A Report on

Implementation of EHR System Through Hyperledger Fabric

Submitted by

Ajit Patil

Krishna Mane

Vishal Waghmare

Prathmesh Mali

Under The Guidance of

Prof. N. M. Sawant

For The Award of The Degree of

Bachelor of Engineering

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SKN SINHGAD COLLEGE OF ENGINEERING

PUNYASHLOK AHILYADEVI HOLKAR SOLAPUR UNIVERSITY, SOLAPUR

2022-2023

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SKN Sinhgad College of Engineering, Korti, Pandharpur.

__(Accredited by NAAC 'A+' Grade)__

__CERTIFICATE__

This is to certify that, the design report entitled

"Implementation of EHR System through Hyperledger Fabric"

Submitted by

__Ajit Patil__

__Krishna Mane__

__Vishal Waghmare__

__Prathmesh Mali__

In the partial fulfillment for the award of the Degree of

BACHELOR OF ENGINEERING

This work is a record of student's own work carried out by them under our supervision and guidance during the academic year

__2022-2023__

Prof. N. M. Sawant
Project Guide

Prof. R. S. Yevale
Project Coordinator

Prof. S. V. Pingale
Head of Department

External Examiner

Acknowledgment

We would like to express our deep sense of gratitude to our **HOD Prof. S. V. Pingale** for his valuable guidance during the project. We are also thanks to our guide **Prof. N. M. Sawant** for constantly encouraging us by giving critics on our work. We express gratitude towards Project Coordinator, **Prof. R. M. Yevale** for providing the support, valuable time and priceless suggestions. We also express gratitude towards our all teaching and non-teaching staff, family members and our Friends for encouraging us with their valuable suggestions and motivating us from time to time.

Mr. Ajit Patil
Mr. Krishna Mane
Mr. Vishal Waghmare
Mr. Prathmesh Mali

Declaration

We, the undersigned hereby declare that the project design report entitled **"Implementation of EHR System through Hyperledger Fabric"** submitted by us to SKN Sinhgad College of Engineering, Korti, Pandharpur for the B.Tech (Final Year) in Computer Science and Engineering, under the guidance of Prof N. M. Sawant.

We further declare that to the best of our knowledge and belief, this work has not been submitted to this or any other university.

Mr. Ajit Patil
Mr. Krishna Mane
Mr. Vishal Waghmare
Mr. Prathmesh Mali

Abstract

The healthcare industry deals with highly sensitive data which must be managed in a secure way. Electronic Healthcare Records hold sensitive data of patient which should store and shared securely. However, the public release of this highly sensitive personal data poses serious privacy and security threats to patients and healthcare service providers. Hence, we foresee the requirement of new technologies to address the privacy and security challenges for personal data in healthcare applications. Blockchain is one of the promising solutions, aimed to provide transparency, security, and privacy using consensus-driven decentralized data management on top of peer-to-peer distributed computing systems. Our solution explores the potential use of Hyperledger Fabric in healthcare industry. With such permissioned blockchain system solution for storing and sharing healthcare record, the patient will have full control on their medical information and authorize the doctors that can view medical records by grant and revoke access mechanism.

Contents

Chapter 1

Introduction

1.1 What is EHR ?

- **Drop-out:** An electronic medical record (EMR) is an electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within one health care organization. **Types of Health Record:**
  1) PHR: A personal health record, or PHR, is an electronic application through which patients can maintain and manage their health information (and that of others for whom they are authorized) in a private, secure, and confidential environment.
  2) EMR: An electronic medical record (EMR) is a digital version of all the information you'd typically find in a provider's paper chart: medical history, diagnoses, medications, immunization dates, allergies, lab results and doctor's notes within one health care organization.
  3) EHR: An electronic health record (EHR) is a digital version of a patient's paper chart. EHRs are real-time, patient-centered records that make information available instantly and securely to authorized users.

1.2 Problems with current EMR systems:

The healthcare industry still seems to be an easy target for hackers and this is due to the lack of technological understanding within the industry. The recent attacks on the healthcare industry are the evidence of data security challenges in this sector. The target attacks include, but not limited to, phishing attacks and ransomware which are successful in retrieving personal data. In fact, the high success rate of ransomware attacks has shown the lack of basic security measures such as backup and system updates. Healthcare applications like EMR are very sensitive as they directly involve personal and critical data, which must be secured from unauthorized access.

1.3 Blockchain

Blockchain is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system. A blockchain is essentially a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. Each block in the chain contains a number of transactions, and every time a new transaction occurs on the blockchain, a record of that transaction is added to every participant's ledger. The decentralised database managed by multiple participants is known as Distributed Ledger Technology (DLT).

1.4 Types of Blockchain:

1) Public Blockchain: Public blockchains are permissionless in nature, allow anyone to join, and are completely decentralized. Public blockchains allow all nodes of the blockchain to have equal rights to access the blockchain, create new blocks of data, and validate blocks of data.
2) Private Blockchain: Private blockchains, which may also be referred to as managed blockchains, are permissioned blockchains controlled by a single organization. In a private blockchain, the central authority determines who can be a node.
3) Consortium Blockchain: Consortium blockchains are permissioned blockchains governed by a group of organizations, rather than one entity, as in the case of the private blockchain. Consortium blockchains, therefore, enjoy more decentralization than private blockchains, resulting in higher levels of security.
4) Hybrid Blockchain: Hybrid blockchains are blockchains that are controlled by a single organization, but with a level of oversight performed by the public blockchain, which is required to perform certain transaction validations.

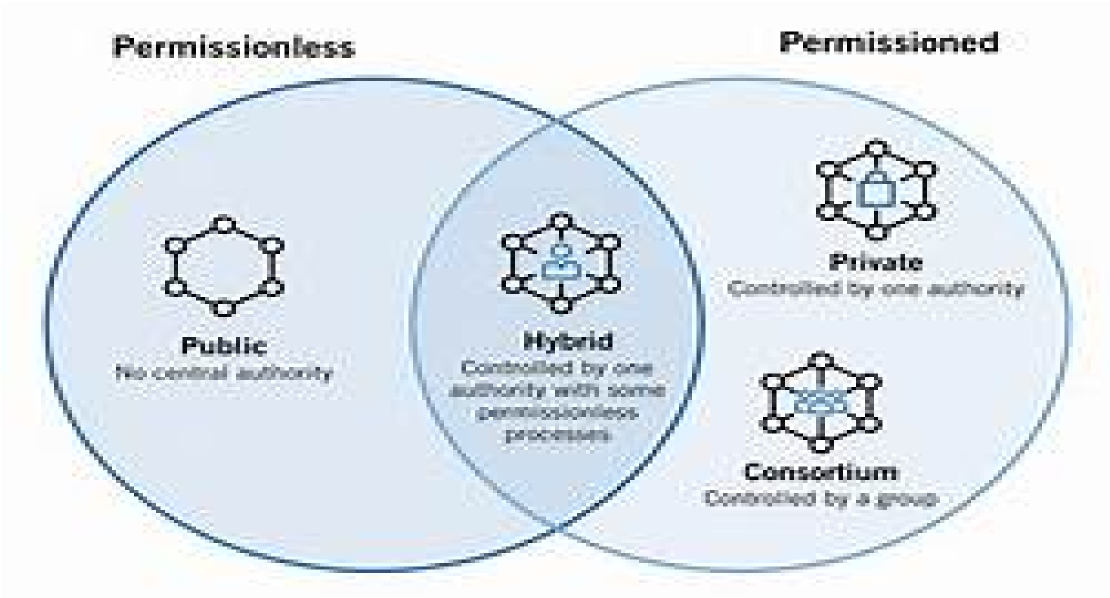

Figure 1.1: Types of Blockchain

1.5 Benefits of Blockchain in EHR

Keeping our important medical data safe and secure is the most popular blockchain healthcare application at the moment, which isn't surprising. Security is a major issue in the healthcare industry. Between 2009 and 2017, more than 176 million patient records were exposed in data breaches. The perpetrators stole credit card and banking information, as well as health and genomic testing records. Some of the major befits of using Blockchain in EMR are:

Decentralization: The same copy of healthcare records will be available to all stakeholders and all of them have same access and control privileges. No single entity will have control over the data.

