access and cyberattack.
To build a system that can verify both patients and doctors. This will create a trustful system where patient can check verified doctors credentials.
One of the core objectives is to provide access control over one's personal data. Patients can decide which doctor can see their data, they can also able to set data access time or direct revoke the access.
The project seeks to overcome the challenges of data leakage by implementing blockchain technology and InterPlanetary File System in the e-mental healthcare system where patients and doctors can securely share and store their data in encrypted manner.
The project offers appointment form and teletherapy sessions to patients where they can get treatment from remote places and save time and money as it reduces cost and time associated with in-person visits. Our goal is to make the mental healthcare services accessible to all whatever their location and financial status is.
Administrative overhead is a challenge for mental health services that shift professionals focus from patients by doing administrative work which reduces valuable time. Our objective is to reduce this administrative burden through blockchains smart contact which automates administrative tasks and makes time efficient for treatment.
We are allowing patients to give feedback according to the doctor's treatment. And other patients can see which doctors get the best review. This enhance the quality of e-mental healthcare system.
This distributed system offers researchers and stakeholders to get anonymous patient's medical data in exchange of funding, that will use to develop system's blockchain technology more further.
The goal of the project is to create a system that is long-lasting and expandable. It need to be ready to accommodate or assist expanding user bases and changing healthcare requirements and long-term maintenance services to guarantee the system's efficacy.

1.4 Work Plan:

In this project an iterative process model is followed (fig.1.1). This is a SDLC process model which helps to build efficient, correct, easily maintained and modified software with minimum effort within lowest possible cost and least possible time. This provides a clear road map for software development, dividing the project phrase with clear objectives and deliverables. This model guides to make the project in a systematic and organized way. As the requirements are not fully identified and there is a possibility to change some features after the development of the project so this SDLC model is suitable for this project.

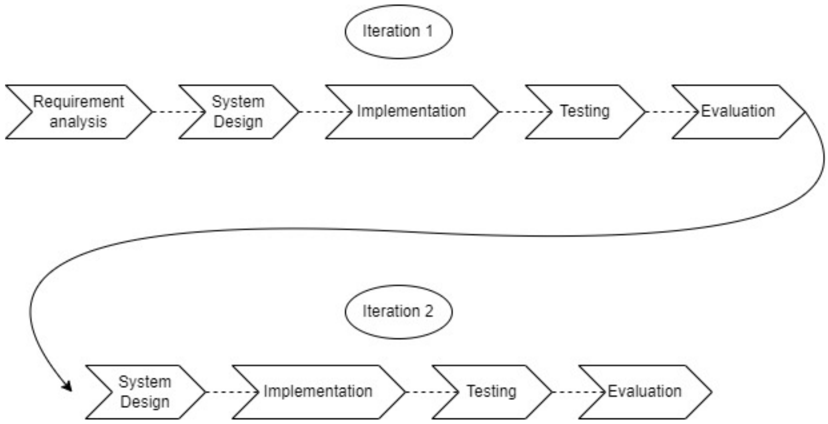

Figure 1.1: Project Work Plan

1.Requirement analysis: Identifying the stakeholders, including mental healthcare providers and users. And to find what should the functions and characteristics of the system by researching or studying related works. Researching blockchain technologies to implement into the system.
2.System design: Blockchain infrastructure design and selecting appropriate blockchain platform. Different types of system related diagram design like database design to know the data structure in the system, component diagram design to know what the system components will be, data flow diagram design to understand how the data will move through the system etc. Lastly, user interface design to experience how the system will look like.
3.Implementation: Developing the blockchain technologies and storage system. Then will start implementing the system environment, first developing the user interface and connecting the database with the system. After that developing other features and implementing blockchain technologies like smart contracts.
4.Testing and evaluations: After the full implementation of the system conducting extensive testing to identify and resolve issues. Testing will help to find the bugs and errors of the system and also check if the system is fulfilling the proposed requirements. Then we will evaluate the system by walking through others in the system, they will give feedback regarding further development. Finally, after finding a problem or according to suggested feedback of, again we will start from the design part or move to the next stage if we do not need any updates.
5.Presentation: After the project is successfully done we will present the project to the coordinators.

Chapter 2

Detailed Literature Review

Blockchain originally designed as a means of facilitating bitcoin transactions and has now transformed into a practical technology with applications for various industries, including the healthcare sector. The healthcare sector is evolving these days, moving toward technology-based remote services. Integrating this distributed database in healthcare system further led to temper proof storage, access control over personal data and many more.
User-oriented records management system based on blockchain technology that ensures safe data exchange through the use of a proxy re-encryption mechanism. Access logs that are maintained by reputable cloud service providers are audited using blockchain technology without any modifications, and patients request that the logs be checked by the service providers.[27]

For valued medical diagnosis, the healthcare industry is implementing cutting-edge technologies. Blockchain technology is being used in the mental health industry to motivate patients and facilitating the safe transfer of private patient information between healthcare facilities. The present study delves into the principles of this technology, examines its evolving effects on the healthcare industry, and focuses on developing an infrastructure.[28],[29],[30]
A popular issue on the internet these days is the metaverse and non-fungible tokens, or NFTs. The use of NFTs and the metaverse to therapy applications is covered in this work. Access to mental healthcare and severe absence of mental health specialists are problems that can be solved by using the metaverse, a three-dimensional web or virtual reality tool. In the metaverse, cryptocurrencies like bitcoin, eth, and NFTs with a blockchain foundation provide a wide range of opportunities for socioeconomic collaboration.[31][32]
The work reported in this article uses a solidity-based smart contract that maintains patient health data obtained from sensors which functions through an Ethereum virtual machine. This constructed private blockchain network allows safety in IoT-based healthcare. Moreover, this smart contract technology will enable notify transactions for patients and medical professionals by integrating web3, Metamask, and truffle environments.citeNihar Some other projects extends Iot framework that stores raw or encrypted data in IPFS a decentralized hypermedia protocol as json format associated with blockchain address to locate and stores the hash value, patient's identity(patient id, area id) and timestamp in private ethereum.[33],[34],[35]
There is a case involving medical record fabrication. To avoid being held legally

accountable, the healthcare professional fabricated the medical record. An online Electronic Medical Record system is being created in order to prevent the fabrication of medical records, this solution leverages the Ethereum blockchain to preserve the hash value of the documents as a point to check inconsistency. The system employs restrictions on access to medical records in order to avoid unauthorized access.[36]
The UniRec (Unified Medical Records) software operates on a peer-to-peer (P2P) network built on the Ethereum Blockchain, preserving an unchangeable shared history of each electronic health record (EHR). Medical records are sent between institutions using IPFS and encrypted via OpenPGP API before added into the network. An IPFS URI is used to add a reference to the file to the Blockchain, allowing for discovery.[37], [38] Another ethereum based healthcare app called SHEMB uses symmetric searchable encryption technique before storing into the blockchain.[39]
This private blockchain project maintains enormous amounts of digital assets, including medical data using decentralized cloud storage (IPFS) in order to provide anonymity, fixed, identifiable, verifiable in teletherapy services. The only data maintained on-chain in this proposed system is the hash value of digital content and transaction metadata.[40][41]
These Ethereum-based apps do have certain limitation though. The primary constraint stemming from the utilization of blockchain smart contracts is the elevated transaction costs. Payments are charged for transactions that invoke contract code.[42] Another issue with the public Ethereum blockchain is scalability problem, which is caused by the limited amount of transactions that can fit in a single block.[42] Compared to public blockchains, permissioned blockchain as Hyperladger provide a number of advantages. It has the capacity to partition the network into segments where a certain percentage of nodes are necessary for transaction validation, hence enabling increased scalability and parallel processing. Additionally, the verified nodes are trustworthy, which makes it possible to implement consensus methods that offer a much higher throughput between 3000 and 20000 transactions per second.[43][44]
The EHR management system PREHEALTH, which utilizes an Identity Mixer (Idemix) and distributed ledger technology to protect privacy. The system offers a proof-of-concept solution that makes use of the permissioned blockchain Hyperledger Fabric to efficiently store patient information which offers anonymity and unlinkability.[45]
This paper presents a hyperledger-fabric based medical data sharing system called MedHypChain that protects patient privacy. Every transaction is encrypted using signcryption method and patients store their health record on the blockchain so that it can be only accessed by authorized parties.[46]
The private permissioned Hyperledger Fabric blockchain offers patient to store health data in IBM cloud and hash value in the distributed database. This app also sloves authentication problem by utilizing cryptographic techniques.[42][47]
This paper proposes a unique system in order to solve single point failure of storage that utilizes decentralized databases called OrbitDB which uses IPFS. They also utilise Hyperledger Fabric to manage access and to stored hash value of data.[48][49]

Chapter 3

Project Details Analysis

3.1 System Design:

This section outlines the layout of the system and describes how patient data is stored on it., how the participant's get verified, how appointment and teletherapy sessions will take place, how the review feature works.

System Architecture

We consider the e-mental service a website based system that can verify the end users like verified patents, doctors and researchers. The patients get verified by their national id number. The doctors get verified by his degree certificate. The authorities are the peer nodes of the hyperledger fabric private network who holds the full ledger of patient's data and they also verify the end users. The researchers have to pay to get registered into the system in order to get patient's data by getting permission from patients. The Verified patients can create appointment to his preferred doctor or the system will choose a doctor for him. Patients have to pay first to create the appointment. The doctor will conduct teletherapy seasons to the patients that are in his appointment list. Therapy sessions recorded videos, documents, patients healthcare data are kept in the distributed cloud storage IPFS. These digital content are encrypted and decrypted using admins private key before uploading as well as downloading. Blockchain will be used to store the hash value which comes back from the IPFS and that is the location of the saved record. The patient can give and revoke access whoever want to see his personal data. And the access will be maintained by a list that will also be stored in the blockchain. The other not sensitive data are stored using mysql database. After treatment has finished the patients can give doctors review according to the quality of the treatment. Both verified and unauthenticated website visitors can see the reviews of a doctor. But Unauthenticated visitors can not create appointment. Researchers have to get permission from patients in order to get their medical reports else they are not able to see the reports. This refered image (fig.3.1) shows the hardware and software connection and user relation of the system.

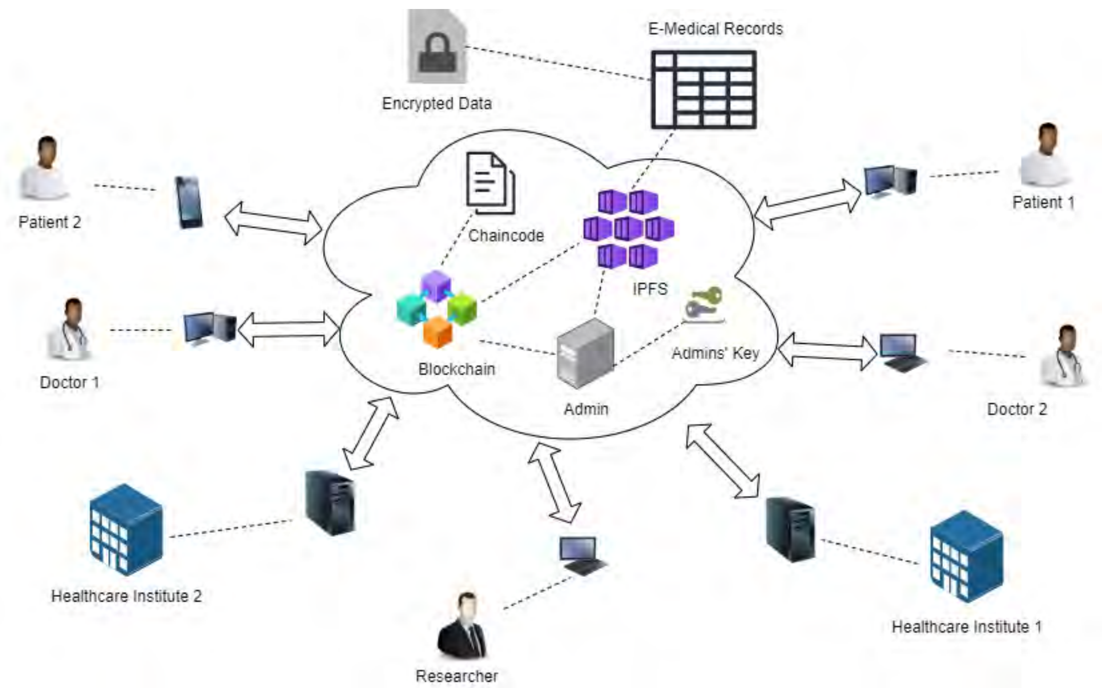

Figure 3.1: System Architecture

System Actors

In (fig.3.2) shows integrating patients and doctors in the initial level

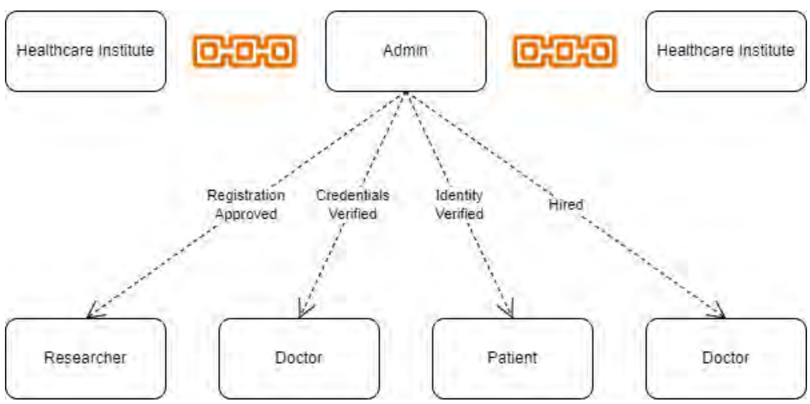

Figure 3.2: Trust Model Between Actors

fosters confidence between them and the system's top tier authorities. Actors are therefore divided into different categories inside the system.

