Siddaganga Institute of Technology Tumakuru

(An Autonomous Institute, Affliated to Visvesvaraya Technological University Belagavi,
Approved by AICTE, New Delhi, Accrediated by NAAC and ISO 9001:2015 certified)

Blockchain Based Medical Data Asset Management System

A project report submitted to
Visvesvaraya Technological University. Belgaum, Karnataka
in the partial fulfillment of the requirements for the award of degree of

Bachelor of Engineering
in
Computer Science and Engineering
By

Akanksha Srivastava	**1SI18CS007**
Khalid Farooq	**1SI18CS046**
Rakshitha B	**1SI18CS085**
Rishika Kumari	**1SI18CS087**

under the guidance of
Mrs. Shruthi K M.Tech
Assistant Professor

Department of Computer Science Engineering
(Program Accredited by NBA)
Siddaganga Institute of Technology
B.H Road, Tumakuru-572 103, Karnataka, India.
Web : www.sit.ac.in

July,2022

Department of Computer Science and Engineering
Siddaganga Institue of Technology, Tumakuru
(An Autonomous Institute under Visvesvaraya Technological University, Belagavi,
Approved by AICTE, New Delhi, Accredited by NAAC and ISO 9001:2015 certified)

Certificate

This is to certify that the Project Report entitled **"Blockchain Based Medical Data Asset Management System"** is a bonafide work carried out by **Akanksha Srivastava (1SI18CS007), Khalid Farooq (1SI18CS046), Rakshitha B (1SI18CS085) and Rishika Kumari (1SI18CS087)** in the partial fulfillment of the requirement for the award of the degree of Bachelor of Engineering in Computer Science and Engineering, Visvesvaraya Technological University, Belagavi during the year 2021-22. It is certified that all corrections/suggestions indicated for the internal assessment have been incorporated in the report.The project report has been approved as it satisfies the academic requirements in respect of project work prescribed for the Bachelor of Engineering Degree.

....
Guide
Mrs. Shruthi K
Asst. Professor
Dept of CSE, SIT

....
Group Convener
Dr. M. B. Nirmala
Associate Professor
Dept of CSE, SIT

....
Dr. A. S. Poornima
Professor and Head
Dept of CSE, SIT

....
Dr. S. V. Dinesh
Principal
SIT, Tumakuru

Name of the Examiners   Signature with Date

1. Prof.

2. Prof.

Department of Computer Science and Engineering

Siddaganga Institute of Technology

Tumakuru - 572103

DECLARATION

We hereby declare that the entire work embodied in this dissertation has been carried out by us at **Siddaganga Institute of Technology** under the supervision of **Mrs. Shruthi K**. This dissertation has not been submitted in part or full for the award of any diploma or degree of this or any other University.

- Akanksha Srivastava(1SI18CS007)
- Khalid Farooq(1SI18CS046)
- Rakshitha B(1SI18CS085)
- Rishika Kumari(1SI18CS087)

ACKNOWLEDGEMENT

With reverential pranams, we express our sincere gratitude and salutations to his holiness, **Dr. Sree Sree Sivakumara Swamigalu**, Founder President, **Sree Sree Siddalinga Swamigalu**, President, Sree Siddaganga Math, for being a constant source of inspiration in the course of study.

First and foremost, we wish to express our deep sincere feeling of gratitude to our institution, **Siddaganga Institute of Technology**, for providing us an opportunity for completing our project successfully.

We are grateful to **Dr. M N Channabasappa**, Director, Siddaganga Institute of Technology, Tumakuru for his kind cooperation and encouragement.

We express our kind thanks to **Dr. S.V. Dinesh**, Principal, Siddaganga Institute of Technology, Tumakuru for his encouragement.

We express our heartfelt thanks to **Dr. A S Poornima**, Professor and Head, Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumakuru for her valuable suggestions and advice.

We would also like to thank the panel convener, **Dr. M B Nirmala, Associate Professor** and panel member **Mr. Gururaj S P, Assistant Professor**, of the project for their scrutiny throughout the various stages of evaluations and presentations. Without their appropriate questioning and guidance, the project would not have been completed.

We express our heart full gratitude and humble thanks to our project guide, **Mrs. Shruthi K**, **Assistant Professor**, Department of Computer Science and Engineering, Tumakuru for guiding and facilitating to complete our major project work successfully.

We are conscious of the fact that, we have received cooperation in many ways from the Teaching, Technical and supporting staffs of the Department of Computer Science and Engineering and we are grateful to all for their cooperation. We would also like to thank our friends and family for being a constant source of moral support and encouragement throughout the project.

Abstract

In today's health care management, medical health records are in the form of electronic medical record (EHR/EMR) systems, an electronic representation of a patient's medical record. However, a patient's medical data to be acquired in an efficient and timely manner is proven to be difficult through these records. In addition to this, in the pharmaceutical industry, monitoring of drug supply chains is a challenge. The outcome of this lack of monitoring gives counterfeiters the chance to put their fake drugs in the supply chain and the market which causes mistreatment and deaths often.

Health management is always hindered by the inability to acquire information, less usage of information acquired, poor data asset security and unmanageable privacy controls. Thus our project, Secure and Efficient Medical Data Asset Management System using Blockchain comes into picture. Blockchain technology eases the accessibility of all such records by maintaining a block for every individual patients. This technology is also used for proper tracking of the supply chain to avoid counterfeit drugs.We provide an architecture that makes use of an off-chain solution to give doctors, lab staff, and patients secure access to the patient records. Blockchain encrypts and makes the medical records immutable for data integrity. The medical records would be accessible to everybody, but only patients would have the secret key, which they could then give to whoever they choose. The smart contracts also helps our data owners to manage their data access in a permissioned manner.

The final project will be viewed as a web and mobile interface to easily access, detect as well as ensure high security data.

Contents

List of Figures

Chapter 1

Introduction

One of the biggest issues faced worldwide in the healthcare and medical sector, is the incapacity for medical data to be acquired in an efficient and timely manner. All medical health records or electronic medical record (EHR/EMR) systems presume that each patient approaches medical practitioners in one clinic or in the common state or province. These systems are only centred around the same practitioner and the use for such information is not useful nor accurate. Patients visit multiple doctors per year and for various reasons. The broader aspect of practitioners that usually aren't taken into account are chiropractors, pharmacists etc. Patients also travel for vacation, work and even relocate for a longer duration. In the present day, a large number of patients are vastly interested in recording their health status using wearable health devices. This health data generated by patients is easily acquired by the service providers/devices but never with medical practitioners. Thus, regardless of patients being the rightful owners of their medical data assets, and in spite of practitioners, health facilities and government providing large medical investments, health management is always hindered by inability to acquire information, less usage of information acquired, poor data asset security and unmanageable privacy controls.

In addition to these problems, in the pharmaceutical industry, monitoring of drug supply chains is a challenge. The outcome of this lack of monitoring gives counterfeiters the chance to put their fake drugs in the supply chain and the market which causes mistreatment and deaths often.

Our project addresses all such issues with a hyperledger based blockchain architecture that is more extensible and scalable. We have three primary parts in our project: a patient centric web app for smooth user experience, an off-chain storage for patient data and a blockchain-based access control module. Our data assets like medical reports, prescriptions, treatments plans, drugs, etc. are kept in a safe cloud-based repository to maintain the level of performance and keep it economically feasible. The application is simple to use for patients, carers, healthcare professionals, distributors, and manufacturers thanks to its web and mobile interfaces. Through a patent-pending technique, the on-chain and off-chain data are safely connected without any additional storage load in the blockchain architecture. By the use of smart contracts our data owners can manage the data access in permissioned and secure manner.

1.1 Background Study

Electronic medical records (EMRs) provide a typical method of storing patient data in hospitals. But even for a common patient, data is stored in multiple hospitals. Thus it is proven hard for a patient to get their multiple records accessed through a summarized EMR because of security and privacy concerns. Pharmaceutical businesses had difficulty tracking their products along the supply chain process for the past decade, allowing counterfeiters to enter the market with their low quality or fake drugs. Counterfeit pharmaceuticals are seen as a major threat to the pharmaceutical sector around the world.

In today's scenario, in spite of practitioners and governments funding for the medical sector, health management is always hindered in fields like accessibility of information, less interoperability, poor data asset security, unmanageable privacy controls, monitoring and discovery of fake drugs, and the inaccessibility of medical data assets by patients, despite being the rightful owners of it. These are the key reasons for developing a health care management system using blockchain.

For security reasons, blockchain is implemented in this healthcare management system. But since permissionless blockchains are susceptible to be disruptive, permissioned chains are being implemented as they avoid pricey consensus processes and work in secure situations.

1.2 Related works

An effective medical data management system is needed because of the increased need for medical records on a daily basis. There have been numerous attempts at the same as of late.

One of them is the MedBlock stated in the paper[1], which uses blockchain to deliver a condensed EMR solution. Some of the papers attempted to address the problems that arise when monitoring patients. These papers concentrated on security issues, alerting the patients while maintaining security. Along with the concern focusing on patient and practitioner privacy and identification, papers have also elaborated on adopting a decentralised approach for a better patient-driven paradigm. Many have attempted to create a peer-to-peer network using a patient-centered concept while retaining the data's security and integrity. Another paper[8] illustrates a different strategy for decreasing costs and boosting efficiency by utilising off-chain storage. The following chapter provides discussion of the specifics of each of these works.

1.3 Project Problem Statement and Objectives

Health management is always hindered by the inability to acquire information, less usage of information acquired, poor data asset security and unmanageable privacy controls. In addition to these problems, in the pharmaceutical industry, monitoring of drug supply chains is a challenge. The outcome of this lack of monitoring gives counterfeiters the chance to put their fake drugs in the supply chain. Our project addresses all such issues using a hyper-ledger based blockchain to create a secure and efficient medical data asset and drug management system.

The chosen project tries to fulfill the following objectives:

- To enable a coherent accessibility of health data amongst caregivers, health practitioners and patients.
- To acquire an enhanced and secure mechanism for the transfer of personal health information.
- To provide an economically feasible health data management system .

1.4 Organization of the Report

The report's organisational breakdown is provided below:

The project's introduction and goals, as well as a few related works, are covered in the first chapter. The literature review is included in the second chapter. Chapter three contains an explanation of the project's architecture and methods. Chapter four talks about the detailed design of the project which includes the interface design and the data structures and algorithms used. The details of the project's execution, the tools and technologies used, the coding standards, and the entire implementation process are covered in the fifth chapter. The testing techniques and test cases used in the project is discussed in chapter six. Conclusion and future scope of the project is discussed in chapter seven. The detail of paper presentation done regarding the project and the paper accepted in “Thirteenth International Conference on Advances in Computing, Control, and Telecommunication Technologies - ACT 2022” is also attached in chapter 8.