Security and Privacy: Blockchain will help to create tamper-proof record through its immutability property. All records are encrypted and time stamped and added in to existing distributed databases in chronological order. Privacy and identity of patient is protected through cryptographic keys.

Data Ownership: Patients will get assurance that their records are not misused or altered. He will get full control of his data. This is achieved by strong cryptographic protocol and pre-defined smart contract.

Data Verifiability: Every stakeholder can check the integrity and validity of records stored on Blockchain. This feature is mostly applicable where data verification process is required such as insurance claim processing.

Trust: As Blockchain records are accessible to all, nobody has to question whether information has been altered for personal benefit.

Chapter 2

Literature Review

- **Mcseth Antwi in 2021** taljs about The Case of Hyperledger Fabric as a Blockchain Solution for Healthcare Applications. He proposed solutions that follows GDPR/HIPAA. But Solution is not fully implemented. Hyperledger Composer is decrypted now so technology is bit old. Not scalable and flexible. Used Hyper Ledger as Fabric

- **Ayesha Shehnaz in 2020** introduces blockchain for electronic health records. She used of chain scaling solution system is scalable, role based access mechanism the execution time increases with the increase of transaction been increased. She used Etherium on this project.

- **Anushree Tandon in 2018** introduces blockchain in Healthcare a systematic literature review synthesizing framework and future agenda. She implied the strategic perspective cost in efficient. Framework focused solely on selected data bases. She used hyperledger Fabric in her solution.

Chapter 3

Problem Statement

"Implementation of EHR System Through Hyperledger Fabric."

Chapter 4

Proposed Work

Electronic Healthcare records (EHR) often contain highly sensitive healthcare data, which are periodically distributed among healthcare providers, pharmacies and patients for clinical diagnosis and treatment. Furthermore, critical medical information must be regularly updated and shared where proper consent is provided by the patient. Along with this we need strong availability, fast access and the appropriate encryption of these records.

There are currently several approaches regarding EMR management and how blockchain technology can be utilized to improve it. We present Hyperledger Fabric blockchain architectures for EHRs to create a trusted and transparent encyclopedia of patient data in EHRs that pledges controlled data access and integrity among the stakeholders of the EHR system.

Blockchain ensures that the majority of the network nodes must validate the information blocks stored on the ledger before being posted to the ledger based on stated and agreed rules. A private permissioned blockchain like Hyperledger Fabric is suitable in achieving patient's privacy and confidentiality, such as their healthcare-related private details. Below are the steps showing the secure workflow of patient records and activities.

Step-1: Initially, the patient visits the physician (doctor) by registering itself to the hospital counter. This patient data consists of medical history, current problem and other physiological information and is stored in the local database connected to the system.

Step-2: An EHR is generated from the initial data collected in step (1) for each patient. Additionally, other medical information such as laboratory test results, medical imaging, nursing care, and drug history-related data will also encompass the EHR.

Step-3: The patient who is the owner of EHR has the sole authority to give different access rights and permissions of sharing and using the sensitive information to various stakeholders of the healthcare ecosystems to achieve data privacy and secrecy.

Step-4: The EHRs have now been stored permanently in the blockchain ledger and other decentralized storage systems. The local database is used to make sure that patient records at initial stage can be modified and stored locally before being updated at the ledger.

Step-5: Hospital and ad hoc clinics, are one of the critical stakeholders who have authorized access to the blockchain ledger to provide better and efficient medical services to the patient using the EMRs. This blockchain-enabled EMR system ensures the secure and transparent transfer of EMRs to various healthcare providers in the globe so that the patient's records can be made available and accessible any time at any place validated and verified through a distributed ledger.

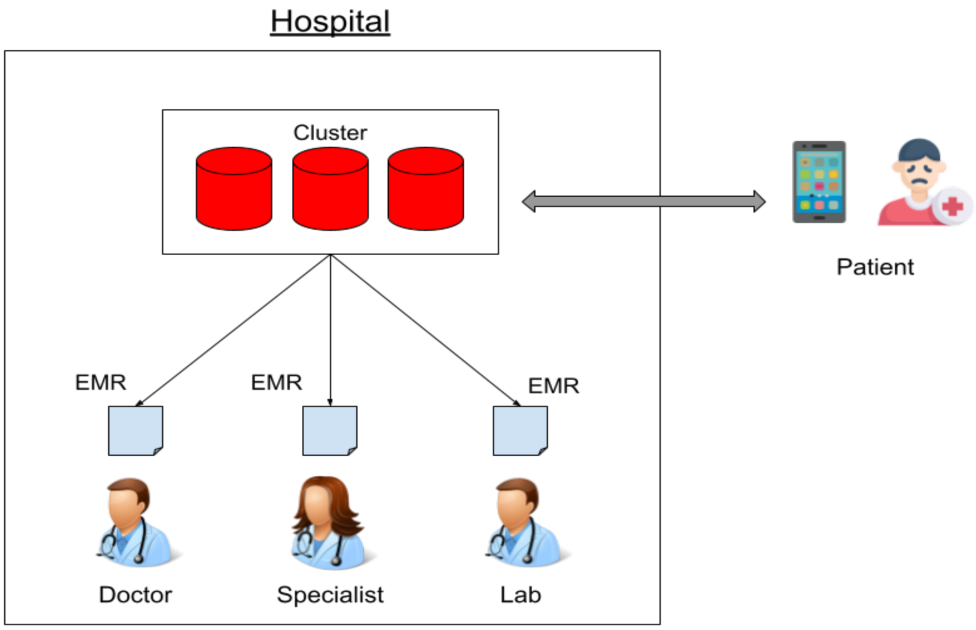

Figure 4.1: Fig. Blockchain-enabled EMR management in healthcare

5.1 Participant Permissions

Role	Permissions
Admin	Has full access to all users and system resources.
Doctor	Create, delete, read and update their own participant information. • Read/update permissioned EMR: If a patient has authorized a practitioner, the latter is able to read or update the patient's EMRs. • Refer to other practitioners: Practitioners can grant update rights to other practitioners on EMRs they have been authorized to update.
Patient	Create, delete, read, and update their own participant information. • Grant update rights to practitioners: the patient can grant the doctor the correct permissions to update their EMR. • Remove permissions from practitioners: The patient can revoke rights from a practitioner if they see fit.

Figure 4.2

5.2 EHR Architecture using Hyperledger Fabric Enabled Blockchain

We choose Hyperledger enabled private permissioned consortium blockchain, which uses the Hyperledger Fabric platform. Multiple healthcare providers with in a hospital are connected to form a private peer-to-peer consortium network. The permission to join the fabric network is determined based on consensus among the participating stakeholders. Furthermore, the efficiency of fabric is much more compare to other public blockchains as it executes more than 3,500 transactions per second.
In the fabric architecture, a permissioned private blockchain network is created where all the participating healthcare stakeholders and their end-users are identified and registered by the health authority using the membership service (MSP) component of the fabric using certificate issuing (C.A.) authorities.