Healthcare Authorities- They are the committing Peers or endorsing Peers of the hyperledger permissioned network. They takes transaction proposals and executes them to create endorsements. And they also maintains the state of the Blockchain and commits, verifies transactions. They can join the network by funding the system that will use to develop the blockchain even further.
Authorities- They are the admins of the system and also plays the role as a healthcare institutes. They are the main authority who give permission to others to join the network. They also verify or remove doctors' certificates and patients' identities, hire doctors and solve any other problems, queries of lower layer users. Their public key is used to encrypt and decrypt medical content. But they cannot decrypt data without the permission of the patients.
Doctors- They are healthcare practitioner who get appointments, provide teletherapy sessions to patients. They are verified by the admin, without verification they cannot get appointment or treat patient. They get verified by uploading their degree credentials and also updating them. They can get and update patients' medical record with getting permission. They can also block their appointment time if there is no appointment in that time.
Patients- They use the system to get teletherapy creating appointment by payment. They can upload their personal information and grant assess on their data. They can choose doctors by the review and after treatment they give review to doctors.
Researchers- They can apply to the system and be approved by the admin. Researcher can get patients confidential data by requesting access permission to them.

3.2 Requirement analysis

The requirements analysis serves as a comprehensive development strategy by defining the features, functions, and characteristics of the project. It lays out the goals of the project in detail, outlining the issue the program aims to address and the benefits it offers to consumers. In addition, this stops developers from implementing pointless features or functionalities.

Functional Requirements
Functional requirements offer users activity in the system, specifies how it should operate to certain action, and how it must function in specific circumstances.

Features for Doctors:
Profile Management Doctors can request for their profile updates for qualifications, specialties, and availability including authentic documents.
Appointment Management Access a calendar for scheduling and managing patient appointments. Receive notifications for upcoming appointments.
Patient Records View, update and download or print patient medical records, treatment histories, and assessment results, all securely stored on the blockchain.
Request Access Can give request to get access to patients' data.
Create Session Can create sessions with appointed patients to give teletherapy.
Treatment Plans Create and update personalized treatment plans for patients, including medication prescriptions if necessary.
Billing: Manage billing through smart contracts, streamlining administrative tasks.
Patient Feedback Get patient feedback and ratings, improving the quality of care.
Fees Pay a monthly fee to the authority for using the platform.
Contact Contact with authorities in case of any complaints or reporting any issue.
Patient List Can see patients list those who create appointment and those who got treated.

Features for Patients:
Profile Creation Patients can create and manage their profiles, including personal information, medical history, and preferences.
Appointment Booking Schedule appointments with doctors based on availability, specialties and the appointment will book after paying session fees.
Access Control Can grant and remove access to others who want to

see medical reports.
Join Session Can participate in teletherapy sessions with mental health professionals.
Contact Contact with authorities in case of any queries, complaints or reporting.
Feedback and Ratings Provide feedback and ratings for healthcare providers.
Doctor List Patients can check the available doctors list, their ratings and also search for doctors by their names and specialities.

Features for Administrators:
User Management Admins can verify and remove user accounts.
Doctor Management Admins can verify and remove doctor's accounts.
Blockchain Network Management Oversee the blockchain network, including nodes, security.
Compliance and Reporting Monitor and ensure compliance with healthcare regulations and reporting requirements.
Analytics and Insights Access analytics tools to monitor system performance and user engagement.
Financial Management Oversee financial transactions, payments, and financial reporting.

Features for Researchers:
1. Researchers can request to get verified by paying.
2. They can make access request to patients.
3. Can see patient's medical records and treatment history after getting access by patients'.
4. The system will give the flowchart of different types of patients mental health conditions.

3.3 Non Functional Requirements:

These describe the characteristics of the system and impose rules on the features it provides. They also relate the overall capabilities of a system.
Verification and Identification

The system must verify every users in the system. In registration form patient has to give their national id number to get verified. One id card can be used only once to get registered. If a NID has used before than patient can not resister himself with that NID and can not get the services of the system. In blockchain patients is identified by blockchain address that is generated by combining patients id + NID number. Without verify patient cannot able to create any appointment but he can see doctors information and review. Doctors will have to upload his credentials in order to get verified. The admin will check for the authenticity of the credentials and permit doctors request. Without verification doctors cannot get any appointment and treat patient. For researchers to get registered they have to pay some money else they cannot have access to the system functionality.

Storage Security

The recorded treatment videos, documents, patients medical records should store in the decentralised storage for better security. Our solution to the storage issue with blockchain is the Inter Planetary File System, a distributed storage that helps.First, an asymmetric encryption method is used to encrypt the medical information using authorities secret key. The patient's identity address will then be linked to the encrypted data in the IPFS. The hash value of the data comes back via cloud storage, which is then logged in the blockchain where the patient's identity address is mapped. Only patient and doctor if granted can able to store the data.

Access Control

The system should able to give patient control over their data. Patients can grant any participants doctors, researchers, authorities to access their data. In the backend the id of the participant will be added in the access list. This list is unique to each patient and is kept on the hyperledger blockchain. The id will be deleted from the list if patient want to withdraw his access from the participant. Only the patients and doctors have the update access to medical data.

Secure Sharing

Participants can able to securely share the medical data. Any participants wants to access a patients sensitive data then the system checks participants id in the access list of patient. If id is in the access list then the system takes the patients identity address and fetch stored materials corresponding to the address. Then the encrypted data is decrypted using admins private key. On the other hand if participants id is not found in the access list than an access request is send to the patient. If the patient accepts the request than the senders id is added to the list and he get the medical information. Else participants data request has been cancelled.

The sequence diagram in (fig.3.3) illustrate the inner structure of how the data is uploaded, encrypted in the system, how the access is granted and how it can be shared to doctors or researchers or how the sharing can be denied.

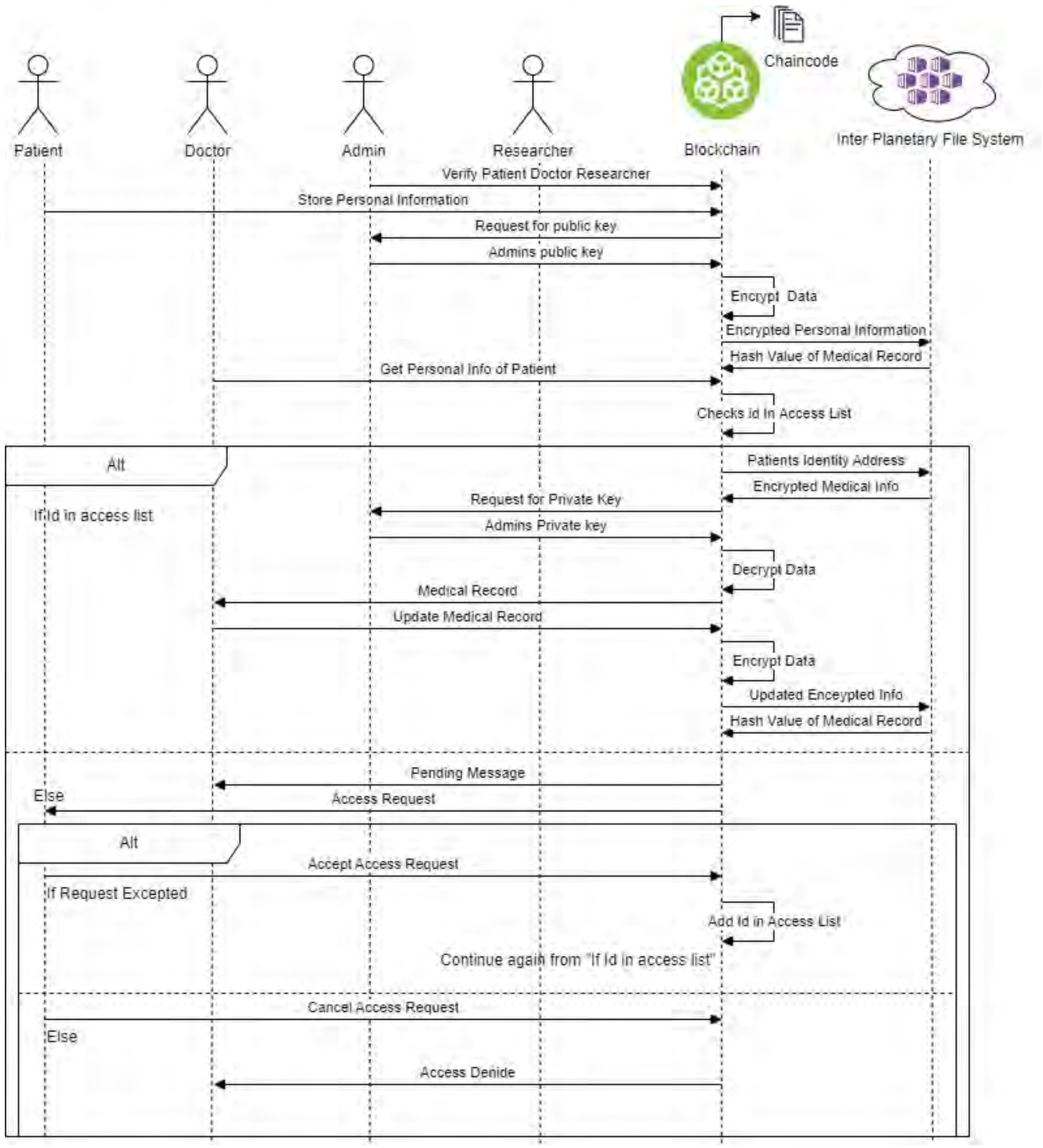

Figure 3.3: Sequence diagram of data storing and sharing

Chapter 4

Project Design

4.1 Use Case Diagram

Use case diagrams focus n order to ensure that software is designed from the viewpoint of the user, use case diagram in (fig.4.1) focus on the relationship between participants and the system. It is possible to detect any problems early on and fix them before moving forward, reducing energy and cost by observing how people communicate with the software. It also helps to capture and illustrate the functional requirements of a system. This results in a product that better satisfies customer demands and is more clear and easy to use.

4.2 Class Diagram

The system stores users in the ledger as key value pair. Value is the users information as javascript object that maps to users nid which is the key and used for crud operations. Each user stores table data separately in their object model. In (fig.4.2) represents the class object of the users and important lists are the children of the class. The class diagram helps to visualise different user classes of the system and how each class has a relation with another class.