Chapter 2

Literature Survey

Title of the work: MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain

Citation : Fan, K., Wang, S., Ren, Y. et al. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J Med Syst 42, 136 (2018). https://doi.org/10.1007/s10916-018-0993-7

Description: The work in [1] aims to provide a familiar method of storing patients' information at hospitals. For a common patient, data is stored in multiple hospitals. Thus for a patient to get their multiple records accessible through a summarized EMR is proven hard because of security and privacy concerns. This paper provides a solution to the above problems by giving a blockchain-based information management system called 'MedBlock'. Here MedBlock's distributed ledger provides easy retrieval and access to data in electronic medical records. This paper also achieves an improved consensus mechanism and high data security by utilizing symmetric cryptography and customized access control protocols.

Title of the work: Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring

Citation : Griggs, K.N. Ossipova, O. Kohlios, C.P. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42, 130 (2018) https://doi.org/10.1007/s10916-018-0982-x

Description: The work in [2] caters to the requirements for problems that may be observed in systems that monitor patients remotely, including challenges with security of data sharing and transaction recording. This research proposes a blockchain based smart contract to provide secure analysis and medical management to address these problems. The solution described in the study, make use of the Ethereum based protocol which allows a smart device to communicate with sensors, invoke smart contracts, and record every occurrence on a blockchain simultaneously. These benefits patients with real time tracking and intervention in the medical field by notifying patients and practitioners, while simultaneously providing security. This paper resolves all security issues in medical smart devices health management in a HIPAA compliant manner.

Title of the work: Health Record Management through Blockchain Technology

Citation : V. M. Harshini, S. Danai, H. R. Usha and M. R. Kounte, "Health Record Management through Blockchain Technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1411-1415, doi: 10.1109/ICOEI.2019.8862594.

Description: Highlighting flaws in the centralized approach to maintaining health records, the research paper [3] brings out the issue of a data breach. There is a huge loss for institutions as well as patients when a data breach happens, in terms of monetary as well as health loss. Moving forward, this paper also reveals the flaws in institution-centralized data control and gives a decentralized system using blockchain as a solution. In health care, smart contracts help to make things simpler. Where Blockchain will be used for invocation, record production and validation. The solution proposed could be used as a solution for various problems in the medical domain such as record maintenance, record sharing, billing, medical research etc. It lays the theoretical base for a model of maintaining records with the help of blockchain, further research, and practical implementation.

Title of the work: A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology

Citation : S. Hasavari and Y. T. Song, "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), 2019, pp. 71-75, doi: 10.1109/SERA.2019.8886792.

Description: The work in [4] focuses on the poor management and causes of failure of Emergency Medical care. A lot of pre-hospital deaths are caused due to the lack of medical history of patients. Many pieces of information are created at one hospital and later useful to another hospital along the patient-care cycle. It is very difficult for a different healthcare system to retrieve a patient's medical history from the previous healthcare system. In this research, a blockchain-enabled secure file system is suggested as a potential solution to the problem of emergency access to patient records. All medical record concerns like authentication and privacy have been taken care of in this approach. With the help of practical implementation of this paper, ambulance crew can access patient's medical history and avail high quality pre-hospital care which leads to a much less death rate.

Title of the work: MedBlock: Blockchain-based Multi-role Healthcare Data Sharing System
Citation :Y. Yu, Q. Li, Q. Zhang, W. Hu and S. Liu, "Blockchain-Based Multi-Role Healthcare Data Sharing System," 2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM), 2021, pp. 1-6, doi: 10.1109/HEALTHCOM49281.2021.9399028.
Description: The work in [5] seeks to use a blockchain technique to eliminate the current centralised system's central point of failure and information sharing. Additionally, it suggests a blockchain-based framework for a multi-role healthcare data exchange system through the joint storage of blockchain and the InterPlanetary File System. According to the system analysis, the proposed blockchain based medical data sharing system which is multi-role, can efficiently manage storage, personal privacy, insurance, and personal data.
Title of the work: Blockchain-based approach for e-health data access management with privacy protection
Citation : L. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla, "Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-7, doi: 10.1109/CAMAD.2019.8858469.
Description: The work in [6] gives an example of how blockchain could be utilized in the healthcare management system to store patient data in hospitals and clinics according to their access regulations. The study presents two different types of chains— a private sidechain and a public mainchain, that either store data with the patients' actual ID or data with a temporary ID. Results were based on two metrics: 1) time taken to iden-

tify the specific patients' medical data and 2) transmission time of the process from the initial blocks inside the peer-to-peer network. Hyperledger Fabric framework was utilised.

Title of the work: Blockchain in Healthcare: A Patient-Centered Model
Citation :Hannah S Chen†, Juliet T Jarrell†, Kristy A Carpenter, David S Cohen, Xudong Huang* Department of Psychiatry, Massachusetts General Hospital and Harvard Medical School, USA
Description: The work in [7] presents a technology that might be used in various components of the healthcare system, such as for the sharing and storage of the insurance related data and medical records, for both physical healthcare facilities and mobile applications. By giving patients control over their own medical records and other health data assets, blockchain has emerged as a highly demanded place for research in software, revolutionising the healthcare system's hierarchical structure. Thus, this research led to a shift of power from doctors to patients, resulting in a model that is patient-centered.

Title of the work: MedAccess: A Scalable Architecture for Blockchain-based Health Record Management
Citation : M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem, "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257720.
Description: The work in [8] seeks to create a decentralised medical system using blockchain, but the cost of doing so is very high because confirming transactions before they are committed to the blockchain requires a lot of computer power. It is impossible and prohibitively expensive to maintain the storage of a patient's electronic health records (EHRs) on a blockchain network. In order to lower the high cost associated of blockchain transactions with significant volumes of data assets, this paper suggests an architecture that leverages an off-chain solution. The research also explores the use of watermarking as a potential method for storing patients' image-based results in addition to the network-stored IPFS objects' encryption.

Chapter 3

High-level Design

In this section, the development method used in the project is explained. The project structure and the phases of development is discussed in detail. The decision on the organisation of project as made in the beginning for the smooth execution of the plan. This chapter also provides details about functional and non-functional requirements of the project.

3.1 Agile Software development methodology

The way software is built is significantly dependent on agile software development. It has emerged as a popular phase for software and software development initiatives, as well as for how they work with external clients and stakeholders and create software or programs for small, medium, and large businesses ranging from communications and sports to health care providers. the media, too. Traditional development methods encourage a "responsive-based approach" to issues or problems and place an emphasis on a "smart, engine-based strategy" that combines extended distribution, integrated processes, and complicated reuse. On the other hand, considering the quantity of individuals and their connections adds to the difficulties of software development in previous approaches to the unexpected world.

Agile Principles: Following are the list of principles followed by agile development methodology:

1. The ultimate goal is to provide a reliable and efficient software.

2. Projects should be made in a dedicated surrounding, where people intend to complete their work with their working life-style freedom.

3. The direct communication is the best way for sharing information in a secured and full-filling manner.

4. The parameter of software development is portion of work done.

5. Creativity and proficiency are focused for increasing agility.

6. Great designs, building and details are built through self-organized teams. Self-organizing teams provide the greatest designs, constructions, and specifications.

Advantages:

Few advantages of Agile methodology are as follows :

1. **No need to go into details:**To begin working on development, you don't need to meet all of the requirements. The builds and testing begin as soon as the core prerequisites have been satisfied.

2. **Face to face interaction:** Proactive approaches to managing client-client and project team communications are highlighted in the prologue. As a result, there is no question about understanding and contribution..

3. **Minimum Marketing Time:** Clients can receive the finished product quickly using agile technique.

4. **Less processing expense for customers:** This results in cost and resource savings both for client and the supplier.

5. **High Quality:**The client will be delighted if the end product is of the greatest calibre as a consequence of the patient's involvement at every stage of software development.

Disadvantages:

Following are few disadvantages of Agile methodology :

1. **Low Plan Horizon:** In the case of active initiatives, inaccurate cost estimates and initial project efforts are prone to limited planning timeframes. This will be in charge of several analyses in the future.

2. **Less complicated design and documentation:** The risk for better design is bigger than the risk for better documentation throughout the entire project development and testing cycle.

3. **Unmistakable client focus:** The final product that customers want must be clearly envisioned in their comments. Because having a general understanding of it

could result in an unorganised product.

Life Cycle

At first look, the Software Development Life Cycle (SDLC) used in the development of agile systems appears to be comparable to the normal SDLC, but closer examination indicates that this is not the case. Due to active SDLCs' increased involvement, increased level of collaboration and dynamic nature, people are said to be stronger than standard projects. There are six steps in the active agile SDLC.

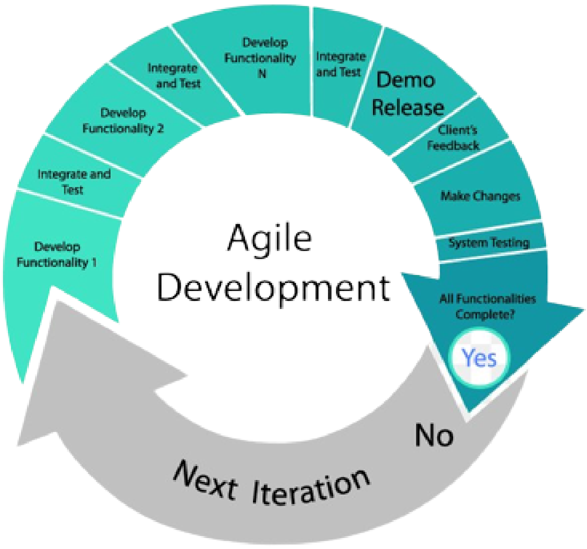


Figure 3.1: Life cycle of Agile system.

As shown in figure 3.1, active agile SDLC consists of 6 phases.

- **First iteration :** By choosing a project and ranking potential projects, this project category is utilised to decide how the Project would look. Before a potential project is taken into consideration, the theoretical concept for the project is produced, and its application is looked into.

- **Iteration zero/warming up :** Initiate the Project: In this phase the basic structure is built including finalizing all the requirements for the basic project by introducing a working space.

- **Iteration of Construction :**This will ensure a functional system that is flexible enough to adapt to the needs of multiple stakeholders. All of the following are required: stakeholder collaboration, cooperative development, model storming, testing design (TDD), diagnostics, and documentation. The program has now been internally installed.
- **Iteration of release :** The integration of software into manufacturing is the main objective of this stage. Training end users and product employees, distributing pilot tests, conducting final system and acceptance testing, completing paperwork, and educating passive shareholders are all parts of this process. When development is finished, the software or system is put into operation.
- **Production stage :** Currently, the software/system is supported and maintained. Fault in the system or program are discovered through this process, and changes are implemented.
- **Retirement stage :** This is done in order to entirely eliminate the system from the product. The last version of the system's data exchange is removed, and it also changes the customers and organisational model.