To create a trusted environment between untrusted participants, the fabric provisions an identity management system that introduces the notion of membership service that established rules and regulations by which different stakeholders (identities) are governed, authenticated, validated, and verified to be part of the network and allowed to access the EMRs systems for ensuring secrecy, privacy, and confidentiality among the stakeholders in the network. The fabric network comprises different peer nodes, and each peer node can be an endorser or committer node. It also contains an ordering service component, also called Orderers. This service accepts the endorsed transactions from the patient, orders them into groups of blocks with cryptographic signatures of the ordering peers, and finally broadcasts these blocks to the committing peers in the blockchain network for validations against the endorsement policies.

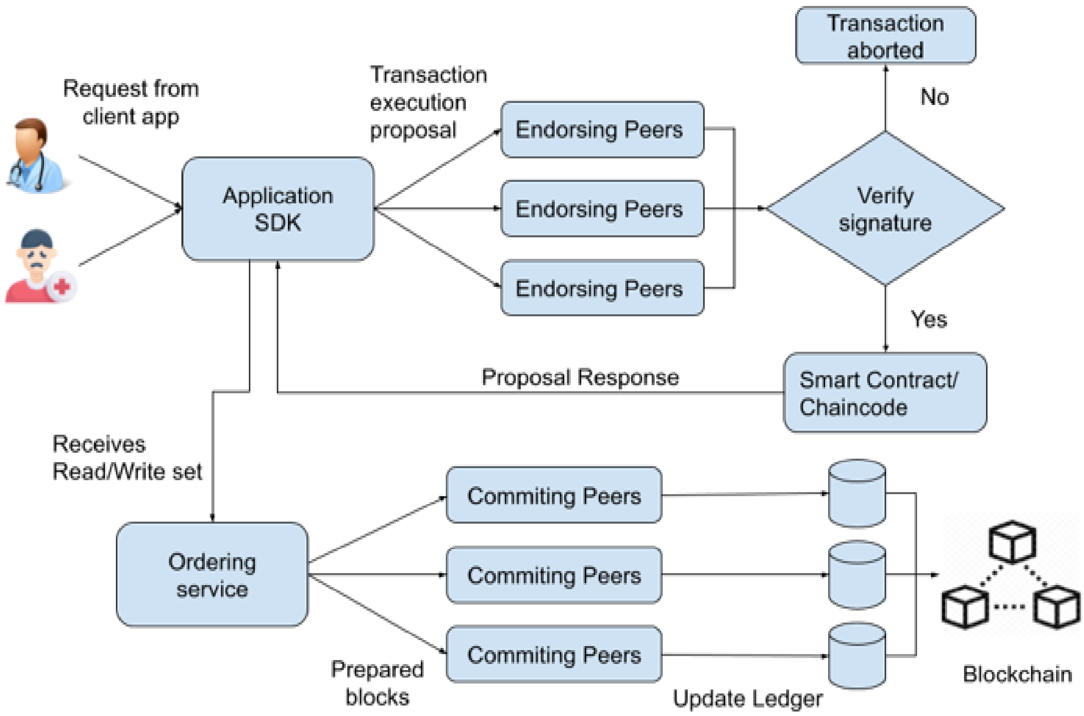

Figure 4.3: Hyperledger fabric consensus mechanism for EMRs

Chapter 5

Objectives

- To study present EHR System with Blockchain..
- Implementation of EHR through Hyperledger Framework.
- To study the performance of implemented EHR.
- To store medical data of patient tamper proof.

Chapter 6

Methodology

Hyperledger Fabric Framework

Hyperledger Fabric (HLF) is an open source permissioned blockchain established by the Linux Foundation that is mainly used to serve enterprises. What distinguishes HLF from other platforms is its new transaction architecture called Execute Order-Validate architecture. This new architecture replaces the traditional order-execute one used by all of the existing platforms. In order-execute architecture, first, transactions are ordered based on the consensus protocol. Then, in the execution phase, each peer executes transactions sequentially in the same order. This execution phase has a negative impact on the performance of the network as the peers have to go through all the transactions in the block and execute them which increases the latency. Another point that differentiates HLF is that it supports general-purpose programming language smart contracts or chain codes as HLF call them. It is obligatory that smart contracts in platforms that follow the order-execute architecture have to be deterministic; and that is why some platforms require writing the smart contract in a Domain Specific Language (DSL) to eliminate the non-deterministic operations

Channels

Based on the requirements, HLF allows the creation of several channels within the same network. A channel could be referred to as a private communication network within the main network. Each channel has its own ledger, therefore only the peers and organizations that are members of this channel will have a copy of this ledger. These members are defined in the channel policy in the configuration block that also defines the type of ordering service. Whenever any configuration is modified a new configuration block is created and added to the chain.

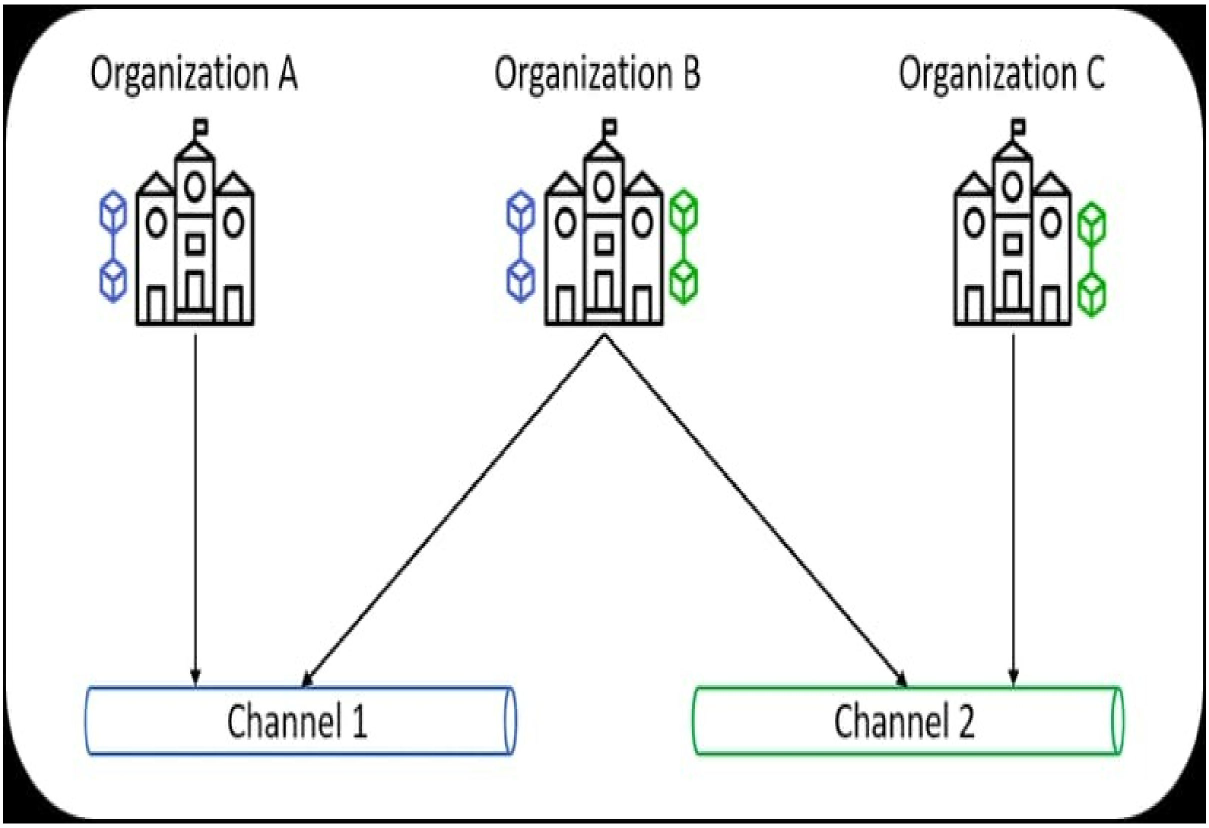

Figure 6.1

Implementations of Ordering Service

To achieve consensus, HLF introduces orderer nodes. As the name implies, the main responsibility of orderer nodes is ordering the transactions in the blocks and broadcasting them to the peers for validation. HLP offers three different implementations of the ordering service

Solo: In solo-based implementation there is only one ordering node, which makes it a single-point-of-failure. Consequently, solo-based ordering service is not suitable for production. Nevertheless, it could be applied for testing and for academic usage as it eliminates the admin is trative overhead in the other implementation schemes.