4.3 ER Diagram

ER diagrams are crucial to design an effective and correct database. It gives a straightforward illustration of the data kept in a database which helps developers to understand the arrangement of data and how various information is linked to each other. This also solves data

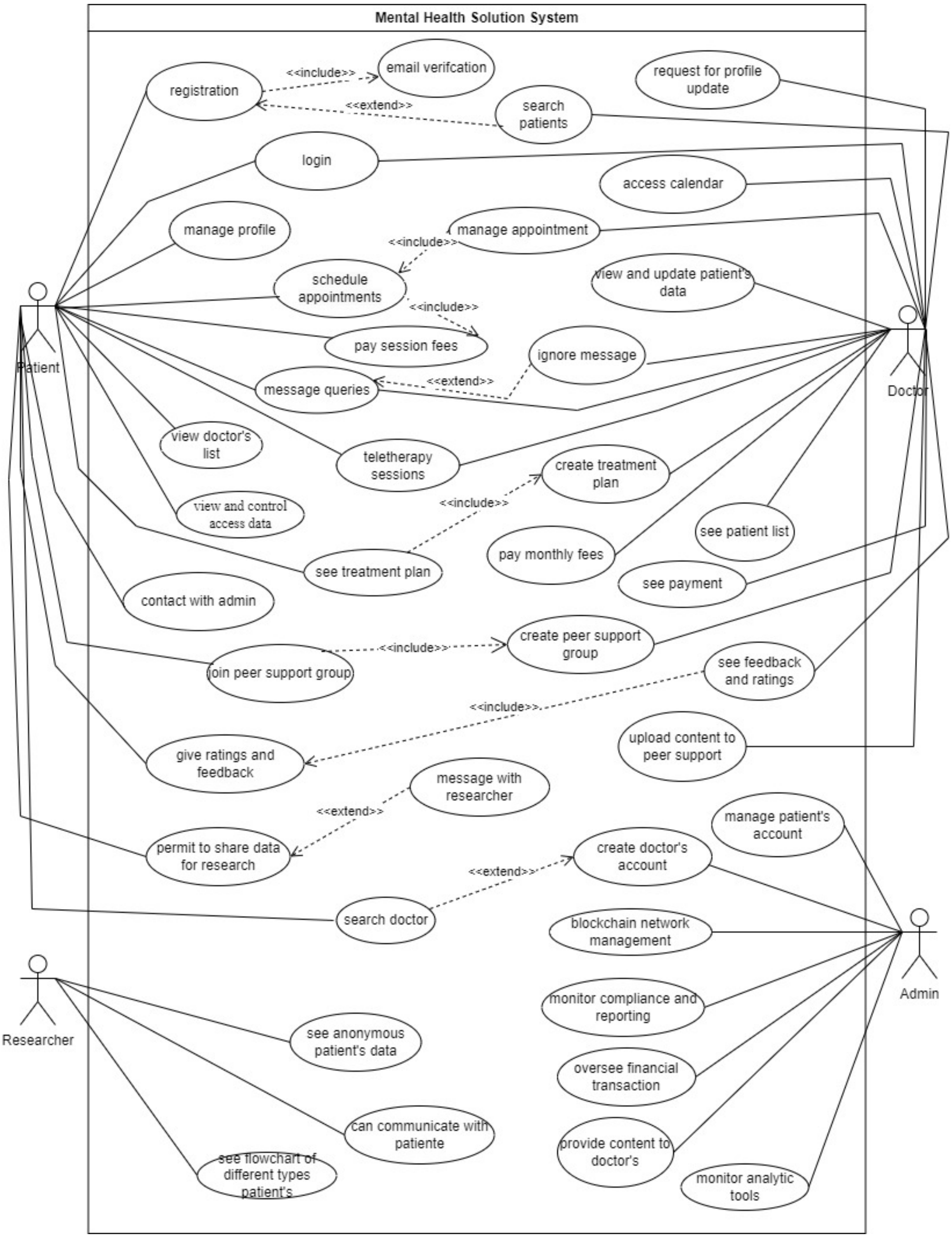

Figure 4.1: Use Case Diagram

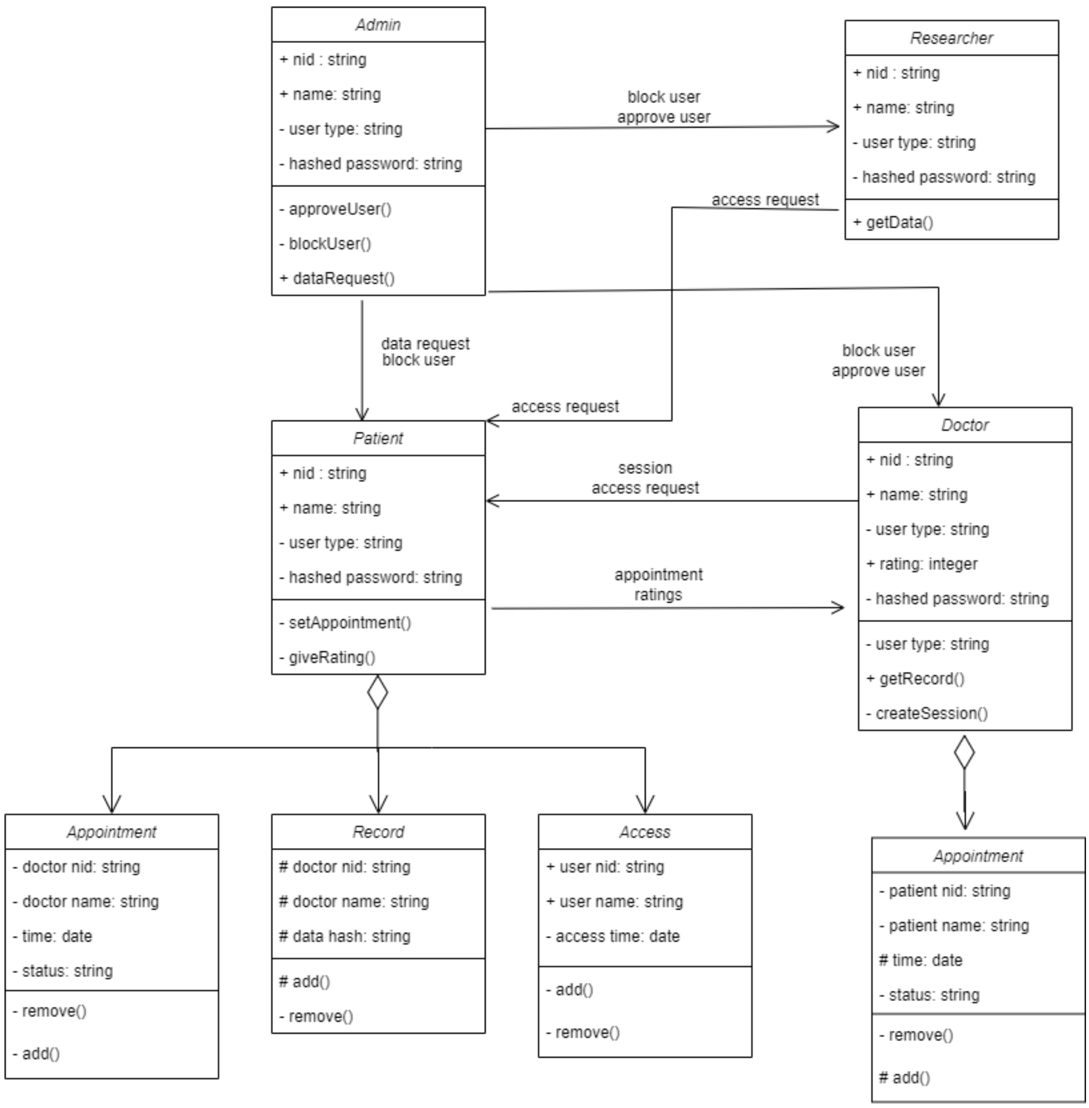

Figure 4.2: Class Diagram

duplication issue which creates an organized database. In (fig.4.3) the er diagram shows the logical structure of data storage.

4.4 Component Diagram

Component diagrams provide an in-depth analysis of the internal workings of a software system by illustrating its main parts and their connections. This makes it easier for us to comprehend the system's general design and the interactions between its many components such as how get appointment component is dependent on the other components more specific one is set appointment to fulfill the feature. It can also be utilized to prepare for expansion after deployment and encourages the reuse of code, makes maintenance easier, and gives the system more flexibility. (fig.4.4) depicts the backend components that makes the system.

4.5 Data Flow Diagram

DFD in (fig.4.5) shows visual representation of how data moves through the system, where the functions retrieve or set the data from which user and storage. This are able to pinpoint instances when data processing is not required and also highlight any security flaws or data discrepancies.

4.6 Context Diagram

The context diagram depicts the top view interactions between the users and the software that is illustrated in (fig.4.6). This helps to understand what this system is used for, its functionalities, what inputs are given by the users and in return what outputs are getting from the system.

4.7 Window Navigation Diagram

This provides an overall graphical interface view of the software to the end user before developing the software which helps us to build the software according to users' needs. How patients, doctors and