3.2 Architecture of the project

The figure 3.2 shows the architecture used for the project. We have 2 main organizations, a data owner and a data request or who will manage the data. The purpose of the project is to give the owner complete control over his data, which is why we will be implementing the Discretionary Access Control (DAC) policy. The architecture is based on Hyperledger Fabric, which contains different nodes for maintaining medical history. Hyperledger Fabric is a distributed ledger platform where all nodes in a hosted network. Each node has a hash key that is used to securely access data from offline storage. Off chain data can contain any data that is too large to be stored in the blockchain properly or that requires the ability to change or delete. Off chain data is classified as any orderly or irregular data that can be stored in a blockchain. In this structure, the patient record is off-chain data.

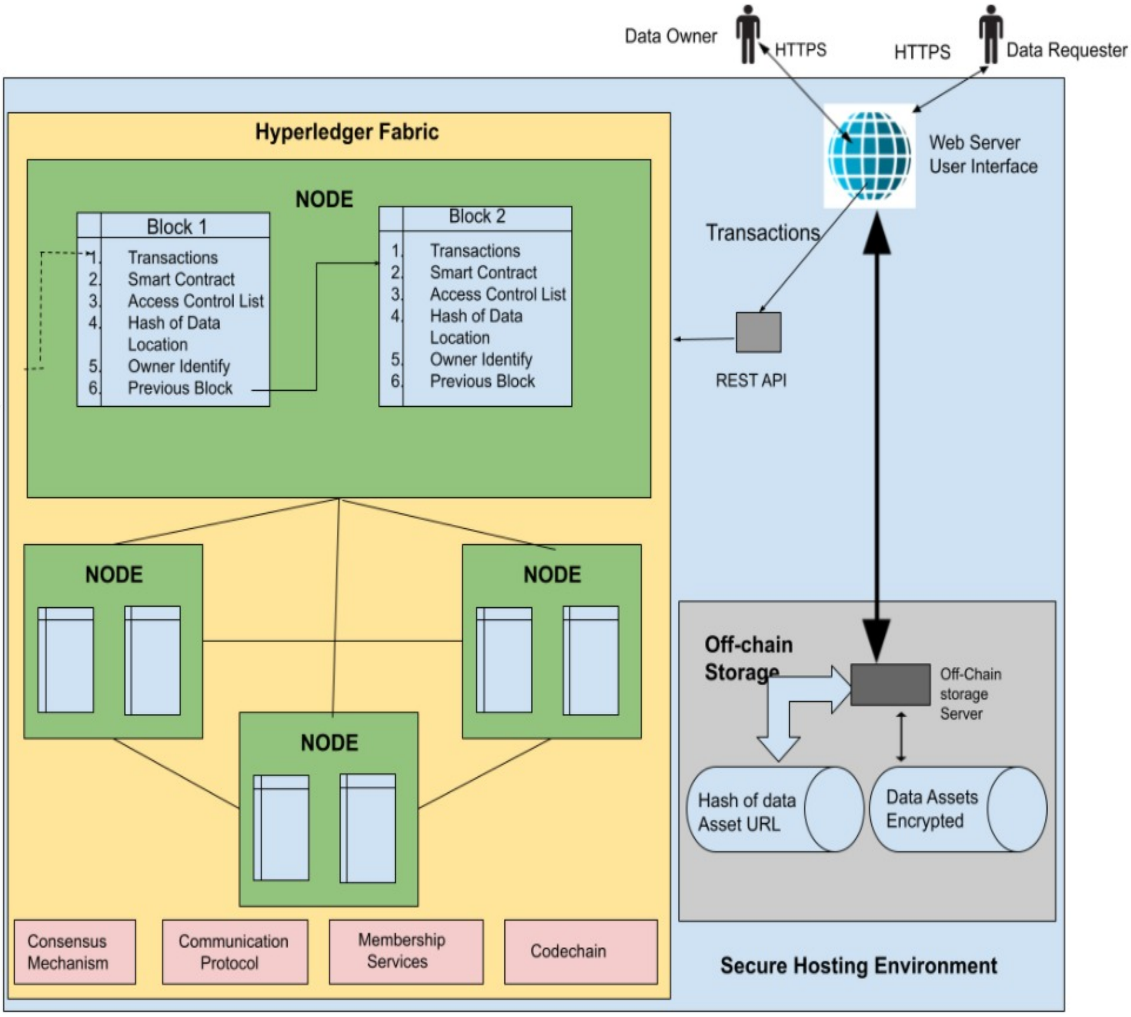


Figure 3.2: Project Architecture.

3.3 Functional Requirements

1. A straightforward web application that patients, physicians, medical facilities, and pharmacists may readily access from any location.

2. Users can update reports, retrieve data from reports after consent from the blockchain, and access medical data.

3. Doctors can update, add comments or refer treatments or drugs through the webapp

4. Pharmacies retrieve data from the reports and provide drugs accordingly.

5. Pathlabs perform tests and update reports in the UI.

6. Patients have real-time access to their reports containing all their medical history.

3.4 Non-Functional Requirement

1. **Blockchain:**

   A blockchain is a growing list of documents, known as blocks, that are cryptographically interlinked together. A cryptographic hash of the preceding block, a timestamp, and transaction data are all included in each block. The timestamp verifies that the transaction data was there at the time the block was released, allowing it to be hashed. The blocks form a chain, with each new block reinforcing the preceding ones as it contains the information of the previous block. As a result, since the data in any one block can never be modified retroactively without impacting all following blocks, blockchains are immune to data manipulation. We have two main entities, the data owner and the data requester who would be handling the data. The purpose of the project is to give the owner total control over their data, hence we will be using Discretionary Access Control (DAC) policy. The architecture is based on Hyperledger Fabric, which contains different nodes to store medical history. Each node has a hash key which is used to securely access data from off-chain storage. Each patient (the data owner) has its own blockchain and access to the blockchain that can be given to the data requester, like doctors, pharmacies, and hospitals for a specified period of time.

   The patient can give permanent consent as well to a requester in order to facilitate emergency access to retrieve data. To maintain the integrity of the data, the patient will have the option to check consent details given till a certain point in time. The application would also facilitate the fetching of reports and prescriptions both by the patient as well as the data requestors. The data requestors who have consent from the patient will have permission to add the blocks to the chain. The doctor can refer to tests and treatments which the patient has to go through and also prescribe drugs using the blockchain. In addition to this, the doctor can add comments and media to the blocks. When a patient visits a hospital a new prescription is made. In a similar way, hospitals will have the permission to create a new report inpatient blockchain. In addition, hospitals will have the functionality to register a patient for the treatment recommended by the doctor and start the treatment.

2. **Off-chain Storage:**

   The medical data management system will contain a huge amount of data that could not be accommodated on the block itself. In order to scale the system, we would need storage off the blockchain. This storage is called off-chain storage. The off-chain storage can be structured or unstructured storage that can contain a variety of data ranging from text to images. There are various issues with current on-chain storage: access issues, performance issues, security issues, success issues, and cryptographic issues. In order to avoid all these, we can use off-chain storage which is shared and secure. To harness the advantages of distributed systems, the project will be using a NoSQL database named CouchDB. CouchDb is a document-based database that facilitates both structured as well as unstructured data. It also is highly compatible with hyperledger and highly responsive to HTTP requests which makes the transaction easier and faster. The CouchDB also has a feature of replication and follows the ACID property which prevents any kind of data loss and maintains the atomicity of each and every transaction happening in the chain. The blocks in the blockchain will contain a hash value which will refer to the partition where the data is stored in the database.

3. **Consensus:**

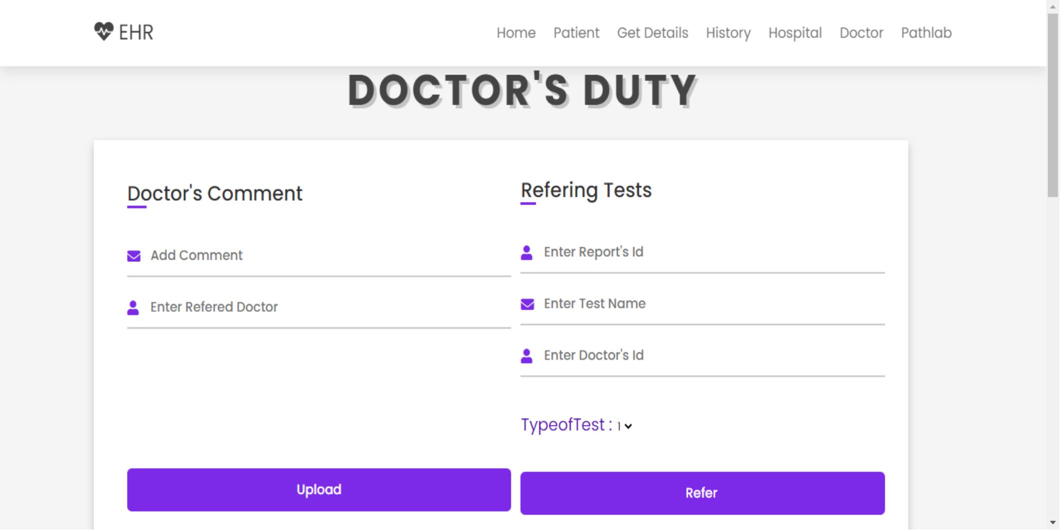
   The mechanism through which a network of nodes ensures transaction ordering and validates a block of transactions is known as consensus.Consensus, which is based on endorsement and consensus policies, confirms accuracy of the transactions made. To verify the accuracy of an ordered group of transactions in a block and, consequently, the outcomes of execution, it interacts with and depends on the smart-contract layer. The model presented in this project is patient-centric, and hence the patient holds the power of decision making in order to reach consensus. Once a patient gives permission, other entities like doctors, hospitals, and pharmacies can access the patient's data and participate in the consensus to agree upon a single, stable, and uniform state of the blockchain. The technical freedom to create channels between the entities to further ensure a safe and secure flow of data across entities allowed to participate in the channel. This in turn helps in creating a private network inside the blockchain between the chosen entities.