Kafka: This mode follows leader and follower approach, where the leader orderer sends the transactions to the follower orderer nodes. The choice of the leader is done in dynamic fashion and as long as the majority of the nodes is up, the system is Crash Fault Tolerant (CFT). This scheme utilizes zookeeper coordination service for managing Kafka clusters. Zookeeper is a service used by decentralized applications in order to maintain configuration information, help in tasks coordination, provide distributed synchronization and cluster membership. Although this scheme was the only option that supports multiple orderers since HLF v1.0, the setup of Kafka based ordering service is challenging and it requires experts to deploy it.

Raft: Recently, HLF added Raft ordering service that is based on Raft protocol. It is similar to Kafka, as it has the advantage of being CFT and it follows the leader and follower approach. From the functional point of view there are no differences between Raft and Kafka, however, Raft is easier to setup.

Transaction Flow

In order to achieve consensus in HLF, each transaction goes through Execute-Order-Validate process summarized in the following Figure, the process starts once the transaction is proposed and ends when it is committed to the ledger.

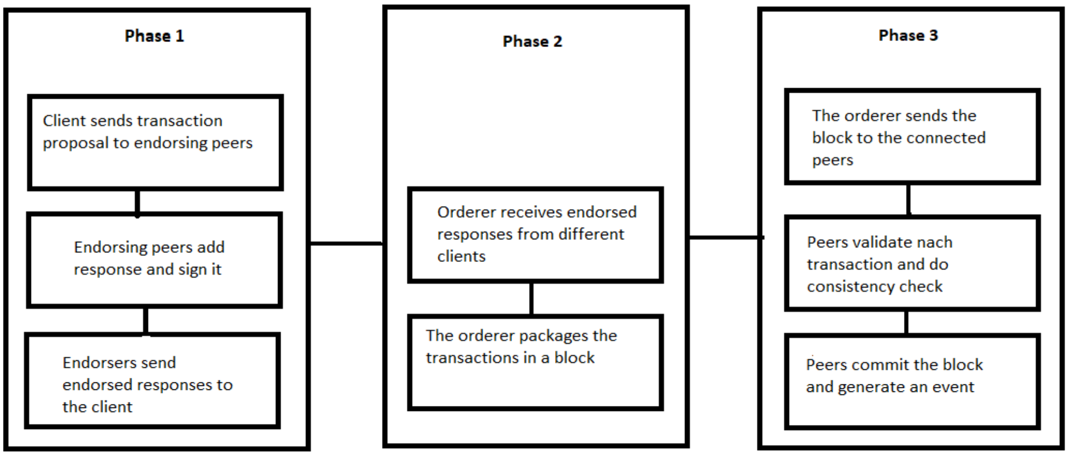

Figure 6.2

Phase 1: Proposal (Execute) The main aim of this phase is endorsing the transactions. This phase starts when the application client sends a transaction proposal to the endorsing peers. The set of the endorsing peers chosen is determined by the endorsement policy, each of these peers checks the following:

1) The proposal is well structured

2) The application is not trying to duplicate a transaction that already exists

3) The signature of the issuer is valid

4) The issuer is allowed to perform the proposed operation Then, each endorser executes the chaincode individually and generates a transaction response based on the execution results, and then it signs the response. Finally, the signed transaction proposal response is sent back to the application. Depending on the number of endorsing peers defined in the endorsement policy, the client waits until it receives a certain number of endorsements, which marks the end of the first phase.

Phase 2: Ordering and packaging (Order)

This phase is concerned with packaging the transactions into blocks, which is the orderer's main responsibility. First, the client sends the endorsed transaction proposal responses to the orderers. Then, the orderers package the authorized trans actions into a block in a strict order.

It is worth noting that the number of transactions per block is decided by the channel. configuration, and it affects the overall latency of admitting the transaction into the blockchain. The orderer does not bother itself looking into the content of the transactions, unless it is a configuration block.

Phase 3: Validation and committing (Validate)

The last phase starts when the orderer sends the block to the peers connected to it, peers that are not connected to the orderer will eventually receive the block by gossiping. Each peer on the channel will validate the transactions in the block separately but in a deterministic way, since all the peers validate the block in the same way, each peer will have an identical copy of the ledger. The process of validation includes ensuring that the transaction is endorsed by the required endorsers according to the endorsement policy. To commit the block to the ledger, the peers perform a consistency check to ensure that of the assets was updated by any other transaction when phase 1 and 2 were taking place. After that, the peers commit the block to the ledger, adding another field to each transaction to indicate whether it is valid or not.