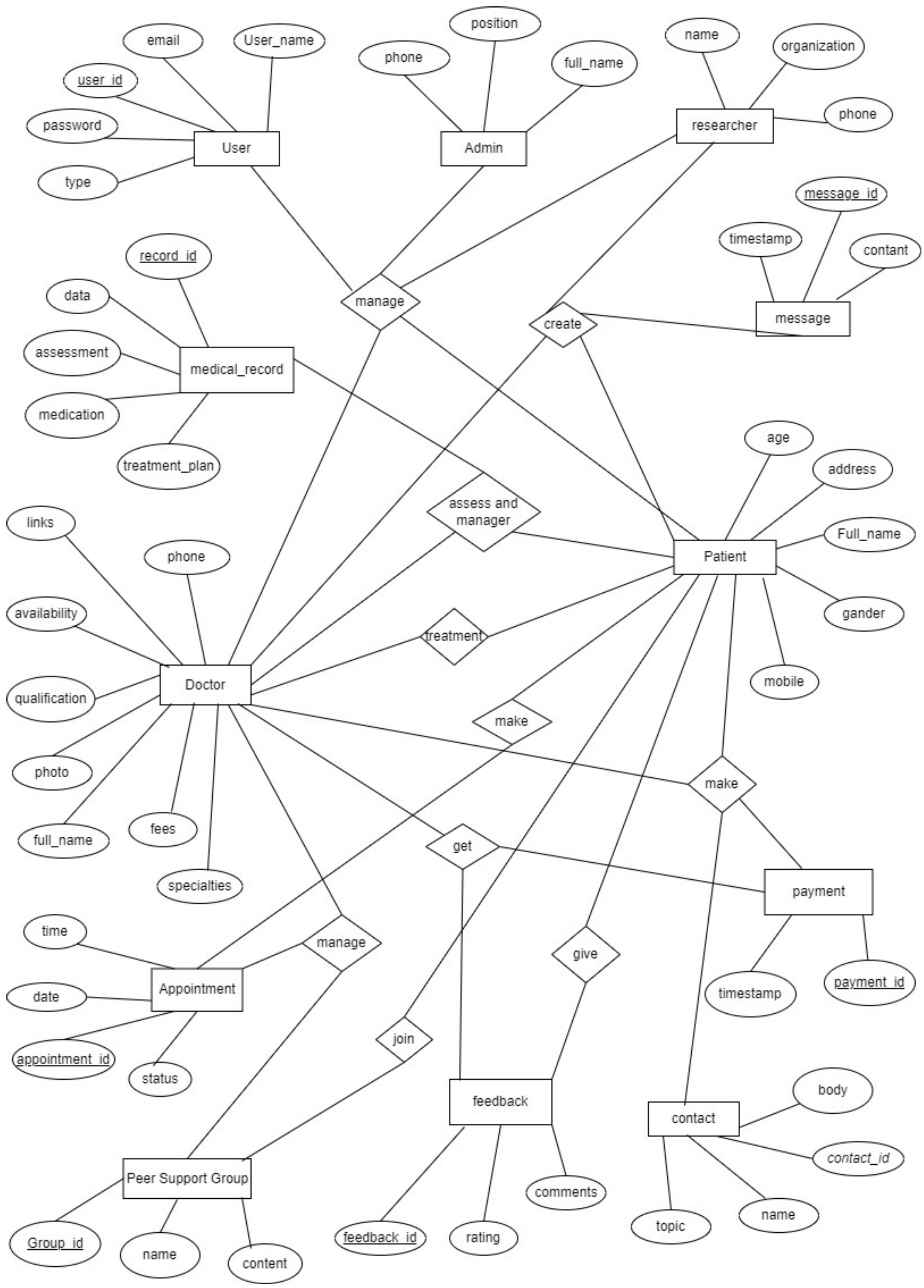

Figure 4.3: ER Diagram

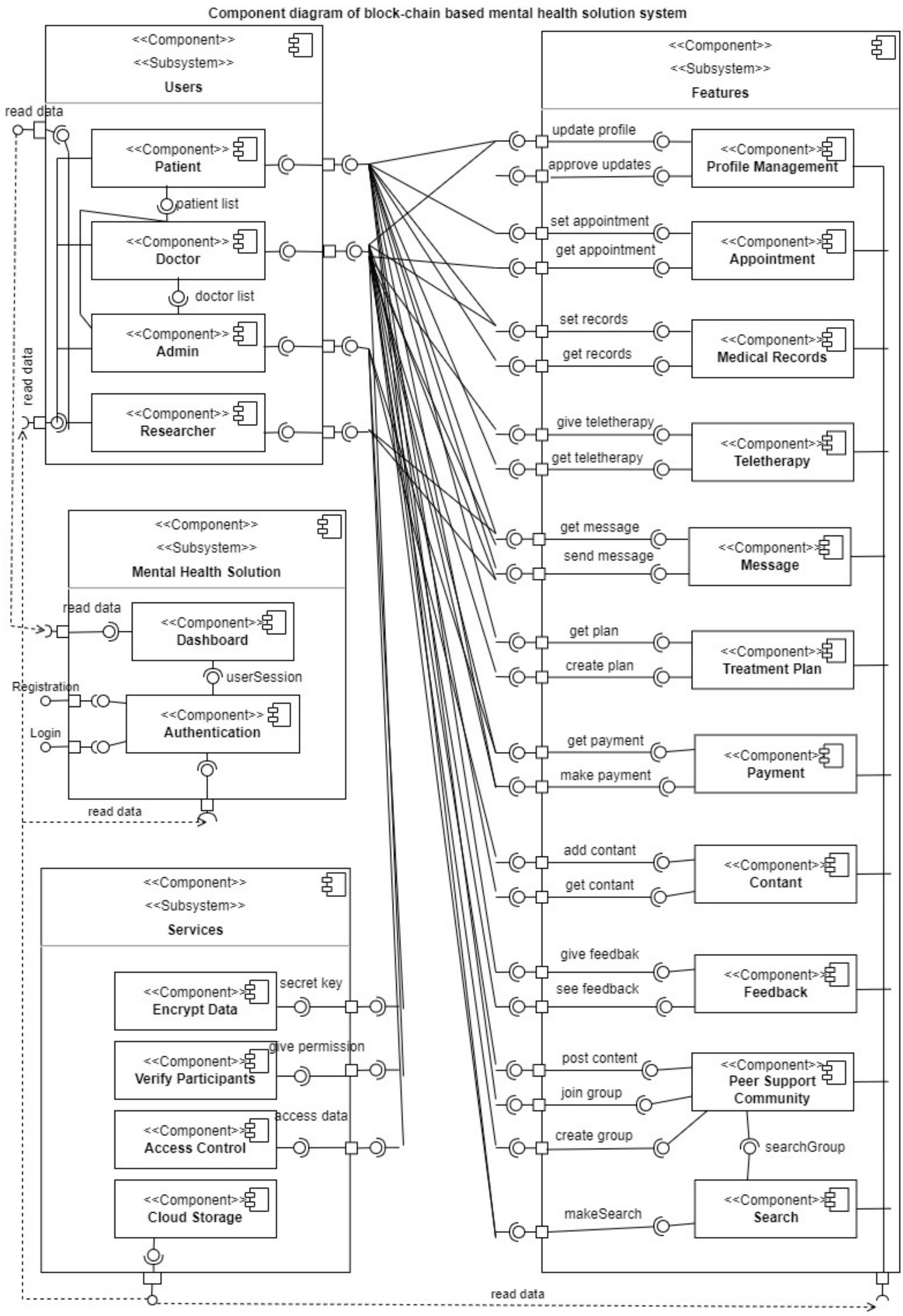

Figure 4.4: Component Diagram

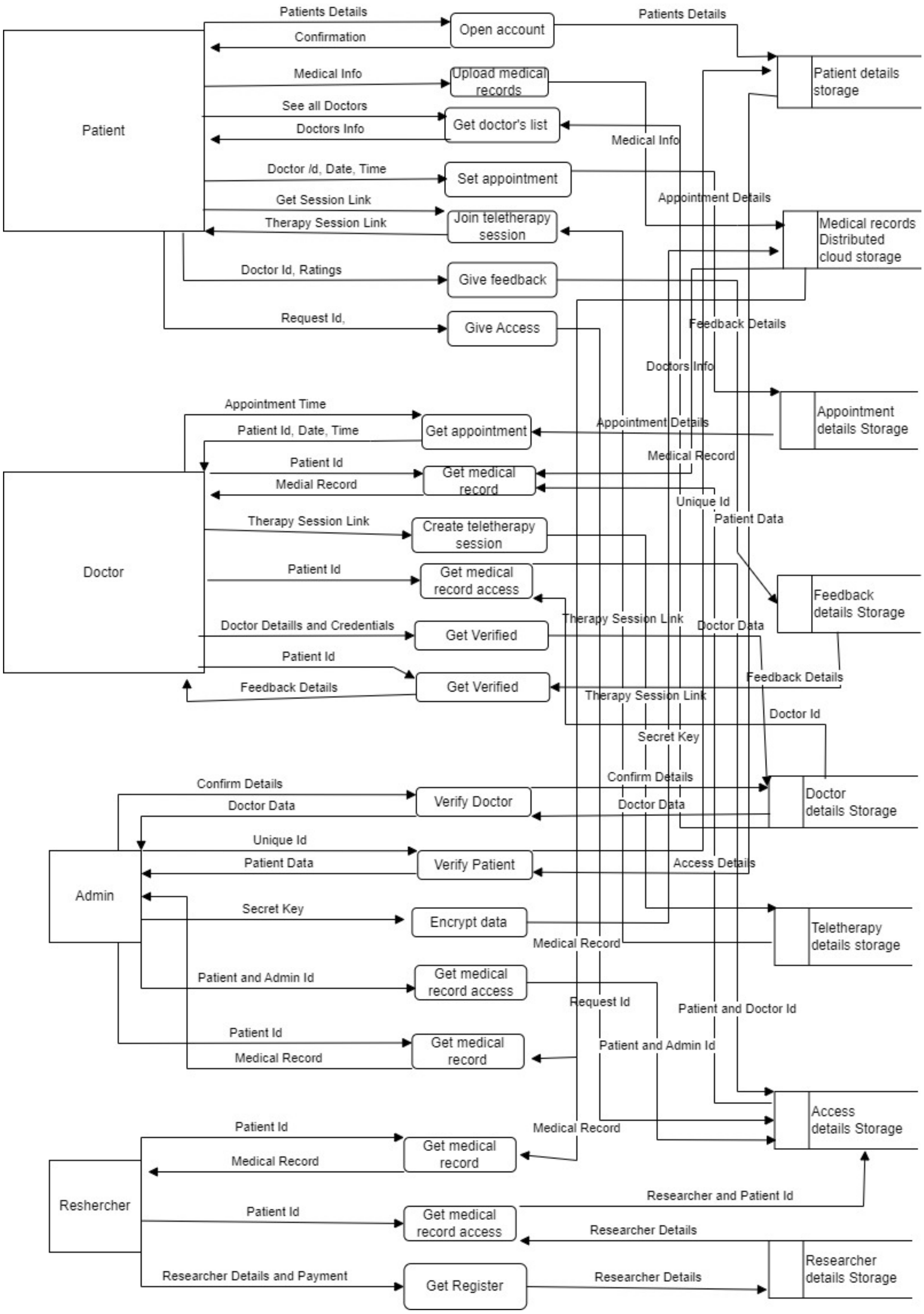

Figure 4.5: Data Flow Diagram

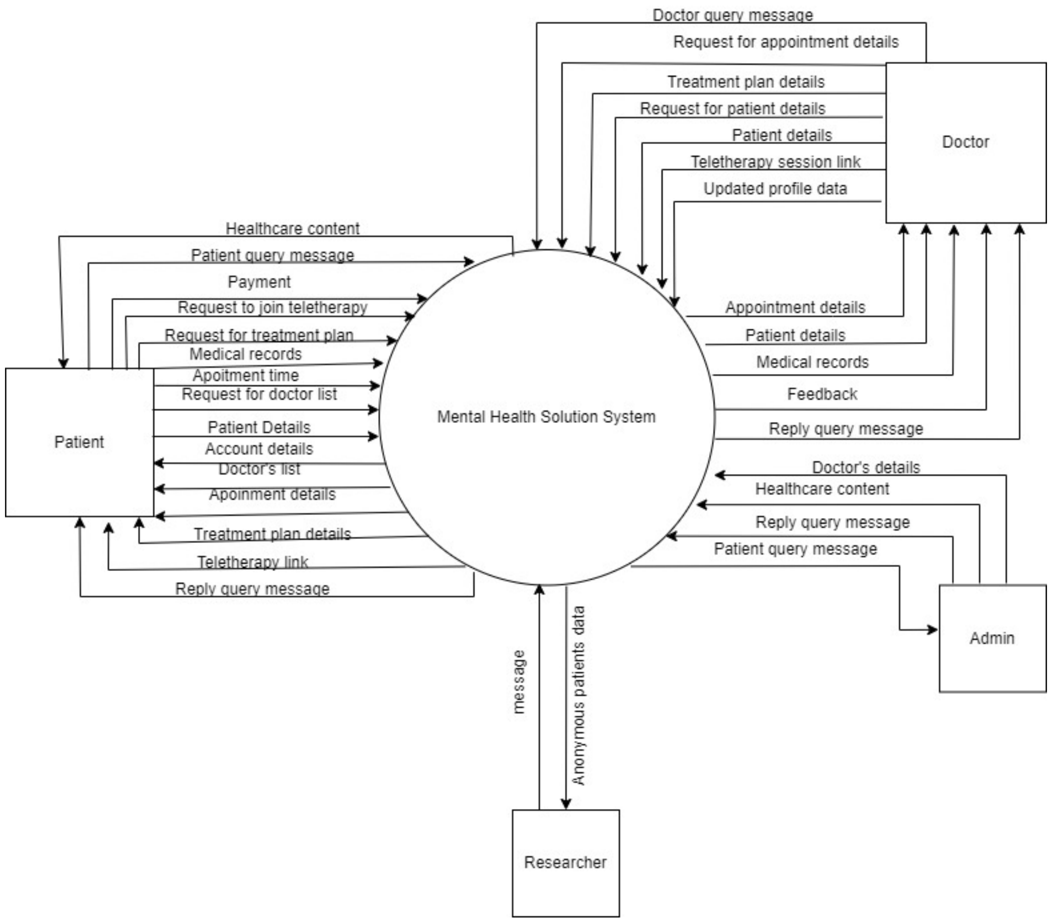

Figure 4.6: Context Diagram

authorities will see and use the system are shown in (fig.4.7), (fig.4.8), (fig.4.9) respectively.