Chapter 4

Detailed Design

4.1 Interface Design

The user interface provides new users to register at our portal. After the new patient has registered to the site, they can provide their consent to the necessary authorities to view their medical records. After receiving the consent doctors can add their comments to their report. The application also has hospitals and doctors as separate entities, where the hospital is responsible for creating a report and starting treatment. On the other hand, the doctor has a couple of responsibilities like referring a test, treatment, or drugs to a patient, adding comments to a report, treatment as well as adding media files for a treatment. The interface also includes a path lab entity whose function is to provide test results and further upload them to our main blockchain storage. Apart from our entities, we have a history and details section which provides all previous medical data of a patient and details of the test, treatment, or reports of a particular patient ID respectively.



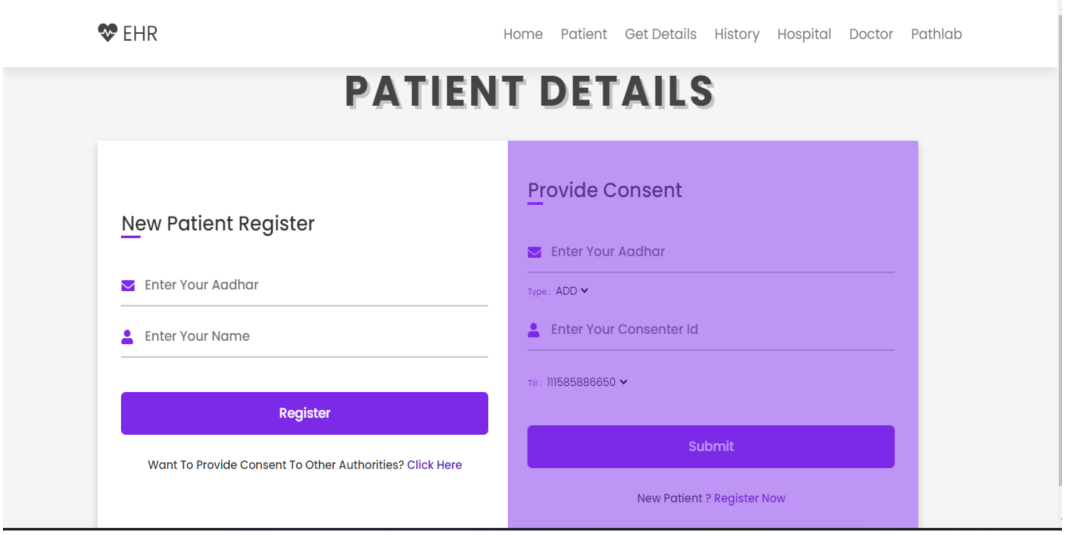
DOCTOR'S DUTY

Doctor's Comment

Refering Tests

Figure 4.1: User interface snapshot of doctor

Figure 4.1 is the snapshot of doctor's interface of the application, doctors can add comment to a patient's report also refer tests for a particular patient.



Type : ADD

Till : 111585886650

Want To Provide Consent To Other Authorities? Click Here

New Patient ? Register Now

Figure 4.2: User interface snapshot of patient

Figure 4.2 is the snapshot of the user interface of the patient entity. Using this functionality of the web app, the patients can register themselves on block using unique identity, aadhaar card. The patient also gets the functionality to give temporary access to the data using the UI.

4.2 Data Structures and Algorithms

4.2.1 Blockchain Data Structure

Blochain data structue is list of data, refered as blocks which are interlinked with the help of hash pointers. A cryptographic hash of the preceding block, a timestamp, and transaction data are all included in each block. The timestamp verifies that the transaction data was there at the time the block was released, allowing it to be hashed. The blocks form a chain, with each new block reinforcing the preceding ones as it contains the information of the previous block. As a result, since the data in any one block can never be modified retroactively without impacting all following blocks, blockchains are immune to data manipulation. The application would also facilitate the fetching of reports and prescriptions both by the patient as well as the data requestors. The data requestors who have consent from the patient will have permission to add the blocks to the chain. The doctor can refer to tests and treatments which the patient has to go through and also prescribe drugs using the blockchain. In addition to this, the doctor can add comments and media to the blocks. When a patient visits a hospital a new prescription is made. In a similar way, hospitals will have the permission to create a new report inpatient blockchain. In addition, hospitals will have the functionality to register a patient for the treatment recommended by the doctor and start the treatment.

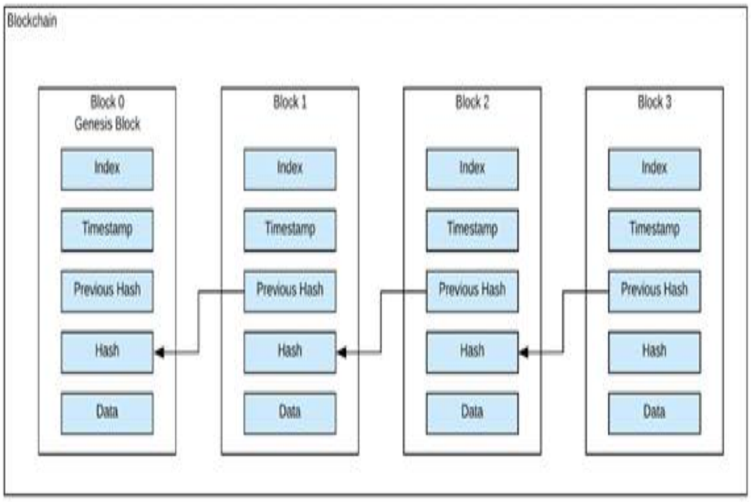


Figure 4.3: Structural diagram of a blockchain

Figure 4.3 is the structural diagram of a blockchain data structure. The nodes of the chain are connected with the hash pointer of their previous block and the first block is determined as genesis block. As all the nodes are connected with their previous block through hash pointers, any block in the blockchain could be traced using the same. This makes blockchain a reliable and secured data structure for implementation and real-time purposes.

4.2.2 SHA-256 Cryptographic Hash Algorithm

SHA-256 is part of the SHA(Secure Hash Algorithm)-2 family. The algorithm is used for most of the encryption-decryption processes. The 256 is significant for the digest value created after the hashing of the input text. The process is irreversible and always produces a hash value of 256 bits. This algorithm follows the general steps of hashing of SHA, which are padding bits, padding length, and initialization of buffer followed by the compression function. In this, the entire input text is broken into 512 blocks which are processed in a 64-round function, where the output of the current block is the input for the next block. After all 64 rounds of a block the output is taken as input for the next block for all of the 512 blocks. the end result of all these blocks is a 2556 hash digest created as the hash value for interlinking our nodes of a blockchain.

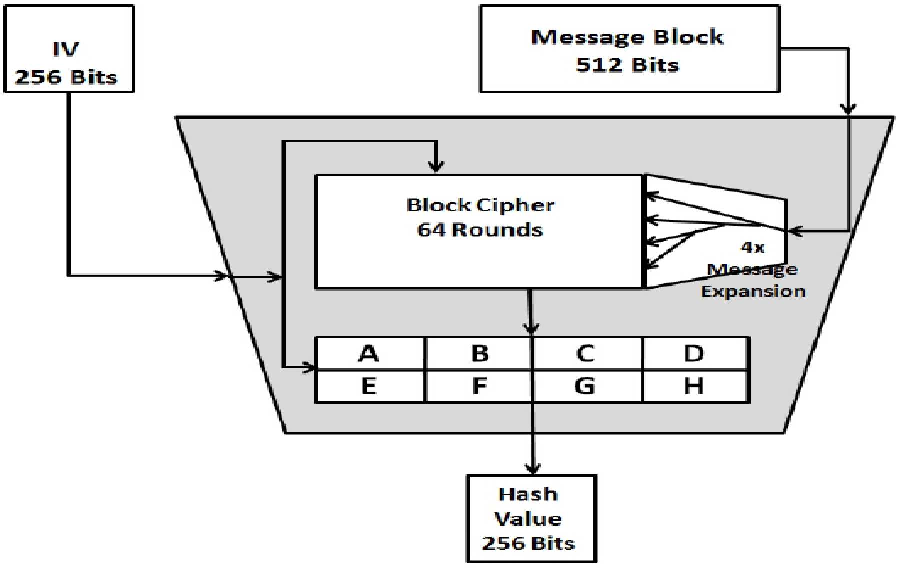


Figure 4.4: Compression function of SHA-256

Figure 4.4 is the compression function of SHA-256 which is responsible for compressing an input text bits to specific 256 bits of hash digest.

4.3 Data Source, Database used and Formats

4.3.1 Data Source

Data source is one of the most important component of your project as the sole purpose of the project is to create a decentralized storage for patient's data. In accordance with the model proposed, there are different data sources namely : patient, hospitals, doctor, and path lab, which can not manipulate but will be able to append into the patient's data. These various data source do not need to follow a specific format of data which is being sent as the storage will be document based. The storage of data and the database used is explained in next section.

4.3.2 Database used

Blockchain

A technology named Hyperledger fabric is used for blockchain. This system is a decentralized, distributed, and permissioned which means the ledger is not available for public access. Each block has a unique hash which is connected to parent block's hash. This provides a high security mechanism and is easily accessible. The technology used only supports append operation which ensures that the stored data cannot be manipulated by external entities.

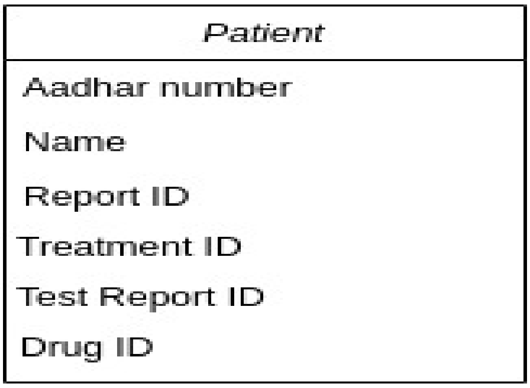
CouchDB

CouchDB is a document based database which is suitable when the structure of data is not defined and is complex. In this project CouchDB is used a state database. A state database stores the information of the blocks. Further CouchDB can be used to store data off the chain. This off chain storage will reduce the devlopment cost as well as the cost of storage in the blockchain. This will also facilitate the storage of multiple media files.

4.3.3 Formats

Patient Detail Storage

In order to identify a patient we need a unique ID for the patient. As shown in the figure 4.5, we are using Aadhaar number as the unique patient identifier for the patient entity. Alongside this identifier patient name is also stored. This helps to identify the patient and retrieve the medical history like treatments, report, drug which is being stored.



Patient

Aadhar number
Name
Report ID
Treatment ID
Test Report ID
Drug ID

Figure 4.5: Patient storage details

Chapter 5

Implementation

In this chapter, the detail of the project implementation was discussed. Explanation about the tools and technologies used are discussed in this chapter. The functionality of the project is explained using use-case and sequence diagram.