Chapter 7

System Design

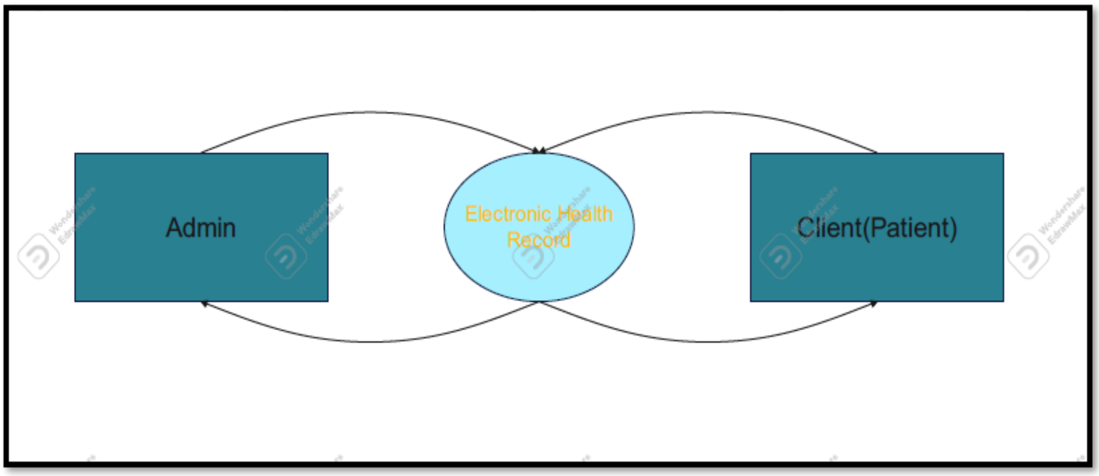

Figure 7.1: 0 level DFD Diagram

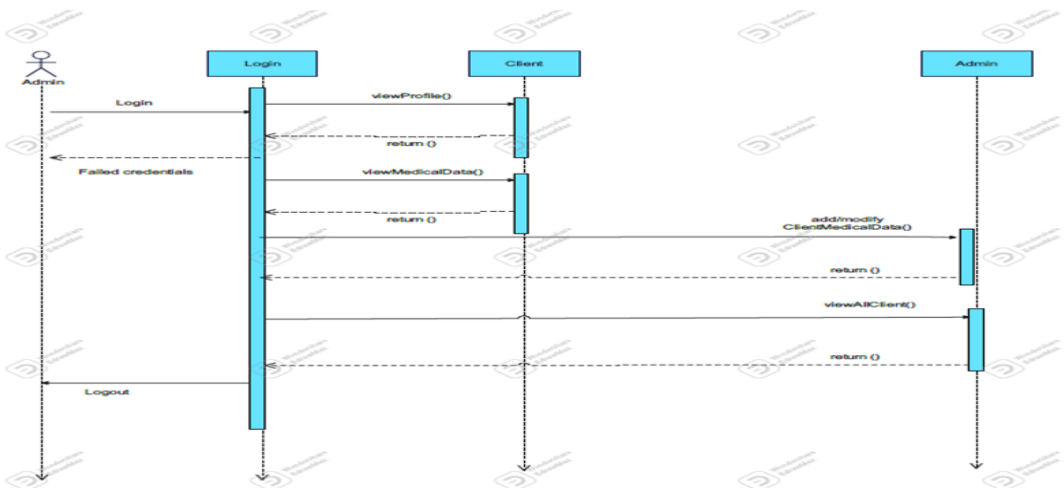

Figure 7.2: Sequence Diagram

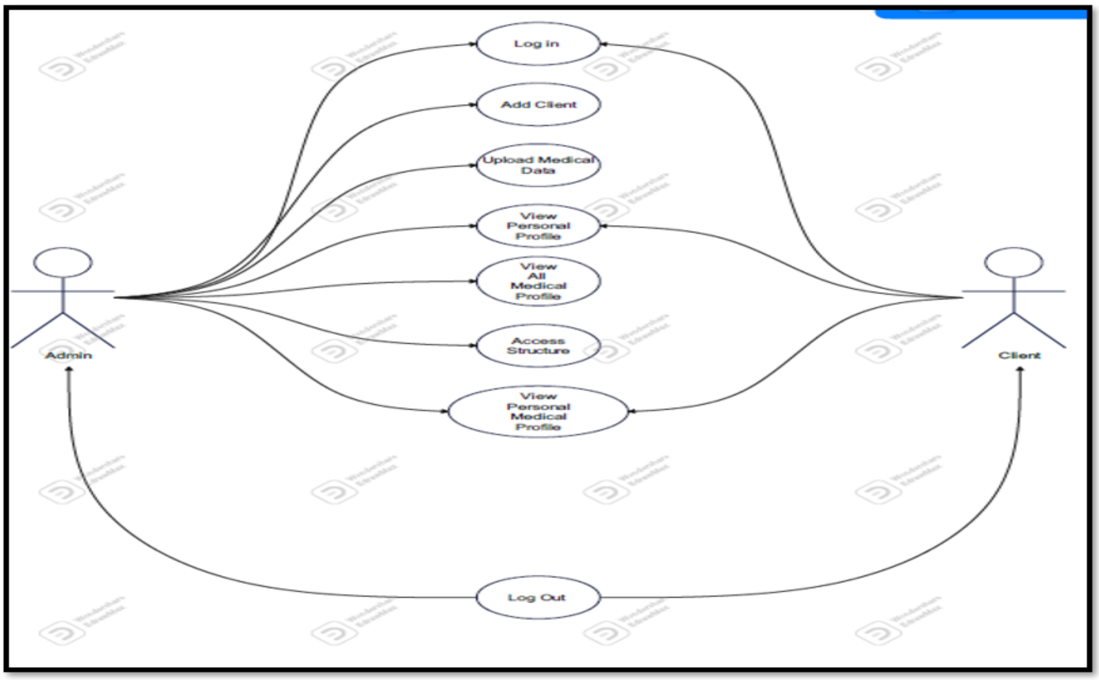

Figure 7.3: Use case Diagram

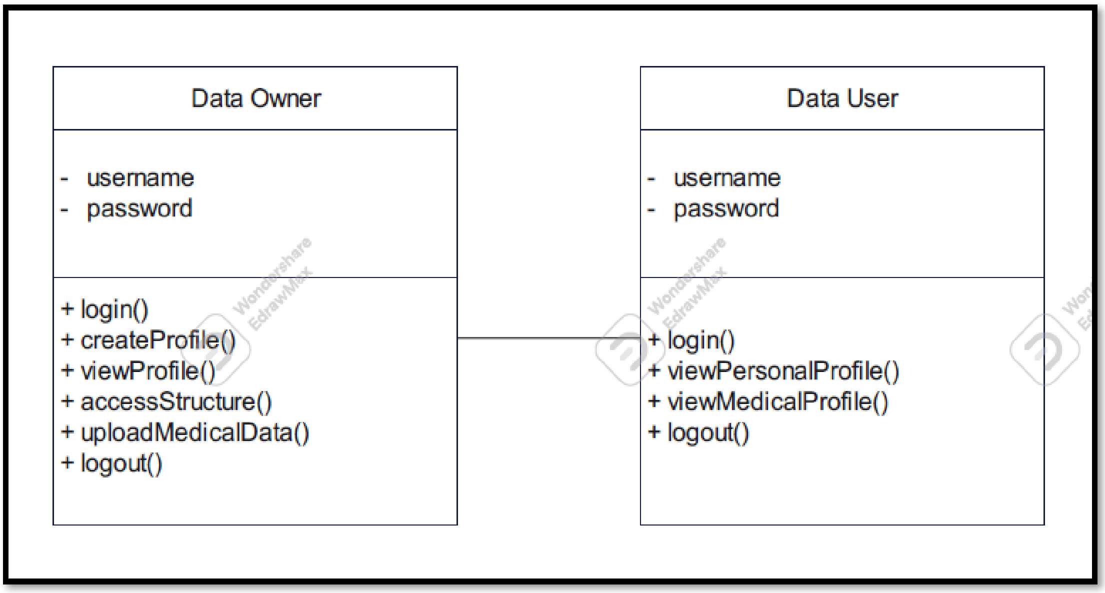

Figure 7.4: Class Diagram

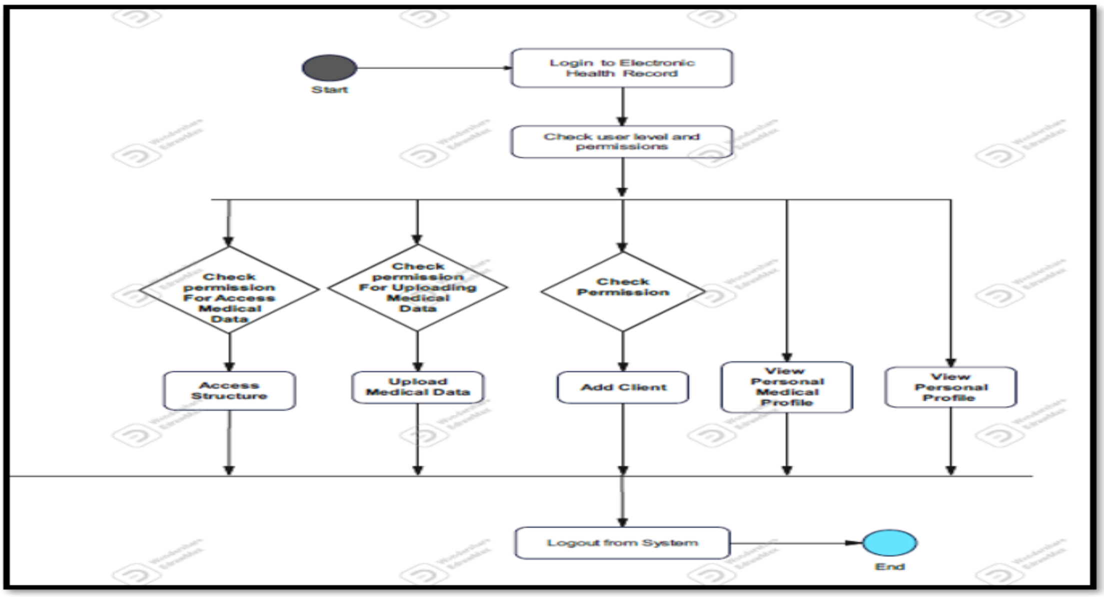

Figure 7.5: Activity Diagram

Chapter 8

System Requirements

8.1 Software Requirement

- Operating system: Linux, Windows
- Front End: HTML, CSS, javascript
- Back end: Nodejs
- Database: LevelDB
- Tool Used: Hyperledger Fabric