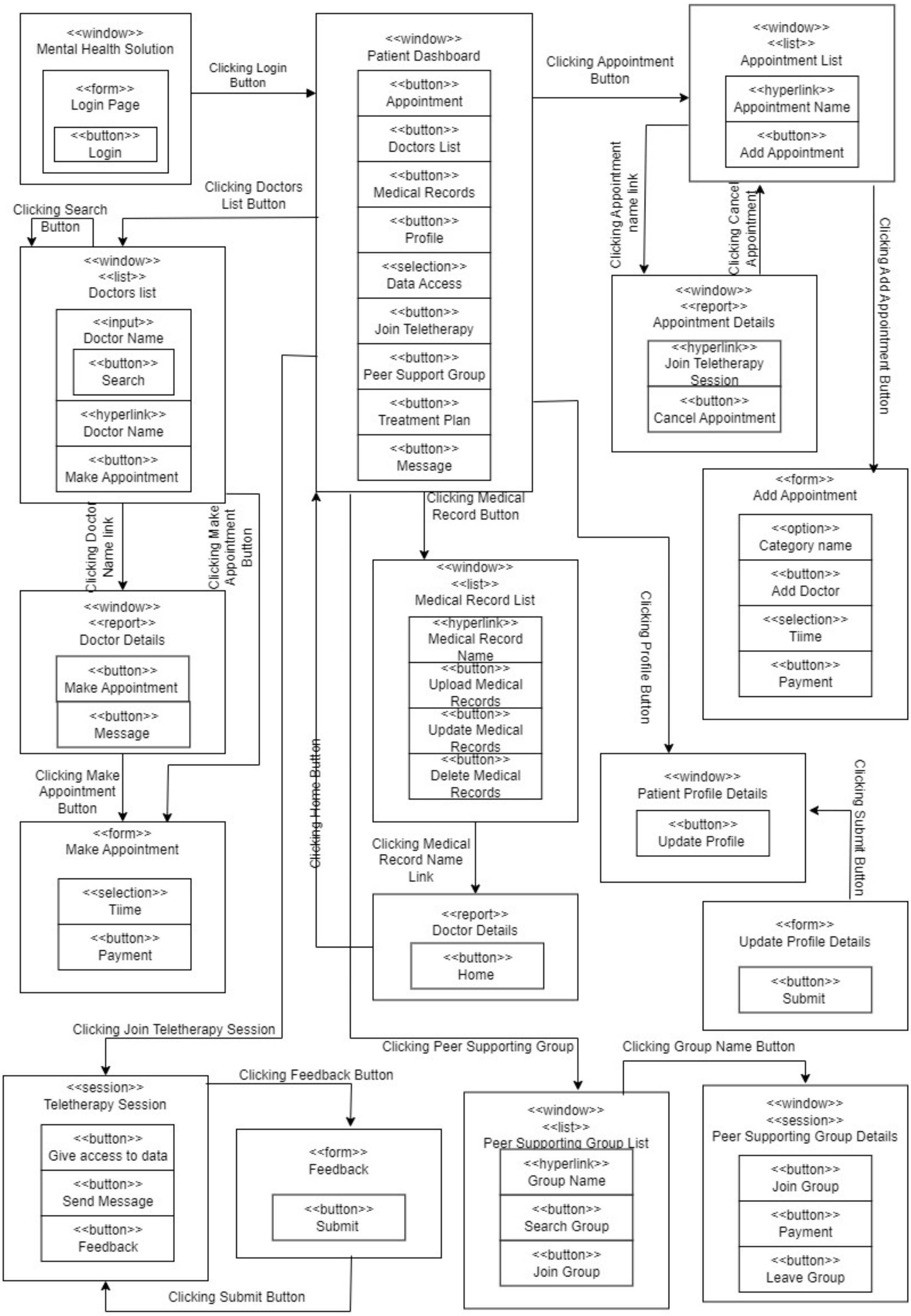

Figure 4.7: Window Navigation Diagram for Patient

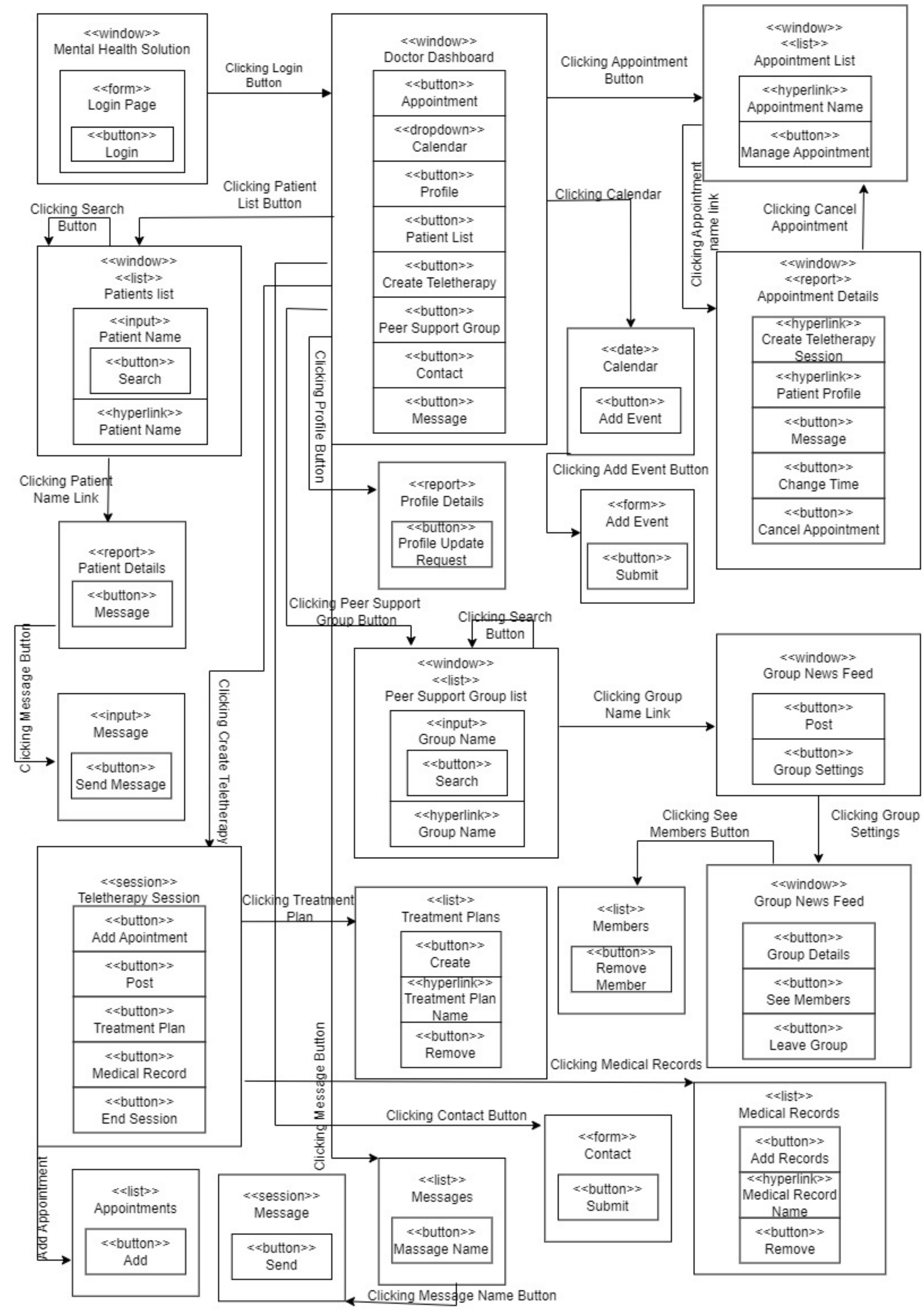

Figure 4.8: Window Navigation Diagram for Doctor

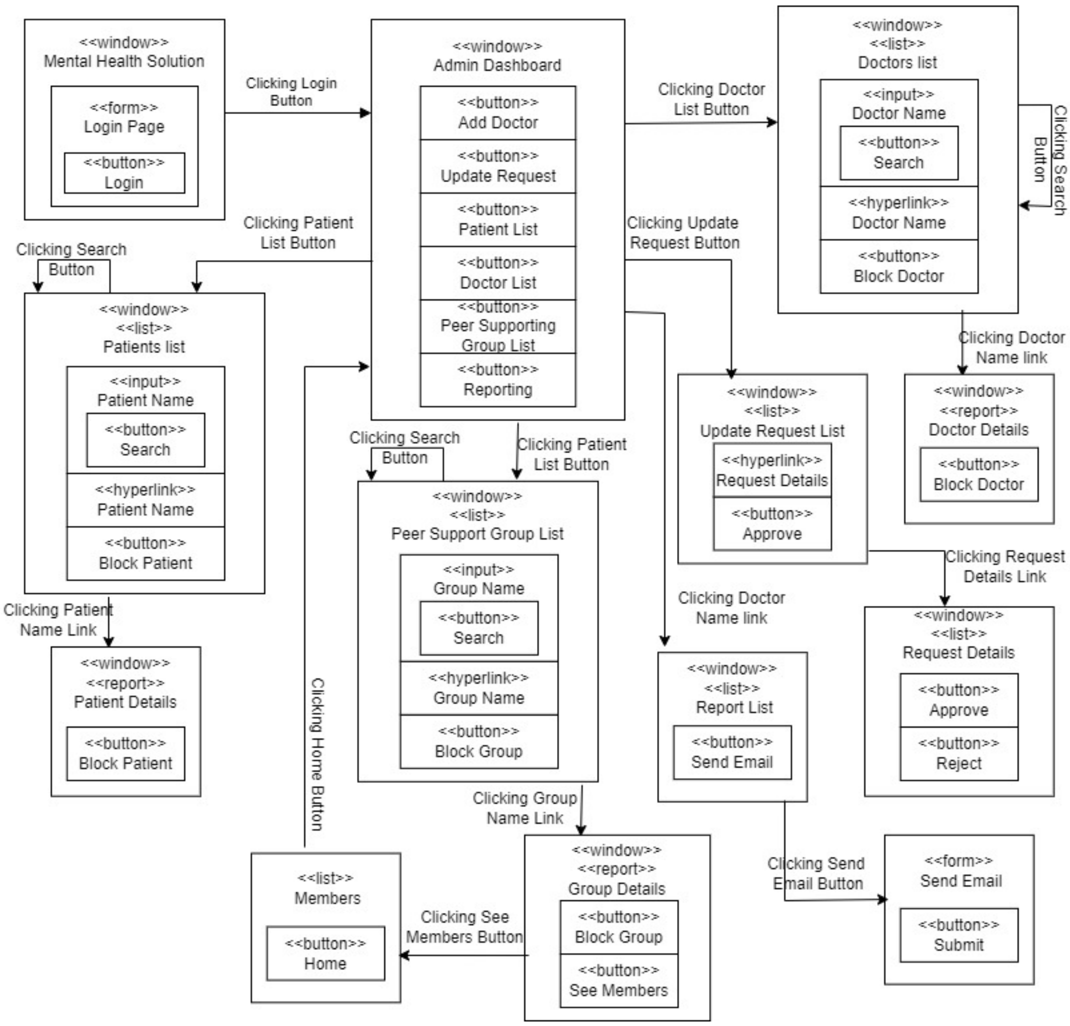

Figure 4.9: Window Navigation Diagram for Admin

Chapter 5

Project Development

5.1 Starting The fabric Network

To run the system we first have to start the private network this will add the organization peers who are responsible for endorsement and committing blocks. Then the chaincode will be deployed in the channel that was created. We have to start the network whenever we edit the chaincode. In (fig.5.1) the starting of the network and the commend to start is shown.

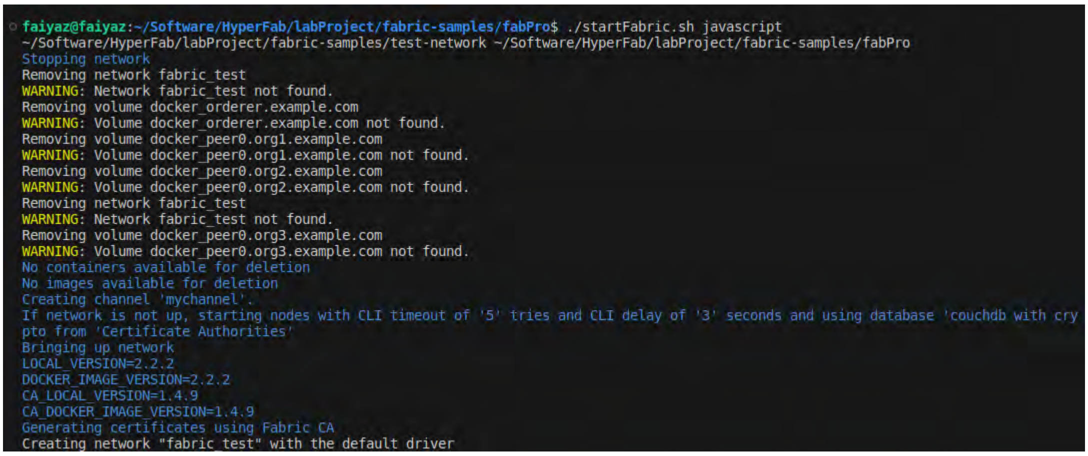

Figure 5.1: Starting Hyperladger Fabric Network

5.2 Register Admin

After starting the network we have to enroll the admin in organization peer for administrative work who will authorize rules and regulation in the network. And this will also create a wallet for the admin which stores the secret key. In (fig.5.2) displaying the admin registration.

Figure 5.2: Enrolling admin and creating wallet

5.3 Register User

This will create a user under organization. They will endorse, validate and commit transactions, also participate in the consensus process for a block. Registration of user in the network and creation of a wallet is illustrated in (fig.5.3).