5.1 Tools and Technologies

1. **Hyperledger Fabric :**

   The Linux Foundation launched the open source, permissioned blockchain system known as Hyperledger Fabric in 2015. It is a general purpose, modular framework which provides distinctive identity management and access control features. As a result, it is appropriate for a range of business applications, including trade finance, loyalty and rewards programmes, track-and-trace of supply chains, and clearing and settlement of financial assets. For it's unique identity management feature and access control, in this project we have utilised hyperledger fabric to access medical records and track-and-trace the drug supply chain.

2. **NoSQL Database :** An alternative to the tabular relations used in relational databases, a NoSQL database offers a framework for the store and retrieval of data. Additionally, NoSQL databases frequently permit developers to directly alter the data's structure. NoSQL databases are employed because they have more easily understandable forms than the kinds of data models found in SQL databases.

3. **Programming Languages :** (JavaScript, Go) Making interactive web pages is possible with JavaScript, a scripting programming language used on both the client-side and server-side. We used JavaScript in the project to use Node.js.

   Go is an open-source programming language that makes it simple to create effective, dependable software. Go is easy to use and has relatively few nuances that take up time. Because it is straightforward and requires little upkeep, we have employed it.

4. **Postman :** An API platform for creating and utilising APIs is called Postman. In order to speed up the creation of better APIs, Postman streamlines cooperation and simplifies every stage of the API life cycle. Here, postman is utilised to create an API connection between the users and the blockchain.

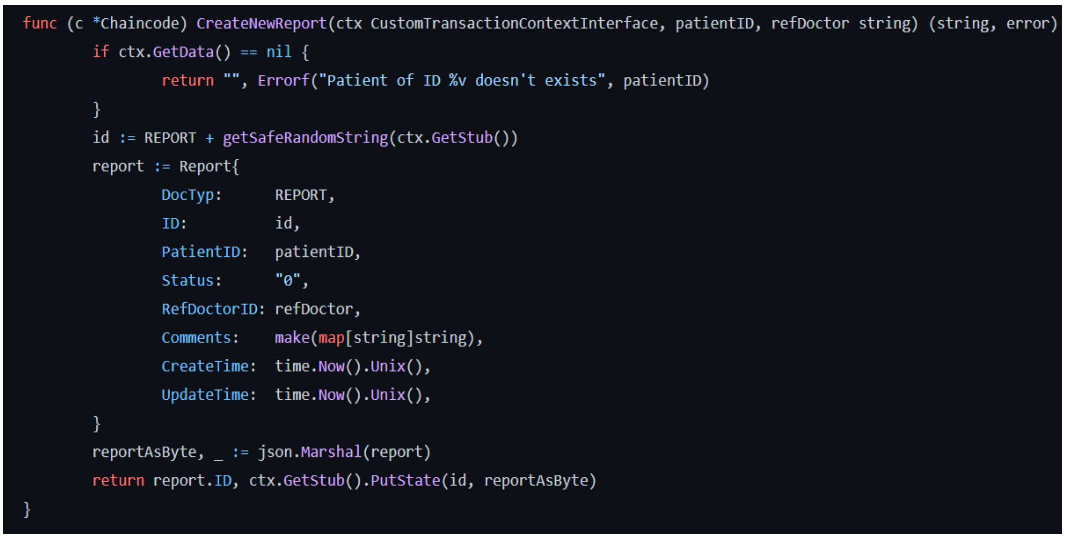
5. **NodeJs :** NodeJs is a Javascript based open-source run time environment which is used for back-end development. It is cross-platform and is powered by Javascript engine(V8 engine). It has the ability to execute code written in Javascript even outside of the browser. To provide a backend foundation and API for our blockchain, we chose nodeJs.

5.2 Implementation Workflow

The implementation of thee project is divided into 3 parts : Blockchain contract development, Node API development, Front-end Development and integration. Each of them are discussed in detail in this section.

5.2.1 Blockchain smart contract development

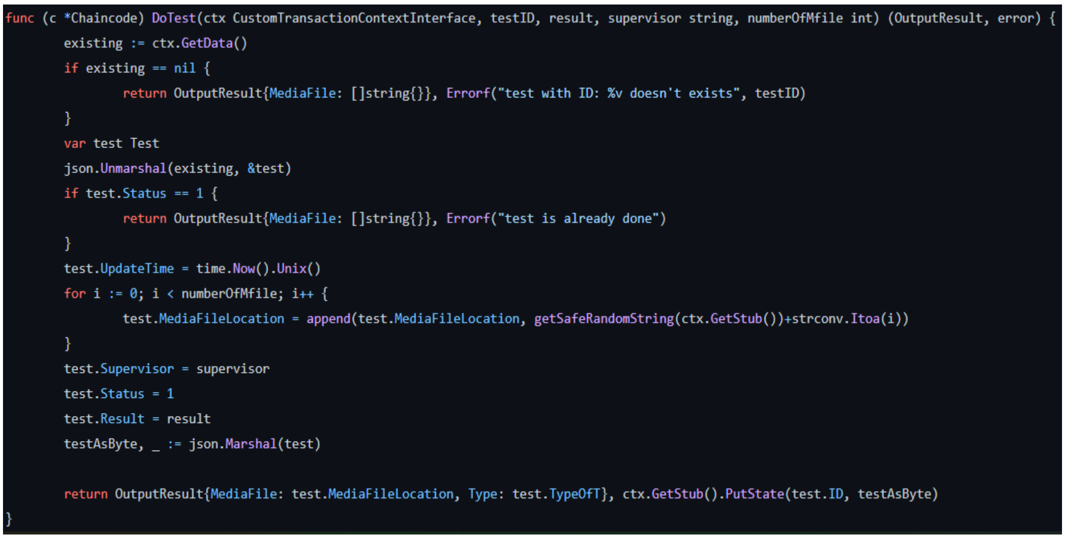
The smart contracts on Hyperledger fabric were built using goLang. There are 4 entities in the project, namely : Patient, Doctor, Hospital and PathLabs. All the entities have their individual contracts in order to come to consensus.



```
func (c *Chaincode) CreateNewReport(ctx CustomTransactionContextInterface, patientID, refDoctor string) (string, error)
        if ctx.GetData() == nil {
                return "", Errorf("Patient of ID %v doesn't exists", patientID)
        }
        id := REPORT + getSafeRandomString(ctx.GetStub())
        report := Report{
                DocTyp:      REPORT,
                ID:          id,
                PatientID:   patientID,
                Status:      "0",
                RefDoctorID: refDoctor,
                Comments:    make(map[string]string),
                CreateTime:  time.Now().Unix(),
                UpdateTime:  time.Now().Unix(),
        }
        reportAsByte, _ := json.Marshal(report)
        return report.ID, ctx.GetStub().PutState(id, reportAsByte)
}
```

Figure 5.1: Chaincode for hospital entity

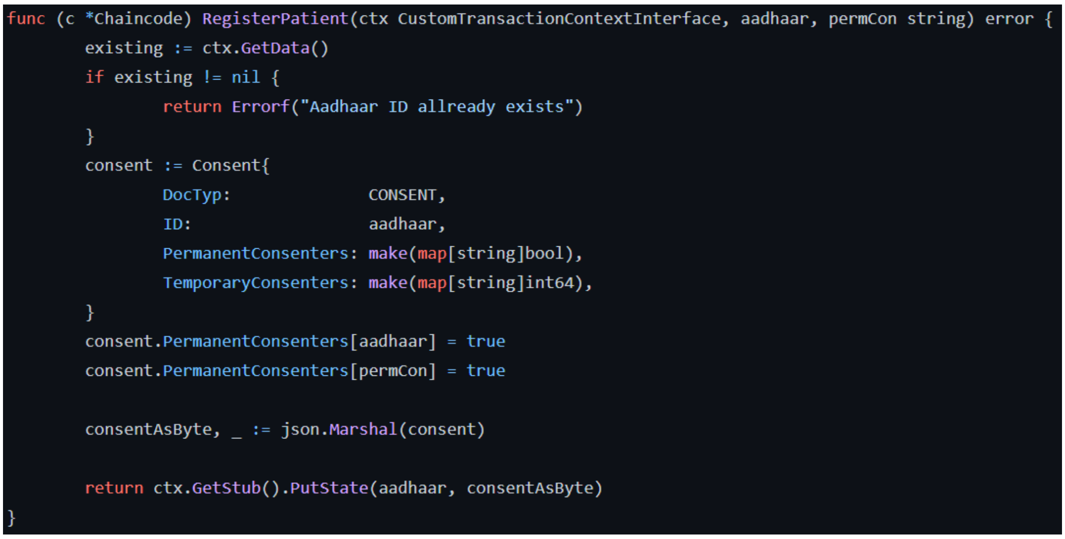
Figure 5.1 shows the smart contract for the hospital entity. The hospital entity has functionalities like make prescription, start treatment within the contract.



```
func (c *Chaincode) DoTest(ctx CustomTransactionContextInterface, testID, result, supervisor string, numberOfMfile int) (OutputResult, error) {
        existing := ctx.GetData()
        if existing == nil {
                return OutputResult{MediaFile: []string{}}, Errorf("test with ID: %v doesn't exists", testID)
        }
        var test Test
        json.Unmarshal(existing, &test)
        if test.Status == 1 {
                return OutputResult{MediaFile: []string{}}, Errorf("test is already done")
        }
        test.UpdateTime = time.Now().Unix()
        for i := 0; i < numberOfMfile; i++ {
                test.MediaFileLocation = append(test.MediaFileLocation, getSafeRandomString(ctx.GetStub())+strconv.Itoa(i))
        }
        test.Supervisor = supervisor
        test.Status = 1
        test.Result = result
        testAsByte, _ := json.Marshal(test)

        return OutputResult{MediaFile: test.MediaFileLocation, Type: test.TypeOfT}, ctx.GetStub().PutState(test.ID, testAsByte)
}
```

Figure 5.2: Chaincode for PathLab entity

Figure 5.2 shows the smart contract for the pathlab entity. The pathlab entity has functionalities like Upload test report within the contract.