8.2 Hardware Requirement

- Processor: minimum dual core processor and above
- Hard Disk: 1 TB
- RAM: 8 GB and above.

Chapter 9

Implementation Details

Login Page: This is the Login page

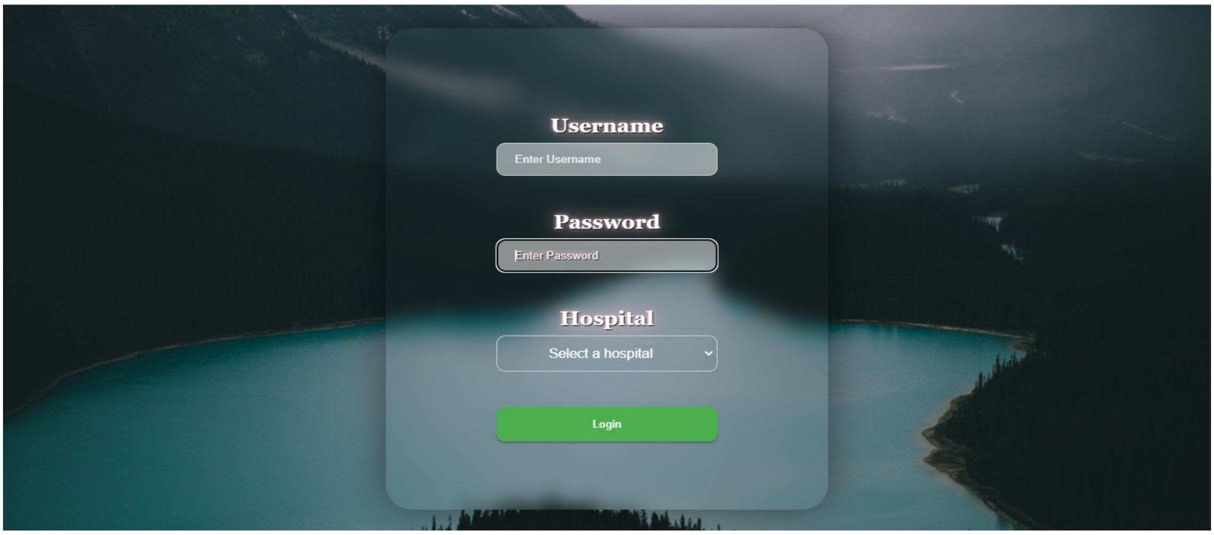

Figure 9.1

Admin login: This is admin login for Hospital-1 or Hospital-2.

It initializes the login credentials of admin whether it is for Hospital-1 or Hospital-2.

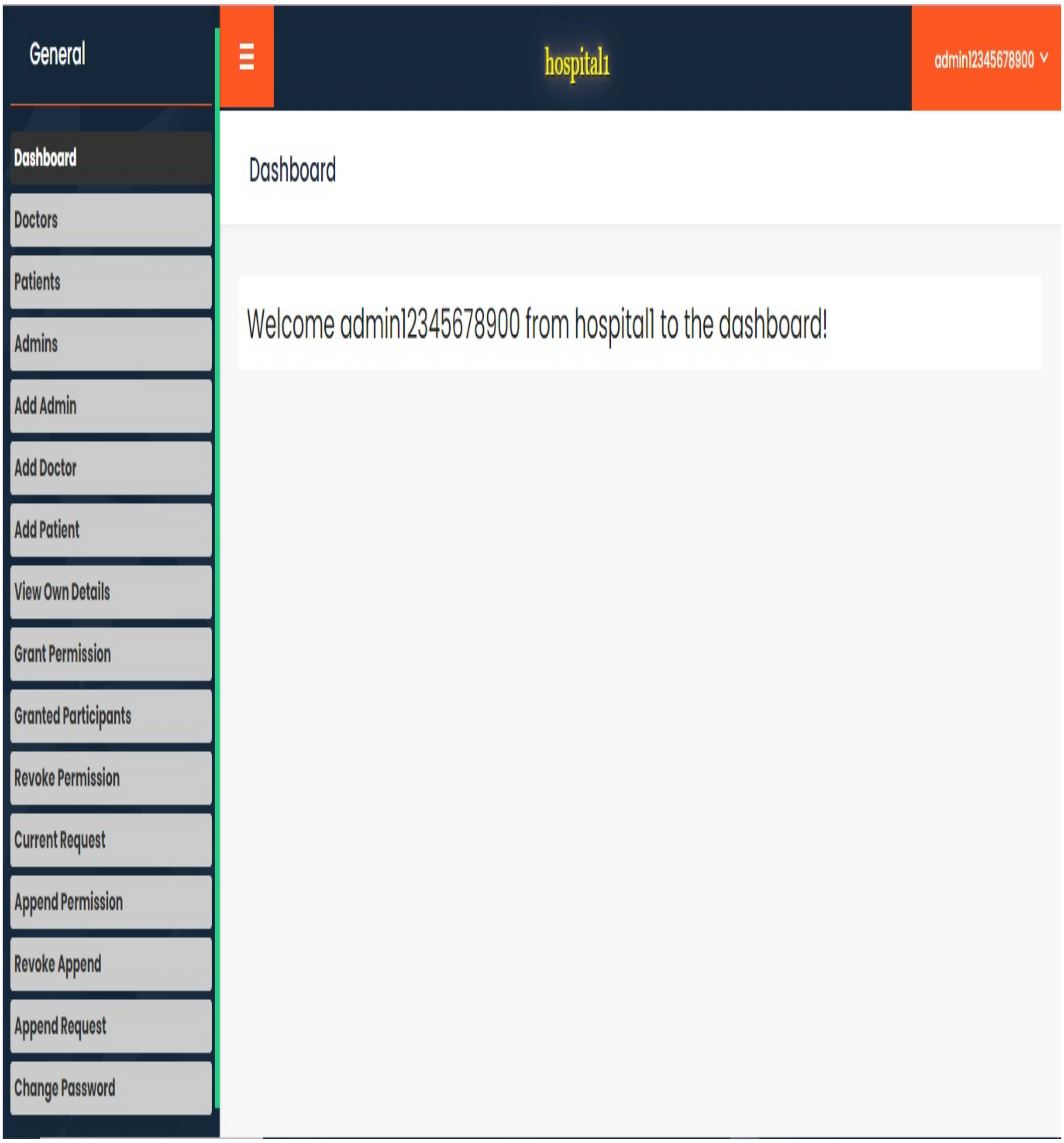

Figure 9.2: Admin Dashboard

Admin Dashboard: This is the Dashboard of Admin with various access permissions such as:

- Doctors
- Patients
- Admins
- Add Admin
- Add Doctor
- View Own Details
- Grant Permission
- Granted Participants
- Revoke Permission
- Current Request
- Append Permission
- Revoke Append
- Append Request
- Change Password

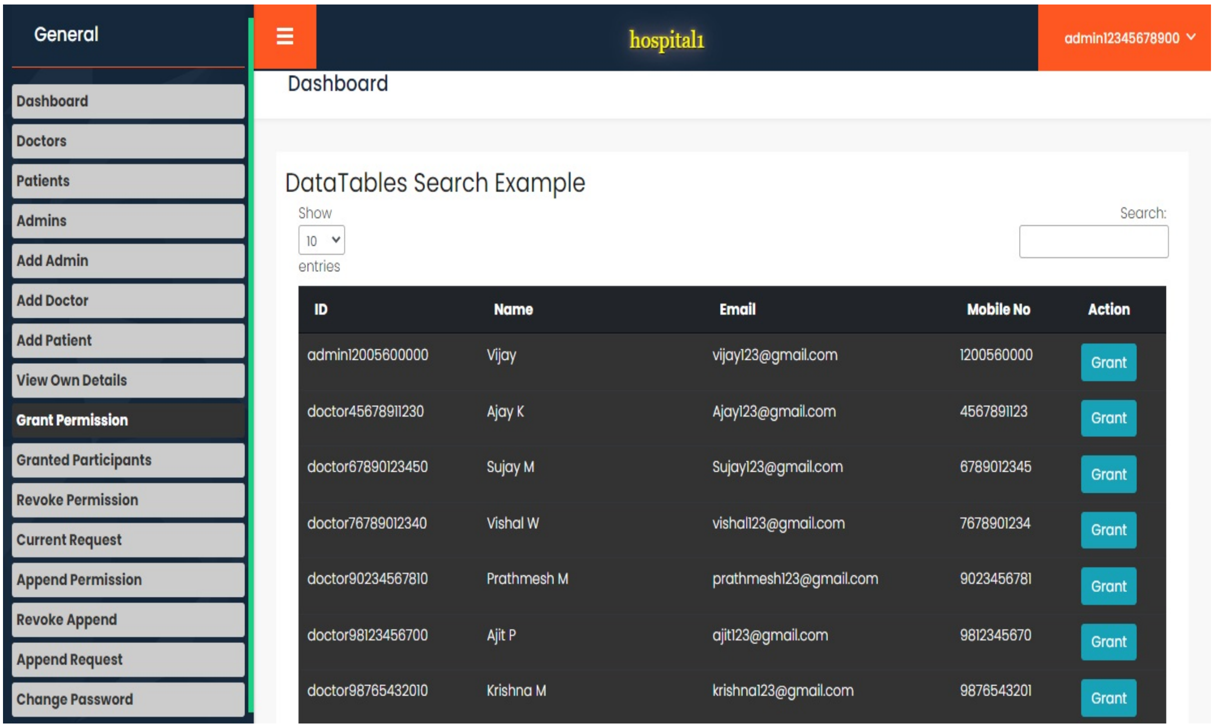

Figure 9.3: Admin's dashboard for grant permission

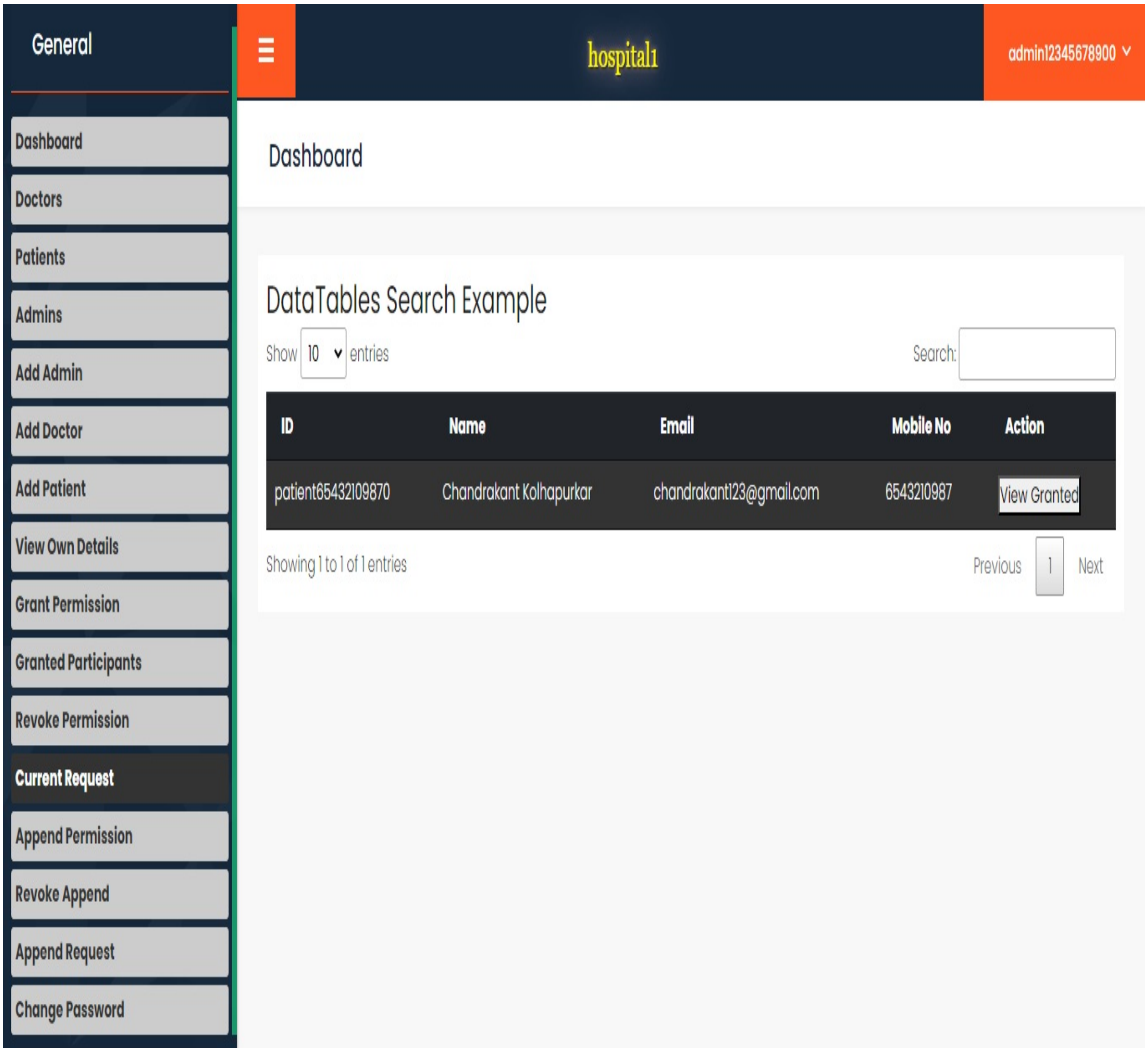

Figure 9.4: Permission granted view list

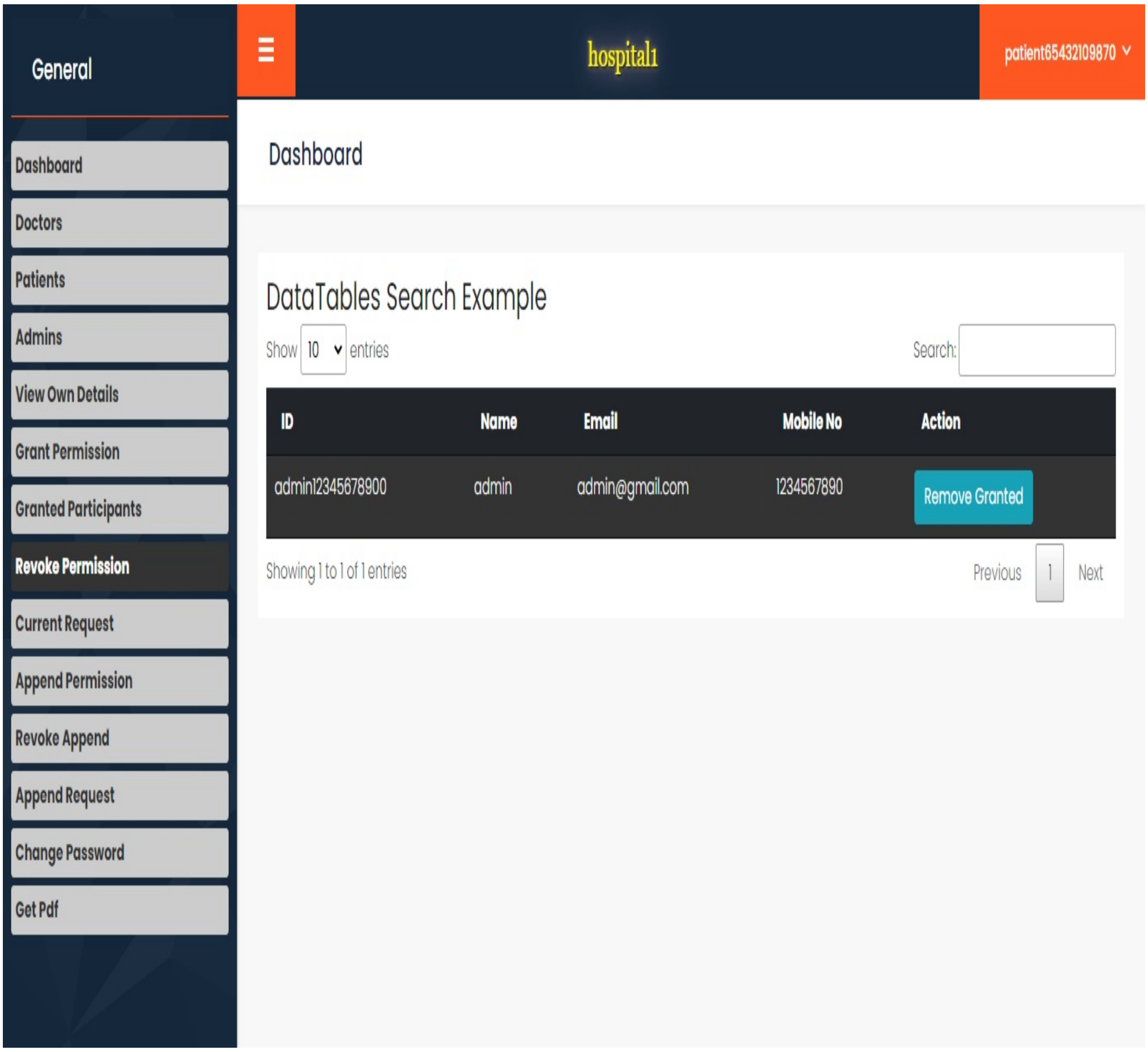

Figure 9.5: Patient dashboard for Revoke Append

Conclusion

Hyperledger fabric is a promising blockchain framework that has some concepts of policies, smart contracts, and provision of secure identities which make the records secure and controlled. It enables the EHR systems to interoperable among multiple hospital organizations. Doctor can track history easily. Patients do not need to carry medical history files and will be significant improvements in digital records. An EHR scenario comes under the private and closed blockchain category and this solution can successfully conclude that it is an encouraging framework of this kind of blockchain. It provides a reliable and secure solution in managing medical field record.

Bibliography

[1] Charalampos Stamatellis Pavlos Papadopoulos, Nikolaos Pitropakis, Sokratis Katsikas and William J. Buchanan; *"Privacy Preserving Healthcare Framework Using Hyperledger Fabric;",* [*MDPI - Sensors Article Published: 18 November 2020.*]

[2] Mueen Uddin, M. S. Memon, Irfana Memon, Imtiaz Ali, Jamshed Memon , Maha Abdelhaq, and Raed Alsaqour; *"Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records; Computers, Materials Continua Tech Science Press",* [*DOI:10.32604/cmc.2021.015354 Article*]

[3] M. Antwi, A. Adnane, F. Ahmad, R. Hussain, M. Habib ur Rehman, C.A. Kerrache, The Case of HyperLedger Fabric as a Blockchain Solution for Healthcare Applications, Blockchain, [*Research and Applications, https://doi.org/10.1016/j.bcra.2021.100012*]