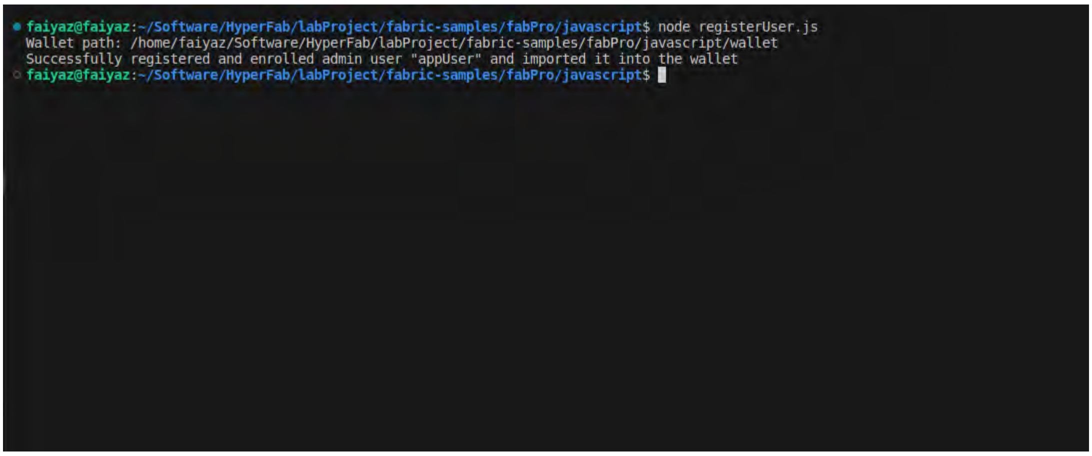

Figure 5.3: Enrolling user and creating wallet

5.4 Initial Ledger

In (fig.5.4), (fig.5.5) shows doctor, patient and admin's sample data that will be stored in the distributed system when chain code is uploaded on the network and these will become the initial ladger of fabric blockchain. (fig.5.6)All the data is stored using key value pair and key is the nid of the user.

```
class fabMed extends Contract {
    async initLedger(ctx) {
        console.info("============= START : Initialize Ledger ===========");
        const users = [
            {
                nid: "5104687630",
                name: "John Doe",
                email: "john.doe@gmail.com",
                phone: "01303940674",
                address: "Bangladesh Specialized Hospital, Shyamoli",
                degree: "MBBS, MCPS, MPHIL",
                website: "www.johndoe.com",
                specialization: "Brain, Drug Addiction, Sex",
                experience: "5 years",
                fees: "600",
                consultationStartTime: "17:00pm",
                consultationEndTime: "20:00pm",
                consultationDuration: "35",
                rating: 0,
                ratedPatientCount: 0,
                userType: "doctor",
                status: "approved",
                createdAt: "17/02/2021, 10:45",
                appointments: [],
                password:
                    "$2a$10$4i4cFW1y1EKp0gqYPl3jH.vbPr430T..l6MgWf.f.AaddQNeaK.WK
            },
            {
```

Figure 5.4: Sample data of doctor in chaincode

```
            {
                nid: "5104687636",
                name: "Admin01",
                email: "admin01@example.com",
                userType: "admin",
                status: "approved",
                createdAt: "01/01/2020",
                appointments: [],
                password:
                    "$2a$10$4i4cFW1y1EKp0gqYPl3jH.vbPr430T..l6MgWf.f.AaddQNeaK.WK",
            },
            {
                nid: "5104687638",
                name: "Patient01",
                email: "patient01@example.com",
                phone: "01911956372",
                userType: "patient",
                status: "approved",
                createdAt: "06/03/2023",
                appointments: [],
                records: [],
                dataAccess: [],
                password:
                    "$2a$10$4i4cFW1y1EKp0gqYPl3jH.vbPr430T..l6MgWf.f.AaddQNeaK.WK",
            },
            {
```

Figure 5.5: Sample data of admin and patient in chaincode

```
for (let i = 0; i < users.length; i++) {
    await ctx.stub.putState(
        users[i].nid,
        Buffer.from(JSON.stringify(users[i]))
    );
    console.info(
        `User ${users[i].name} type ${users[i].userType} is added`
    );
}
console.info("============= END : Initialize Ledger ===========");
```

Figure 5.6: Storing data as key value pair

5.5 Adding User

Doctors and researchers can apply to get a role in the app and they need admin's approval to access the system (fig.5.7). Patients only need to register with their nid number in order to use the benefit of the app (fig.5.8). In the blockchain how their data is stored are showed in (fig.5.9), (fig.5.10) of chain code.

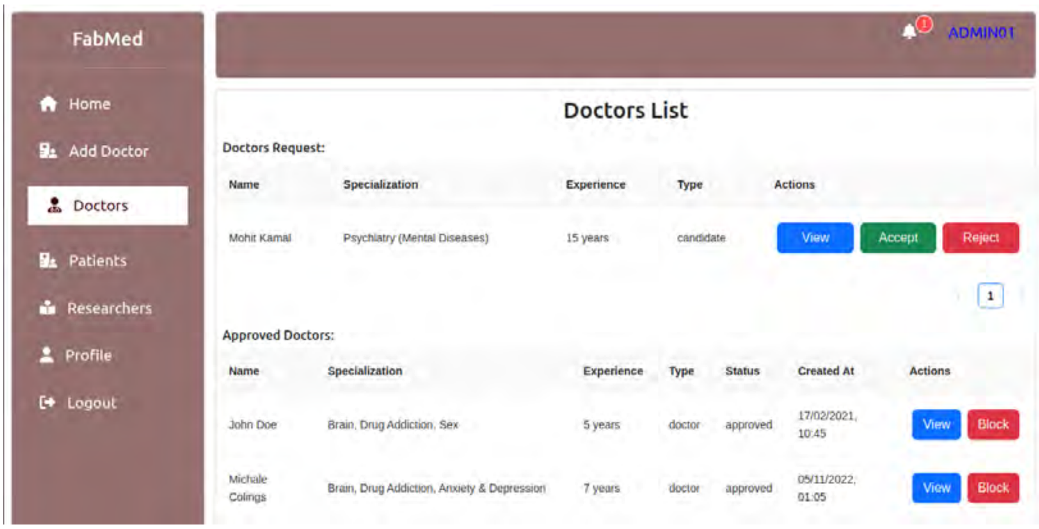

Figure 5.7: Doctor's list in the admin window

5.6 Appointment and Access Controle

In (fig.5.11) displays that appointment information for both patient and doctor is saved in the blockchain as well as for access list of patients medical record in patient's object (fig.5.12). Patient can add or remove access permission (fig.5.13).

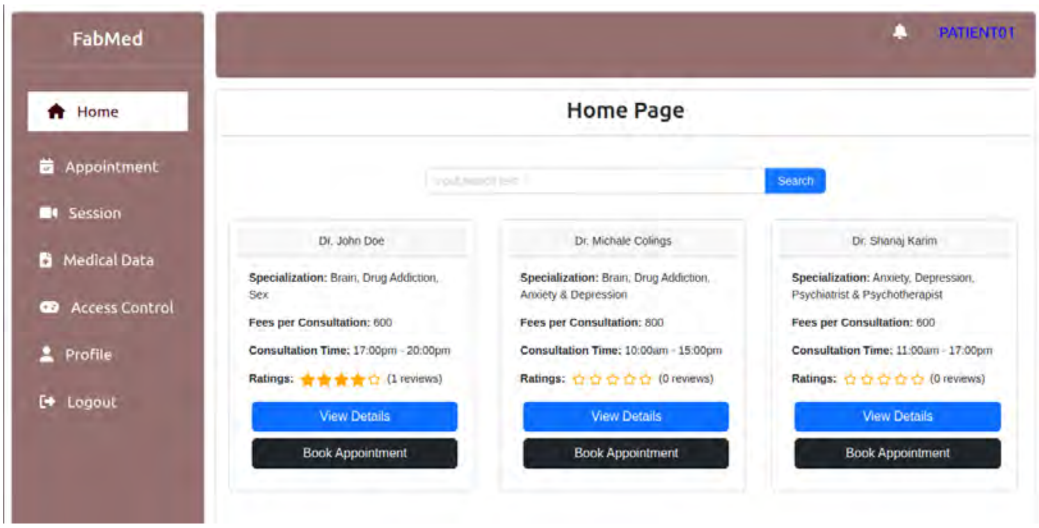

Figure 5.8: Doctor's list in the patient window

```
async storeDoctor(
    ctx, key, name, email, password, userType, phone, degree, address, website,
    specialization, experience, fees, consultationStartTime, consultationEndTime,
    consultationDuration, status, createdAt
) {
    try {
        console.info("============= START : Create Doctor ===========");

        const doctor = {
            ctx, key, name, email, password, userType, phone, degree, address, website,
            specialization, experience, fees, consultationStartTime, consultationEndTime,
            consultationDuration, status, createdAt, rating: 0, ratedPatientCount: 0,
            appointments: [],
        };

        await ctx.stub.putState(key, Buffer.from(JSON.stringify(doctor)));
        console.info("============= END : Create Doctor ===========");
    } catch (error) {
        console.log(error);
        return error;
    }
}
```

Figure 5.9: Chaincode of storing doctor

```
async storeResearcher(
    ctx, key, name, email, password, userType, phone, degree, address, status, createdAt
) {
    try {
        console.info("============= START : Create Desearcher ===========");

        const researcher = {
            nid: key, name, email, password, userType, phone, degree, address, status, createdAt,
        };

        await ctx.stub.putState(
            key,
            Buffer.from(JSON.stringify(researcher))
        );
        console.info("============= END : Create Researcher ===========");
    } catch (error) {
        console.log(error);
        return error;
    }
}
```

Figure 5.10: Chaincode of storing researcher

```
async storeAppointment(
    ctx, doctorKey, patientKey, doctorName, doctorEmail, doctorPhone,
    patientName, patientEmail, patientPhone, date, startTime,
    endTime, status, createdAt, sessionId
) {
    try {
        const doctorAsBytes = await ctx.stub.getState(doctorKey); // get the use
        const doctor = JSON.parse(doctorAsBytes.toString());
        const patientAsBytes = await ctx.stub.getState(patientKey); // get the u
        const patient = JSON.parse(patientAsBytes.toString());
        const appointment = {
            ctx, doctorKey, patientKey, doctorName, doctorEmail, doctorPhone,
            patientName, patientEmail, patientPhone, date, startTime,
            endTime, status, createdAt, sessionId
        };
        doctor.appointments.push(appointment);
        patient.appointments.push(appointment);

        await ctx.stub.putState(
            doctorKey,
            Buffer.from(JSON.stringify(doctor))
        );
        await ctx.stub.putState(
            patientKey,
            Buffer.from(JSON.stringify(patient))
        );
    } catch (error) {
        console.log(error);
        return error;
    }
```

Figure 5.11: Chaincode of storing appointments

```
async storeAccess(
    ctx, userKey, patientKey, userName, address, usertype, createdAt
) {
    try {
        const patientAsBytes = await ctx.stub.getState(patientKey); // get t
        const patient = JSON.parse(patientAsBytes.toString());
        const dataAccess = {
            userKey,
            userName,
            address,
            usertype,
            createdAt,
        };
        patient.dataAccess.push(dataAccess);
        await ctx.stub.putState(
            patientKey,
            Buffer.from(JSON.stringify(patient))
        );
    } catch (error) {
        console.log(error);
        return error;
    }
}
```

Figure 5.12: Chaincode of storing access list

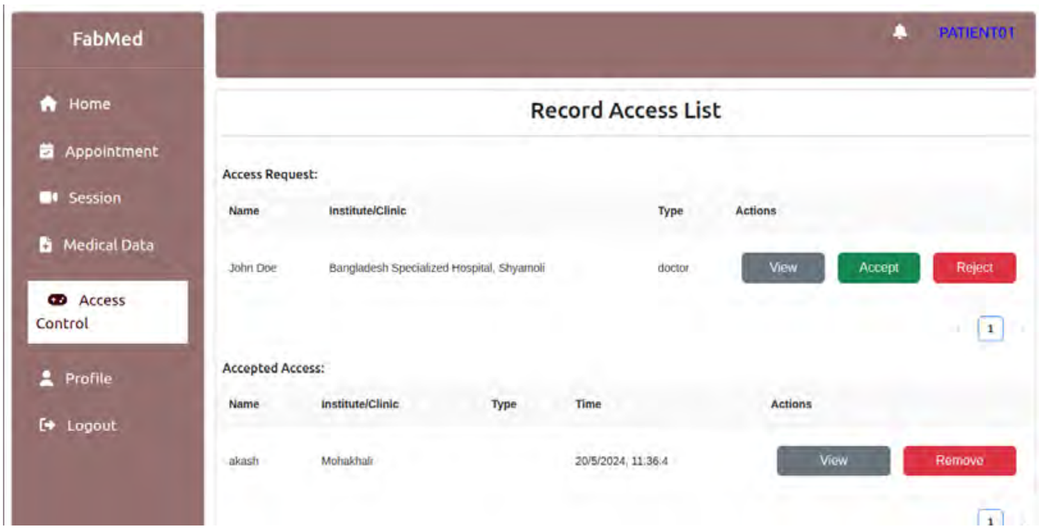

Figure 5.13: Access list patient view

5.7 Video Session

(fig.5.14) In the system only doctor can create sessions at the appointed time. After creating session both can join one on one video call (fig.5.15). The video session is developed using a third party app called zegocloud (fig.5.16).