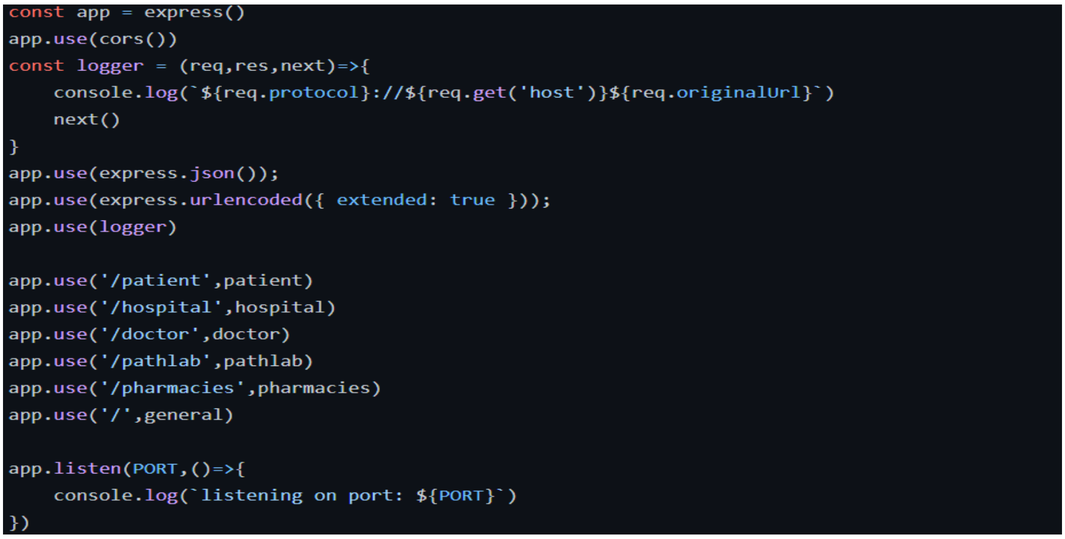
```
func (c *Chaincode) RegisterPatient(ctx CustomTransactionContextInterface, aadhaar, permCon string) error {
        existing := ctx.GetData()
        if existing != nil {
                return Errorf("Aadhaar ID allready exists")
        }
        consent := Consent{
                DocTyp:                CONSENT,
                ID:                    aadhaar,
                PermanentConsenters: make(map[string]bool),
                TemporaryConsenters: make(map[string]int64),
        }
        consent.PermanentConsenters[aadhaar] = true
        consent.PermanentConsenters[permCon] = true

        consentAsByte, _ := json.Marshal(consent)

        return ctx.GetStub().PutState(aadhaar, consentAsByte)
}
```

Figure 5.3: Chaincode for Patient entity

Figure 5.3 shows the smart contract for the patient entity. The patient entity has functionalities like register itself with unique ID (Adhara number) and giving consent to the requester for a certain period of time within the contract.

5.2.2 Node API development

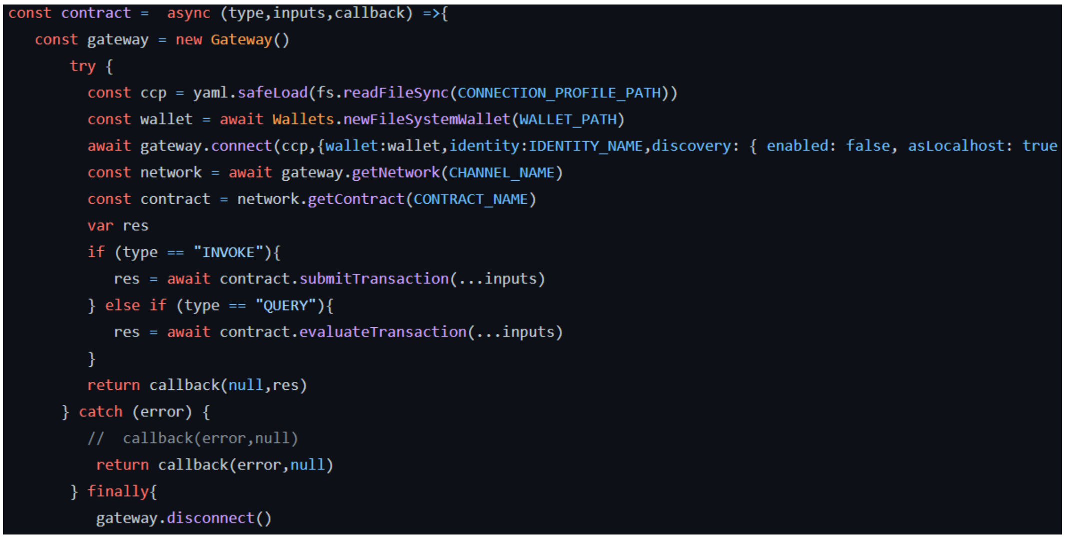
An API was developed in order to establish a communication between the frontend and the block chain. The API was developed using nodeJs and expressJs. The API establishes the routes to access different functionalities in order to put and retrieve the data from the blockchain.



```
const app = express()
app.use(cors())
const logger = (req,res,next)=>{
    console.log(`${req.protocol}://${req.get('host')}${req.originalUrl}`)
    next()
}
app.use(express.json());
app.use(express.urlencoded({ extended: true }));
app.use(logger)

app.use('/patient',patient)
app.use('/hospital',hospital)
app.use('/doctor',doctor)
app.use('/pathlab',pathlab)
app.use('/pharmacies',pharmacies)
app.use('/',general)

app.listen(PORT,()=>{
    console.log(`listening on port: ${PORT}`)
})
```

Figure 5.4: Registering of all the API routes

Figure 5.4 shows all the registered routes which can me accessed through node API, either by using postman or after integrating the front-end.



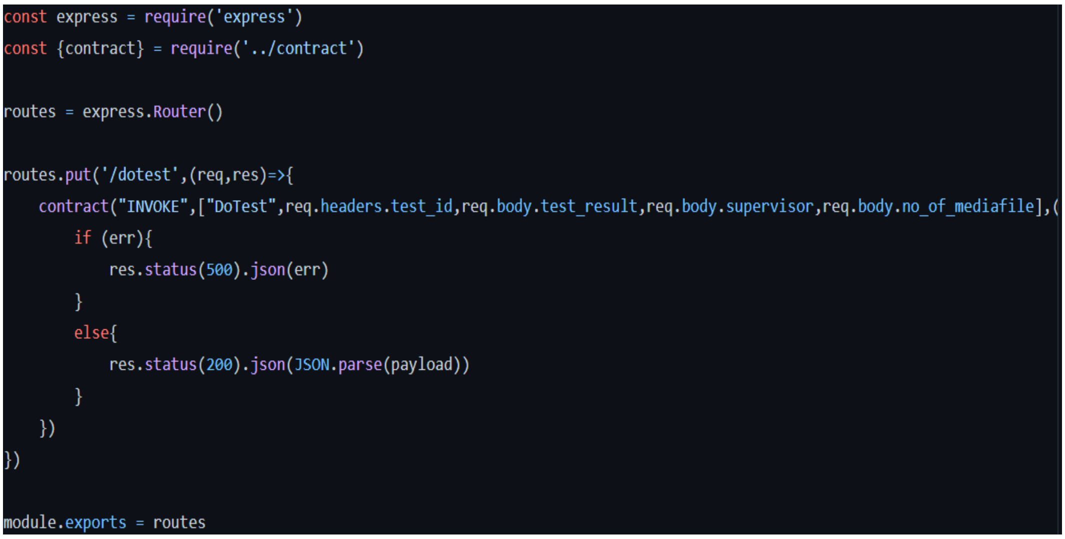
```
const contract =  async (type,inputs,callback) =>{
   const gateway = new Gateway()
       try {
         const ccp = yaml.safeLoad(fs.readFileSync(CONNECTION_PROFILE_PATH))
         const wallet = await Wallets.newFileSystemWallet(WALLET_PATH)
         await gateway.connect(ccp,{wallet:wallet,identity:IDENTITY_NAME,discovery: { enabled: false, asLocalhost: true
         const network = await gateway.getNetwork(CHANNEL_NAME)
         const contract = network.getContract(CONTRACT_NAME)
         var res
         if (type == "INVOKE"){
            res = await contract.submitTransaction(...inputs)
         } else if (type == "QUERY"){
            res = await contract.evaluateTransaction(...inputs)
         }
         return callback(null,res)
      } catch (error) {
         //  callback(error,null)
          return callback(error,null)
       } finally{
          gateway.disconnect()
```

Figure 5.5: Invoking contract from node API

Figure 5.5 shows the part of the project where the API call the contract in order to access different functionalities which have been implemented in the contract.

5.2.3 Front-end Development

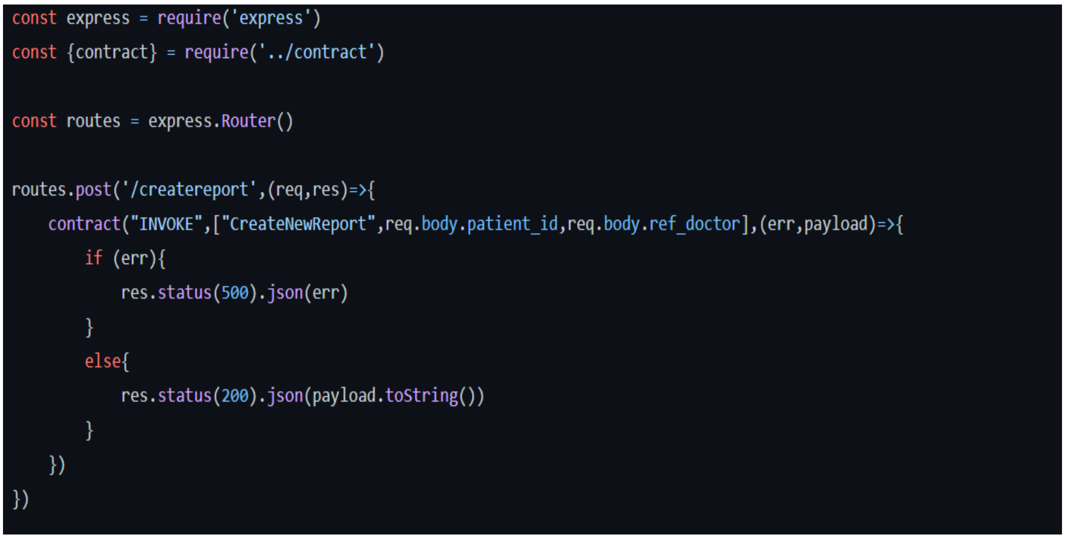
A web-page was developed for smooth user interaction. The web-page has different components for different entities. Patient can register and give consent to doctors in a very easy manner. The hospital, doctor, and pathlabs can update can update and retrieve the patient data.



```
const express = require('express')
const {contract} = require('../contract')

routes = express.Router()

routes.put('/dotest',(req,res)=>{
    contract("INVOKE",["DoTest",req.headers.test_id,req.body.test_result,req.body.supervisor,req.body.no_of_mediafile],(
        if (err){
            res.status(500).json(err)
        }
        else{
            res.status(200).json(JSON.parse(payload))
        }
    })
})

module.exports = routes
```

Figure 5.6: Script to access PathLab API from front-end

Figure 5.6 is the snippet of javascript code for front-end which shows the connection to API from which we can access the function of pathLab. In the front-end, the pathlab gets the functionality to upload the reports of the tests prescribed by the doctor, using testid.