[4] Neeraj Kumar Muhammad Khurram Khan Shuyun Shi Debiao He and Kim-Kwang Raymond Choof, *"Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey.",* [*In: NCBI. 2020. doi: 10.1016/j.cose.2020.101966.*]

[5] Downloadfabricsamplesprocedure,*"In:url:",* [*https://hyperledgerfabric.reo/en/release.2/test*$_{n}etwor.hn.$]

[6] Kevin J. Peterson, Rammohan Deeduvanu, Pradip Kanjamala, and K. Mayo., *"A Blockchain- Based Approach to Health Information Exchange Networks.",* [*In 2016.*]

[7] Prerequisites before start test network of hyperledger fabric, *"In: url: https://hyperledfabric.readthedocs.io/en/release2.2/ prereqs.htmlpreequisites",*

[8] Alevtina Dubovitskaya et al. "ACTION-EHR: Patient-Centric BlockchainBased Electronic Health Record Data Management for Cancer Care, *"In: Journal of Medical Internet Research 22.8 (Aug. 2020), e13598 Hyperledger Fabric SDK for Node.js. https://hyperledger.github.io/fabric-sdk-node/release- 2.2/module-fabric-network.html.doi: 10.2196/13598. url: https://doi.org/10.2196/13598",* [*Accessed 27.03.2021*]

[9] Identity.https://hyperledgerfabric.readthedocs.io/en /release2.2/ identity/identity.html., [*Accessed 27.03.2021*]

[10] Sudeep Tanwar, Karan Parekh, and Richard Evans, *"Blockchain-based electronic healthcare record system for healthcare 4.0 applications",* [*In: Journal of Information Security and Applications 50 (Feb. 2020), p. 102407. doi:10.1016/j.jisa.2019.102407.url:https://doi.org/10.1016/j. jisa.2019.102407.*]

[11] Gebremedhin T., *"Blockchain as a Technology to Facilitate Privacy and Better Health Record Management",* [*2020-07- https://bora.uib.no/handle/1956/19621.*]

[12] Linn, L.A.; Martha, B.K., *"Blockchain for Health Data and Its Potential Use in Health It and Health Care Related Research. In Use of Blockchain for Healthcare and Research Workshop",* [*ONC/NIST: Gaithersburg, MD, USA, 2016.*]

[13] Bryatov, S.R.; Borodinov, A.A., *"Blockchain Technology in the Pharmaceutical Supply Chain: Researching a Business Model Based on Hyperledger Fabric."*