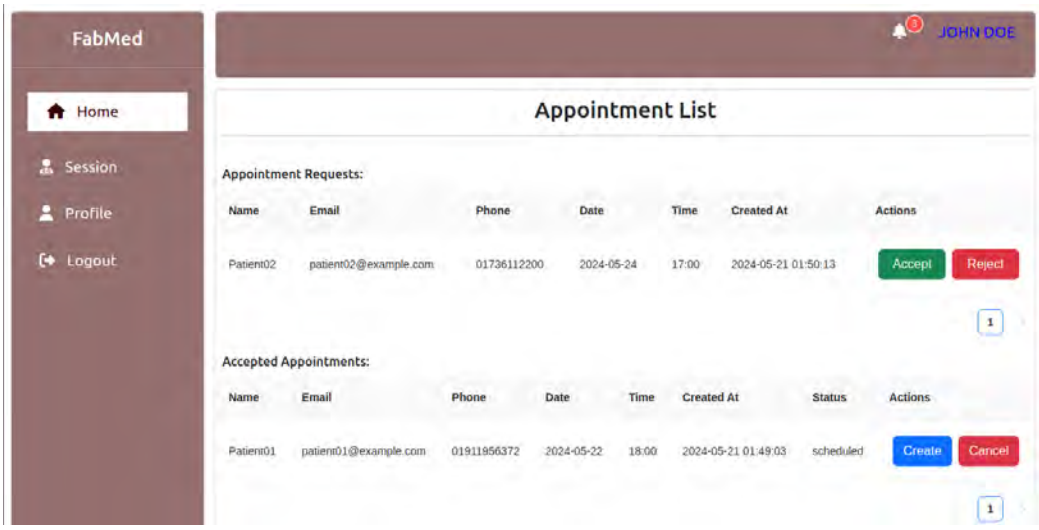

Figure 5.14: Creating session from doctor window

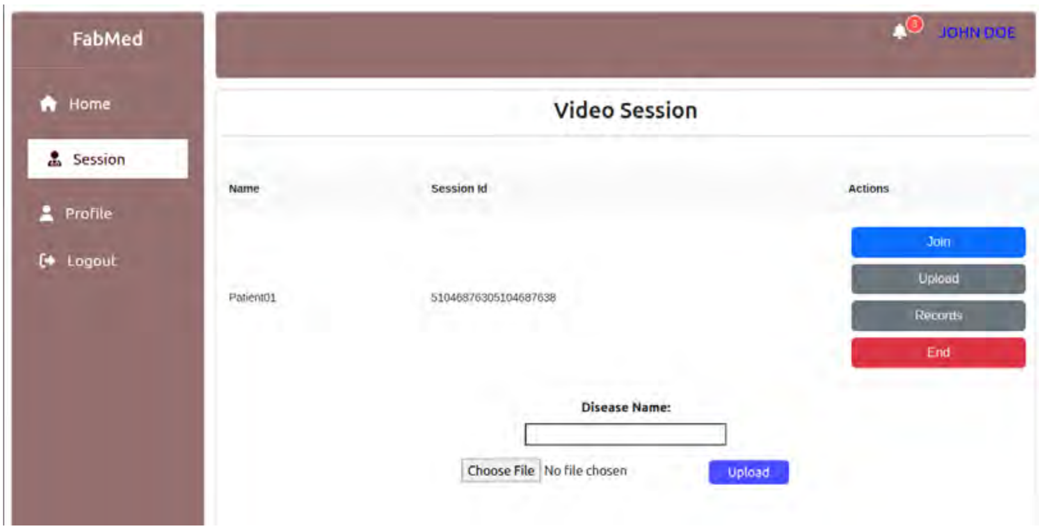

Figure 5.15: Join one in one video call

5.8 Confidential Record

Patients medical record are stored in the ipfs by encrypting the file (fig.5.17) and using the hash value the file can be retrieved (fig.5.18). And the encryption and decryption is done by crypto-js library. In

```
const session = async (element) => {
    const userNid = "3454645";
    const userName = "dfgef";
    const appID = 759841595;
    const serverSecret = "b48499a98bd3cc41ff2a1cfc073a07fa";
    const kitToken = ZegoUIKitPrebuilt.generateKitTokenForTest(
        appID,
        serverSecret,
        roomId,
        userNid,
        userName
    );
    const zc = ZegoUIKitPrebuilt.create(kitToken);
    zc.joinRoom({
        container: element,
        scenario: {
            mode: ZegoUIKitPrebuilt.OneONoneCall,
        },
        showPreJoinView: false,
    });
};
```

Figure 5.16: Building one on one video call

(fig.5.19) exhibits the chaincode of storing the hash of encrypted record or location of the record in ipfs. Only patient and doctor can upload medical record but for to access the data one have to request permission from patient (fig.5.20).

```
    const reader = new FileReader();

    reader.readAsText(file);
    reader.onload = async () => {
        const encryptedFile = crypto.AES.encrypt(
            reader.result,
            process.env.REACT_APP_SECRET_KEY
        ).toString();
        const blob = new Blob([encryptedFile], {
            type: fileType,
        });
        const fileData = new FormData();
        fileData.append("file", blob);
        const res = await axios({
            method: "post",
            url: "https://api.pinata.cloud/pinning/pinFileToIPFS",
            data: fileData,
            headers: {
                pinata_api_key:
                    process.env.REACT_APP_PINATA_API_KEY,
                pinata_secret_api_key:
                    process.env.REACT_APP_PINATA_API_SECRET,
                "Content-Type": fileType,
            },
        });
```

Figure 5.17: Uploading file to ipfs using pinata

```
const res = await axios({
    method: "get",
    url: `https://gateway.pinata.cloud/ipfs/${record.dataHash}`,
});
const decryptedFile = crypto.AES.decrypt(
    res.data,
    process.env.REACT_APP_SECRET_KEY
).toString(crypto.enc.Utf8);
const blob = new Blob([decryptedFile], {
    type: fileType,
});
const downloadLink = document.createElement("a");
downloadLink.href = URL.createObjectURL(blob);
downloadLink.setAttribute("download", record.fileName);
downloadLink.click();
```

Figure 5.18: Downloading file to ipfs using pinata

```
async storeRecord(
    ctx, doctorKey, patientKey, doctorName, disease, dataHash,
    fileName, createdAt
) {
    try {
        const patientAsBytes = await ctx.stub.getState(patientKey); // get
        const patient = JSON.parse(patientAsBytes.toString());
        const data = {
            ctx, doctorKey, patientKey, doctorName, disease, dataHash,
            fileName, createdAt
        };
        patient.records.push(data);
        await ctx.stub.putState(
            patientKey,
            Buffer.from(JSON.stringify(patient))
        );
    } catch (error) {
        console.log(error);
        return error;
    }
}
```

Figure 5.19: Storing data hash in the blockchain

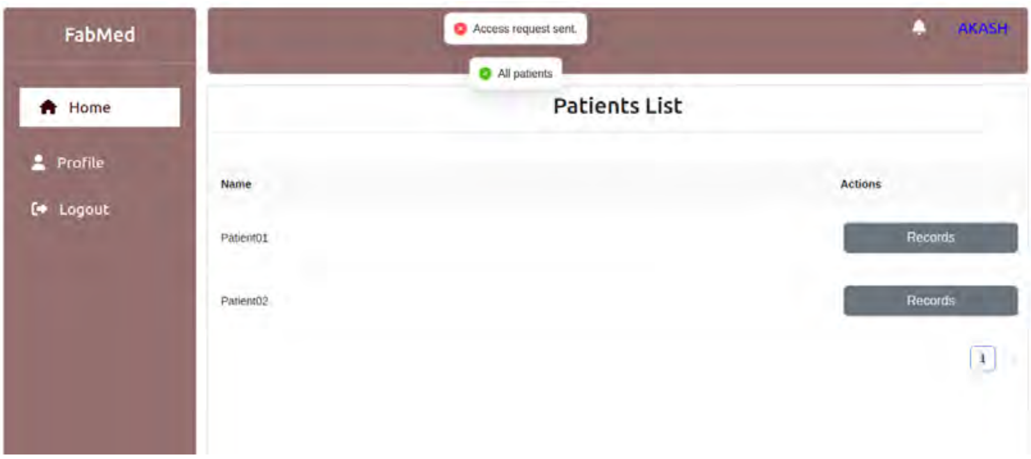

Figure 5.20: Accessing patient medical record by a researcher

5.9 Shutdown Network

This figure-5.21 describes how to shutdown the blockchain network. To update a chain code in the network we have to shutdown previous network then the network have to start again with the new updated chaincode.

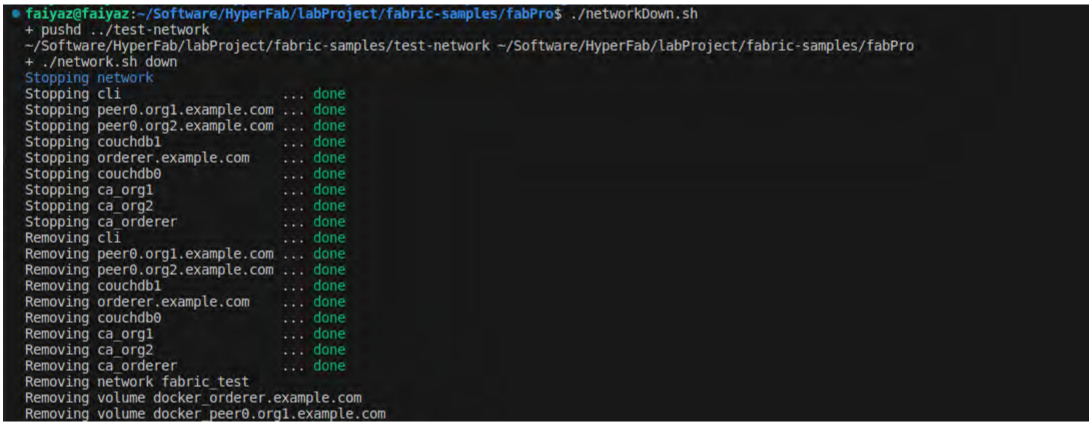

Figure 5.21: Shutting down Blockchain network

Chapter 6

Conclusion

Due to technological and digitalization of the world healthcare services like mental healthcare services are transforming into e-systems from physical systems. As a result there arrives a necessity to save ones' medical content securely and can control access over his data. All those things can be solved by our implemented Hyperladger fabric private blockchain system which offers trust environment by verifying doctors and patients, data security by storing and encrypting medical record using IPFS cloud, immutability by storing hash in blockchain and controlling access over medical records, solve mental treatment access barrier by teletherapy, increase quality treatment by review feature. In future we can further develop our project by improving secure sharing , safely storing the public and private key, increasing the quality of video therapy system and many more.

Bibliography

[1] G. P. Koocher, "Ethical challenges in mental health services to children and families," *wiley*, Apr. 2008. [Online]. Available: https://doi.org/10.1002/jclp.20476.

[2] N. D. V. QuanQiu Wang Rong Xu, "Increased risk of covid-19 infection and mortality in people with mental disorders: Analysis from electronic health records in the united states," *World Psychiatry*, Oct. 2020. [Online]. Available: https://doi.org/10.1002/wps.20806.

[3] T. Johannes, C. Andrew, F. Matthias, T. Oliver, and F. Frank, "Challenges for mental health services during the 2020 covid-19 outbreak in germany," *Psychiatry and clinical neurosciences*, 2020. [Online]. Available: https://doi.org/10.1111/pcn.13019.

[4] R. A. R. Kayla M. Theriault and T. G. Rhee, "Increasing emergency department visits for mental health conditions in the united states," *Clinical Psychaitry*, Jul. 2020. [Online]. Available: https://www.psychiatrist.com/jcp/ed-visits-for-mental-health-conditions-in-the-us/.