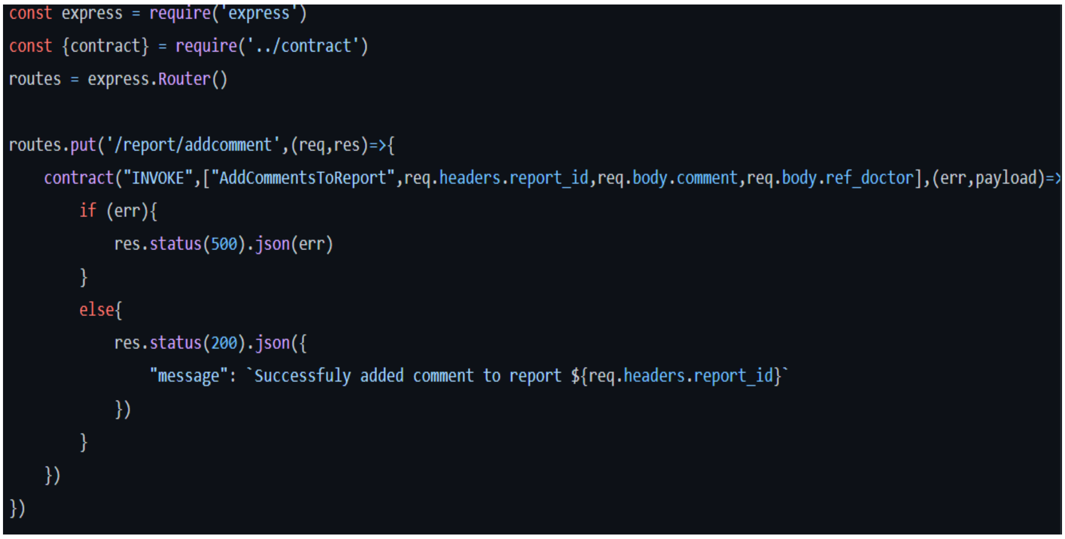


```
const express = require('express')
const {contract} = require('../contract')

const routes = express.Router()

routes.post('/createreport',(req,res)=>{
    contract("INVOKE",["CreateNewReport",req.body.patient_id,req.body.ref_doctor],(err,payload)=>{
        if (err){
            res.status(500).json(err)
        }
        else{
            res.status(200).json(payload.toString())
        }
    })
})
```

Figure 5.7: Script to access hospital API from front-end

Figure 5.7 is the snippet of javascript code for front-end which shows the connection to

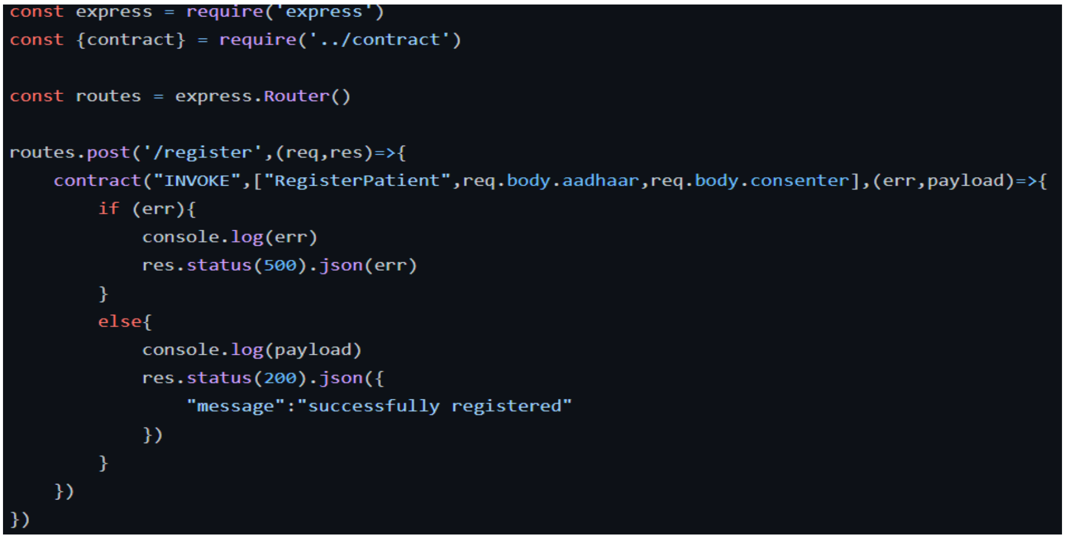
API from which we can access the function of hospital. In the front-end, the hospital gets the functionality to create report for a registered user and in turn creates a report id which is used by doctor in further process. Hospital also has the functionality to start the treatments which are recommended by the doctor.



```
const express = require('express')
const {contract} = require('../contract')
routes = express.Router()

routes.put('/report/addcomment',(req,res)=>{
    contract("INVOKE",["AddCommentsToReport",req.headers.report_id,req.body.comment,req.body.ref_doctor],(err,payload)=>
        if (err){
            res.status(500).json(err)
        }
        else{
            res.status(200).json({
                "message": `Successfuly added comment to report ${req.headers.report_id}`
            })
        }
    })
})
```

Figure 5.8: Script to access doctor API from front-end

Figure 5.8 is the snippet of javascript code for front-end which shows the connection to API from which we can access the function of doctor. In the front-end, the doctor gets the



```
const express = require('express')
const {contract} = require('../contract')

const routes = express.Router()

routes.post('/register',(req,res)=>{
    contract("INVOKE",["RegisterPatient",req.body.aadhaar,req.body.consenter],(err,payload)=>{
        if (err){
            console.log(err)
            res.status(500).json(err)
        }
        else{
            console.log(payload)
            res.status(200).json({
                "message":"successfully registered"
            })
        }
    })
})
```

Figure 5.9: Script to access patient API from front-end

functionality to refer tests, treatment, and drugs to patient. The doctor entity can also add comments during the treatment using the treatment ID produced by the hospital.

Figure 5.9 is the snippet of javascript code for front-end which shows the connection to API from which we can access the function of patient. In the front-end, the patient gets the functionality to register itself to the blockchain and create a block for itself using an unique ID (Aadhar in this case). It also has the sole authority to give consent to access it' data for defined time period.

5.3 Implementation

The overview of all the stakeholders and the code for their block chain to be created on hyperledger fabric is implemented.

This project leverages a hyperledger fabric (v2.0) network maintained to store a medical record of the patient securely with keeping the patient at the center. That means the medical record of any patient cannot be accessed without the consent of his/her. All the participants of the network like doctors, hospitals, pharmacies and private clinics will be given digital certificates by the Official Medical board of the country to join the network. Doctors will able to perform all the CRUD operations on their patient records.

5.3.1 UML diagrams

5.3.1.1 Use-case Diagram

The user with our safe and effective medical management system is depicted in the figure, 5.10. Let's examine the participants, use cases, and actions taken. The system, their kinds and actors are as follows:

1. **Primary actor:** Patient, Hospital, Doctors, Pharmacies, PathLabs
2. **Secondary actor:** Blockchain, Offchain storage
3. **System:** Secure and efficient medical management system

The Usecases represented are as follows:

1. **Login:** The patient registers to the system and a block is created in the blockchain in order to manage the patient data.
2. **Gives Consent:** The patient has the authority to give consent to other actors, i.e,

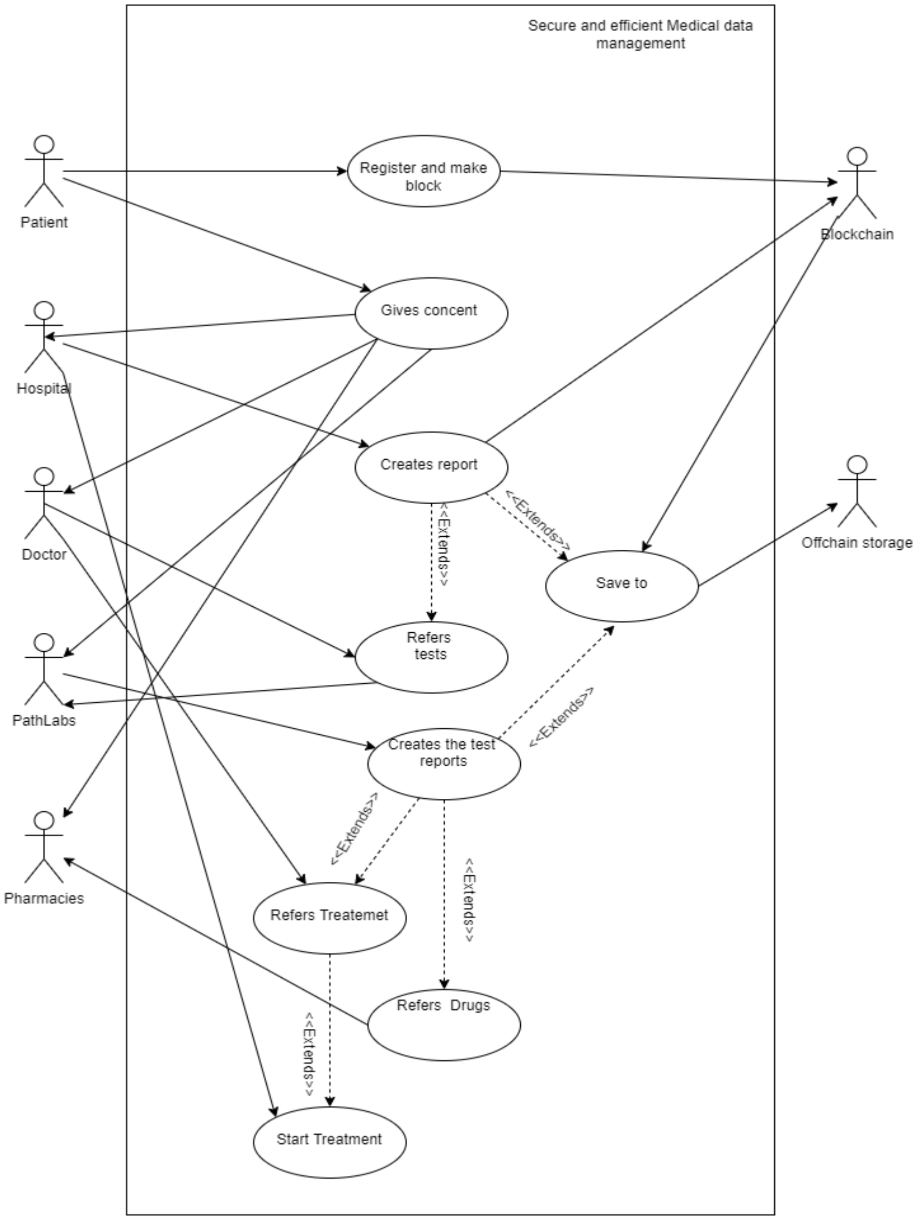


Figure 5.10: Use case Diagram of the medical data asset management system

doctor, hospital, pharmacies, and path labs. The patient has the authority to give permanent as well as temporary consent.