[5] K. V. R. Debra Houry Robin Kemball and N. J. Kaslow, "Intimate partner violence and mental health symptoms in african american female ed patients," *The American Journal of Emergency Medicine*, vol. 24, pp. 444–445, Jul. 2006. [Online]. Available: https://doi.org/10.1016/j.ajem.2005.12.026.

[6] S. S. Sarmah, "Understanding blockchain technology," *Academia*, pp. 23–29, 2018. DOI: 10.5923/j.computer.20180802.02.

[7] Immunebytes, "Pseudonymity and anonymity: Be untraceable in the blockchain world," *Immunebytes*, Jun. 2023. [Online]. Available: https://www.immunebytes.com/blog/pseudonymity-and-anonymity-be-untraceable-in-the-blockchain-world/#:~:text=In%20the%20context%20of%20blockchain,a%20person's%20real%2Dworld%20identity..

[8] Ibm, "Blockchain overview," *Ibm*, [Online]. Available: https://www.ibm.com/topics/blockchain.

[9] D. T. Y. Mahendra Kumar Shrivas, "The disruptive blockchain: Types, platforms and applications," *Texila International Journal of Academic*, 2018. DOI: 10.21522/TIJAR.2014.SE.19.02.Art003.

[10] A. Baliga, N. Solanki, S. Verekar, A. Pednekar, P. Kamat, and S. Chatterjee, "Performance characterization of hyperledger fabric," *IEEE*, Nov. 2018. [Online]. Available: https://doi.org/10.1109/CVCBT.2018.00013.

[11] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, and K. Christidis, "Hyperledger fabric: A distributed operating system for permissioned blockchains," *ACM Digital Library*, Apr. 2018. [Online]. Available: https://doi.org/10.1145/3190508.3190538.

[12] N. 1. Okkels, C. B. Kristiansen, P. Munk-Jørgensen, and N. Sartorius, "Urban mental health: Challenges and perspectives," *The American Journal of Emergency Medicine*, vol. 13, p. 3, May 2018. [Online]. Available: https://doi.org/10.1097/YCO.0000000000000413.

[13] V. Patel, G. S. Belkin, A. Chockalingam, J. C. S. Saxena, and J. Unützer, "Grand challenges: Integrating mental health services into priority health care platforms," *PLOS Medicine*, May 2013. [Online]. Available: https://doi.org/10.1371/journal.pmed.1001448.

[14] M. E. Stefl and D. C. Prosperi, "Barriers to mental health service utilization," *Community Mental Health*, vol. 21, p. 3, 1985. [Online]. Available: https://link.springer.com/article/10.1007/BF00754732.

[15] D. B. Saraceno, M. van Ommeren, R. Batniji, *et al.*, "Barriers to improvement of mental health services in low-income and middle-income countries," *The Lancet*, Sep. 2007. [Online]. Available: https://doi.org/10.1016/S0140-6736(07)61263-X.

[16] P. L. OWENS, K. HOAGWOOD, S. M. HORWITZ, *et al.*, "Barriers to children's mental health services," *The American Academy of Child Adolescent Psychiatry*, vol. 41, pp. 731–749, Jun. 2002. [Online]. Available: https://doi.org/10.1097/00004583-200206000-00013.

[17] M. D. Venegas, J. M. Brooks, A. L. Myers, M. Storm, and K. L. Fortuna, "Peer support specialists and service users' perspectives on privacy, confidentiality, and security of digital mental health," *IEEE*, vol. 21, pp. 41–50, Mar. 2022. [Online]. Available: https://doi.org/10.1109/MPRV.2022.3141986.

[18] N. Shen, L. Sequeira, M. P. Silver, A. Carter-Langford, J. Strauss, and D. Wiljer, "Patient privacy perspectives on health information exchange in a mental health context: Qualitative study," *JMIR Publication*, vol. 6, p. 11, Nov. 2019. [Online]. Available: https://preprints.jmir.org/preprint/13306?__hstc=102212634.f98a080e0988727088670c8a7b0a5ea7.1707637818927.1707637818927.1707637818927.1&__hssc=102212634.2.1707637818930&__hsfp=359042293.

[19] L. H. Andrade, A. and. Mneimneh, Wells, *et al.*, "Barriers to mental health treatment: Results from the who world mental health surveys," *Cambridge University Pres*, Aug. 2013. [Online]. Available: https://doi.org/10.1017/S0033291713001943.

[20] R. B.-C. Javier Bartolomei, D. Framorando, F. Kasina, N. Premand, A. Eytan, and Y. Khazaal, "What are the barriers to access to mental healthcare and the primary needs of asylum seekers? a survey of mental health caregivers and primary care workers," Sep. 2016. [Online]. Available: https://bmcpsychiatry.biomedcentral.com/articles/10.1186/s12888-016-1048-6.

[21] N. C. Coombs, W. E. Meriwether, J. Caringi, and S. R. Newcomer, "Barriers to healthcare access among u.s. adults with mental health challenges: A population-based study," *SSM - Population Health*, vol. 15, Sep. 2021. [Online]. Available: https://doi.org/10.1016/j.ssmph.2021.100847.

[22] D. D. M. Kathleen Rowan and L. A. Blewett, "Access and cost barriers to mental health care, by insurance status," *Health Affairs*, vol. 32, Oct. 2013. [Online]. Available: https://doi.org/10.1377/hlthaff.2013.0133.

[23] A. Pomerantz, B. H. Cole, B. V. Watts, and W. B. Weeks, "Improving efficiency and access to mental health care: Combining integrated care and advanced access," *General Hospital Psychiatry*, Dec. 2008. [Online]. Available: https://doi.org/10.1016/j.genhosppsych.2008.09.004.

[24] C. U. Pres, "Stigma and discrimination limit access to mental health care," May 2011. [Online]. Available: https://www.cambridge.org/core/journals/epidemiology-and-psychiatric-sciences/article/stigma-and-discrimination-limit-access-to-mental-health-care/2FA22511D1878BA80162D7FDD891C00A.

[25] A. C. Enthoven, "Integrated delivery systems: The cure for fragmentations," *The American Journal of Managed Care*, vol. 15, Dec. 2009. [Online]. Available: https://doi.org/10.1017/S0033291713001943.

[26] V. B. A Maris H van Gaalen, "A legislative amendment within dutch mental healthcare increases the administrative burden: A follow-up study," 2022.

[27] S.-W. Noh, Y. Park2, C. Sur3, S.-U. Shin2, and K.-H. Rhee2, "Blockchain-based user-centric records management system," *International Journal of Control and Automation*, vol. 10, pp. 133–144, 2017. [Online]. Available: http//dx.doi.org/10.14257/ijca.2017.10.11.12.

[28] T. A. Naqishbandi, E. S. Mohammed, S. Venkatesan, A. Sonya, K. Cengiz, and Y. Banday, "Secure blockchain-based mental healthcare framework:—a paradigm shift from traditional to advanced analytics," vol. 133, Jul. 2022. [Online]. Available: https://link.springer.com/chapter/10.1007/978-3-031-04613-1_12.

[29] S. D. Yi Chen, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," *Journals of Medical Systems*, vol. 43, Nov. 2018. [Online]. Available: https://link.springer.com/article/10.1007/s10916-018-1121-4.

[30] A. Dubovitskaya, P. Novotny, Z. Xu, and F. Wang, "Applications of blockchain technology for data-sharing in oncology: Results from a systematic literature review," *Oncology*, Dec. 2019. [Online]. Available: https://www.scienceopen.com/document?vid=598b8749-9e85-4b39-83f8-b4dfbd888b32.

[31] M. S. Sadia Suhail Usmani and M. Mehendale, "Future of mental health in the metaverse," Jul. 2022. [Online]. Available: https://doi.org/10.1136%2Fgpsych-2022-100825.

[32] P. P. Ray, N. Kumar, and D. Dash, "Blwn: Blockchain-based lightweight simplified payment verification in iot-assisted e-healthcare," *IEEE*, vol. 15, pp. 134–145, Mar. 2021. [Online]. Available: https://doi.org/10.1109/JSYST.2020.2968614.

[33] M. D. Dinh C. Nguyen Pubudu N. Pathirana and A. Seneviratne, "Blockchain for secure ehrs sharing of mobile cloud based e-health systems," *IEEE*, vol. 7, pp. 66 792–66 806, May 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2917555.

[34] D. D. Taralunga and B. C. Florea, "A blockchain-enabled framework for mhealth systems," *Sensors and Biomedical Signal Processing for Patient Monitoring*, 2021. [Online]. Available: https://doi.org/10.3390/s21082828.

[35] 1. S.-E.-M. Farjana Khanam Nishi, M. M. Khan, A. Alsufyani, S. Bouroui, P. Guptav, and D. K. Saini, "Electronic healthcare data record security using blockchain and smart contract," May 2022. [Online]. Available: https://doi.org/10.1155/2022/7299185.

[36] C. C. W. oh Chee Ming, "Electronic medical record system using ethereum blockchain and role-based access control," *UTHM*, vol. 2, Nov. 2021. [Online]. Available: https://doi.org/10.30880/aitcs.2021.02.02.004.

[37] C. A. d. C. Tiago Quaini Alex Roehrs and R. da Rosa Righi, "A model for blockchain-based distributed electronic health records," *IADIS International Journal*, vol. 16, pp. 66–79, 2018. [Online]. Available: https://www.iadisportal.org/ijwi/papers/2018161205.pdf.

[38] M. M. Madine, A. A. Battah, I. Yaqoob, and K. Salah, "Blockchain for giving patients control over their medical records," *IEEE*, vol. 8, Oct. 2020. [Online]. Available: https://doi.org/10.1109/ACCESS.2020.3032553.

[39] N. Andola, Raghav, S. Prakash, S. Venkatesan, and S. Verma, "Shemb:a secure approach for healthcare management system using blockchain," *IEEE*, Apr. 2021. [Online]. Available: https://doi.org/10.1109/CICT48419.2019.9066237.

[40] H. R. Hasan, K. Salah, R. Jayaraman, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-enabled telehealth services using smart contracts," *IEEE*, vol. 9, pp. 151 944–151 959, Nov. 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3126025.

[41] U. Q. Ayesha Shahnaz and A. Khalid, "Using blockchain for electronic health records," *IEEE*, vol. 7, pp. 147 782–147 795, Oct. 2019. [Online]. Available: https://doi.org/10.1109/ACCESS.2019.2946373.

[42] A. Nedaković, A. Hasselgren, K. Kralevska, and D. Gligoroski, "Hyperledger fabric platform for healthcare trust relations—proof-of-concept," *Blockchain: Research and Applications*, vol. 4, Dec. 2023. [Online]. Available: https://doi.org/10.1016/j.bcra.2023.100156.

[43] M. Scherer, "Performance and scalability of blockchain networks and smart contracts," 2017. [Online]. Available: https://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1111497&dswid=5496.

[44] L. G. Christian Gorenflo Stephen Lee and S. Keshav, "Fastfabric: Scaling hyperledger fabric to 20 000 transactions per second," *International journal of Network Management*, vol. 68, Feb. 2020. [Online]. Available: https://doi.org/10.1002/nem.2099.

[45] C. Stamatellis, P. Papadopoulos, N. Pitropakis, S. Katsikas, and W. J. Buchanan, "A privacy-preserving healthcare framework using hyperledger fabric," *Sensors*, Nov. 2020. [Online]. Available: https://doi.org/10.3390/s20226587.

[46] S. C. Mahender Kumar, "Medhypchain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in covid-19 pandemic," *Journal of Network and Computer Applications*, vol. 179, Apr. 2021. [Online]. Available: https://doi.org/10.1016/j.jnca.2021.102975.

[47] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. H. ur Rehman, and C. A. Kerrache, "The case of hyperledger fabric as a blockchain solution for healthcare applications," *Blockchain: Research and Applications*, vol. 2, Mar. 2021. [Online]. Available: https://doi.org/10.1016/j.bcra.2021.100012.

[48] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, Dec. 2021. [Online]. Available: https://doi.org/10.1016/j.comnet.2021.108500.

[49] M. Uddin, M. andIrfana Memon, I. Ali, J. Memon, M. Abdelhaq, and R. Alsaqour, "Hyperledger fabric blockchain: Secure and efficient solution for electronic health records," *Computers, Materials Continua*, vol. 68, Feb. 2021. [Online]. Available: http://dx.doi.org/10.32604/cmc.2021.015354.