3. **Create report:** After receiving consent from the patient, the hospital creates a report for the patient.

4. **Refers Tests:** The doctor, after referring the report created, and acquiring consent from the patient, refers tests accordingly to the patient.

5. **Creates test report:** Path labs creates the test report from the patient, after acquiring consent.

6. **Refers Treatment:** After acquiring consent doctors recommends the needed treatment for the patient.

7. **Refers Drugs:** After acquiring consent doctors prescribe drugs to the patient. Later the patient can collect the same from pharmacies.

8. **Start Treatment:** After hospital assigns a doctor to the patient, they begin the treatment for the same.

9. **Saves to:** Every change made to the report including the test reports and comments from doctors are updated to the off-chain storage.

5.3.1.2 Sequence Diagram

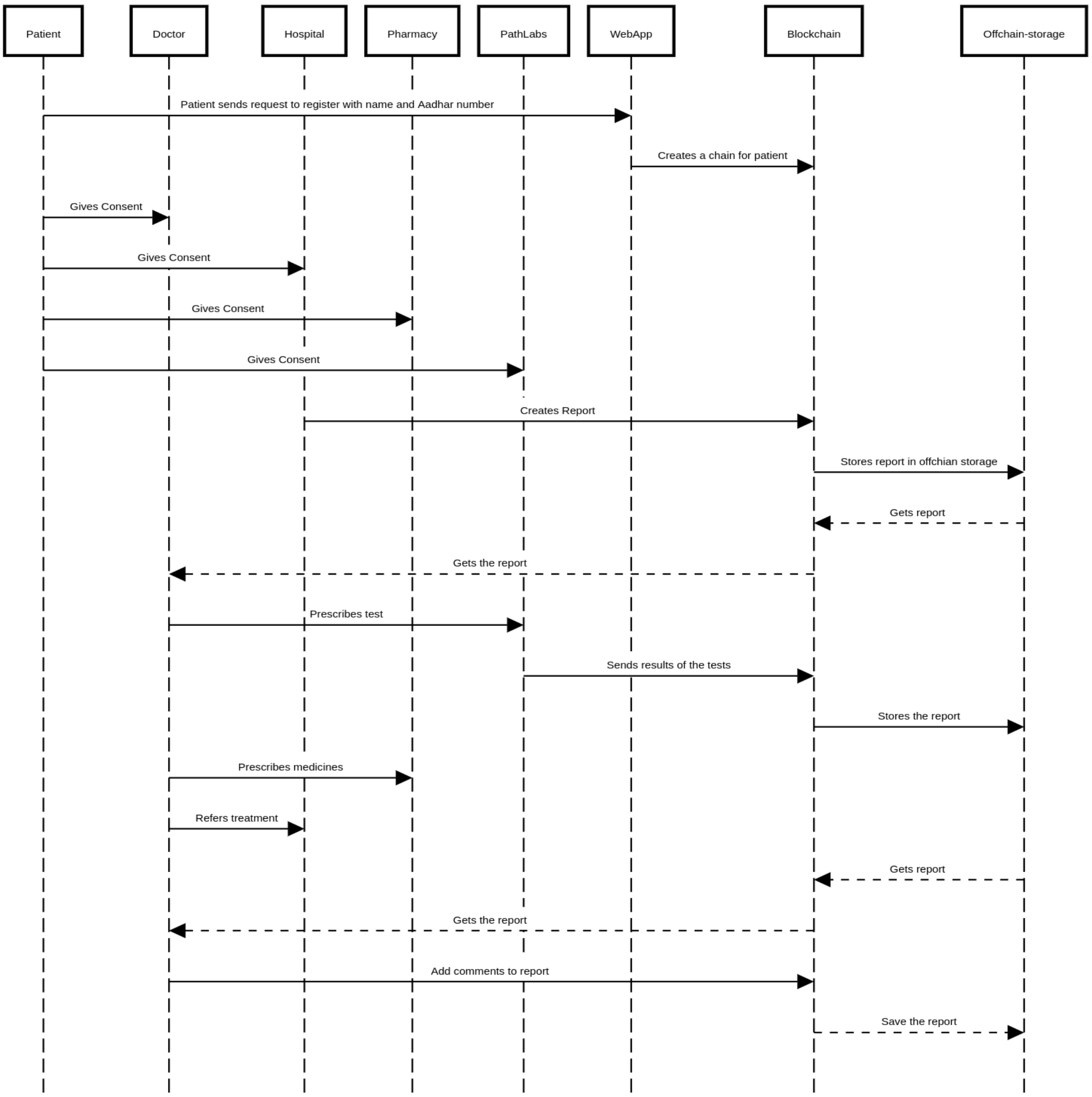


Figure 5.11: Sequence Diagram of the medical data asset management system

According to the figure 5.11 a patient requests the application to register themselves where a new block is created in the blockchain. Now, the patient gives consent to all the other entities i.e., doctors, hospitals, pharmacies and pathlabs to view their report. The hospital creates a report and updates the blockchain which is then stored in the off-chain storage. Consequently the off-chain data can be retrieved and produced to the hospital on demand. Doctors refer treatments, tests or drugs for a patient which is then reflected in their reports. The prescribed drugs are provided from the pharmacy, which is then tested by pathlabs and later updates the report in the blockchain. The treatment is carried out by the doctor who also adds comments to the reports which is reflected in the off-chain storage.

Chapter 6

Testing

Any software development process must include testing. Software testing is the stage that is most crucial. It examines the steady construction and displays the operating system's or framework's coding, specifications, and functionality. This phase, which involves unit testing and integration testing, is finished once each component or module has been developed. Every component is tested for performance and quality separately before being put through a second round of testing with the rest of the modules.

Different tests are written and executed when the frameworks or application requires testing. They are examined to see how it reacts, and inspected and see if there are some issues or errors. Test is carried taking into account certain test conditions anywhere within the app. If a mistake is discovered, it is evaluated for improvements, after which the engineer corrects it. The procedure of creating an error-free application is intended to service various user types in the market. There are significant reputational stakes for the developing organisation that must be carried out until the error-free application has been produced. There are instances where updates are made after end customers test the software and offer feedback. This section also includes discussion of significant test cases. This section also includes discussion of important test cases.

6.1 Unit Testing

Testing specific software modules or components is known as unit testing. It aims to make sure that every section of a software code functions as intended. Unit testing is done by engineers while they work on the software editing component. Unit tests are used to break out some of the code, which verifies its accuracy. Unit testing is used to parse and validate a section of the code. The unit could be a single procedure, method, or activity.

Each blockchain is tested by a unit test in Blockchain. In contrast to traditional testing, blockchain testing involves blocks, mining bags etc., which call for specific testing equipment.

6.1.1 Principles of Unit Testing

1. **Fast:**
   Unit tests must be performed quickly for effective development time. As their capacity to offer continuous, thorough, and quick feedback about the state of our system declines, so does the utility of the suite of unit tests.

2. **Isolated:**
   The test is independently detailed to make it simple to identify the reason for the failure. Separate test cases make it easier to spot faults than writing test cases based on other tests, which might cause false alarms.

3. **Repeatable:**
   Repeated tests are ones that yield consistent results over time. In order to undertake repetitive tests they must be kept apart from everything outside direct control. If the test is not done again, false test's findings will turn up and it will be unable to recover the cost of time spent chasing after imaginary issues.

4. **Self-validating:**
   Tests should be able to recognise if a result is expected or not. If the result has passed or failed must be determined. The outcomes must not be handled manually.

5. **Timely:**
   Unit tests are done at any time. It is done when the code is to be deployed.

6.1.2 Test Workflow

Before being used, the framework is tested using several methods. Here are a few instances of testing methods that are actually used:

6.1.2.1 Unit Based Testing

Unit tests are a form of software test that involve testing individual software modules or components. Its goal is to guarantee that the entire software code performs as planned. The developers finish the unit test as they work on the application during the development stage. Piece of code is defined and validated using unit testing. Units include any individual skill, approach, methodology, module, or thing. The engineer often tests the unit using the WhiteBox test approach. In the real world, though, time restraints or designers' aversion to testing force QA builds to reevaluate a unit.

Unit testing was done on different components in thus project, namely: blockchain containing smart contract, front-end and API. Once the contracts were written it was tested using terminal against all the possible test cases. The front end was tested for it's responsiveness and compatibility using different browsers.

6.1.2.2 Integration Testing

After integrating sub-code units and running a few tests against the integrated code, integration testing is carried out. The entire bit of software is regularly tested using a few new tests thanks to this collection and structured codes which are integrated in various locations and enormous code. We were able to assess whether the data collected from the actual servers was accurate after running unit tests on every component in our project, which would likely result in the finest forecast model imaginable. At a certain time, we had the choice to alter the information's source if it wasn't useful or practical for our application.

In this project, once the front-end was integrated with the back-end using the node API, integration testing was done to ensure successful requests and response from the front-end and the back-end. Test cases corresponding to user registration, consent, data entry, and data retrieval were tested. Some of the crucial test cases will be discussed in the next section of this report.

6.2 Test Case Details

6.2.1 Test Case ID: 1

Unit that has to be tested: User specific validation

Assumptions made during testing: The distinct user id input is properly validated, and a suitable error message is generated.

Data used for testing the specified testcase: Alphanumerical string

Steps to be performed during the testig of specified testcase:The entered string, which is under 8 characters long and need to be distinctive.

Result which is expected after the testcase is run: If the user ID is unique, register the user and create a block.

Result obtained: Register the user and make of block if user ID is unique.

Pass/Fail: Pass

6.2.2 Test case ID: 2

Unit that has to be tested: Validating consent

Assumptions made during testing: The user's input is properly validated in order to give consent to doctors, and a suitable error message is generated as a result.

Data used for testing the specified testcase: Alphanumerical string

Steps to be executed: Doctor ID should to be entered with the time till which the consent is given.

Result which is expected after the testcase is run: The only ID provided that has permission can view the patient's data.

Result obtained:The patient's data can only be accessed with the ID provided with permission.

Pass/Fail: Pass

6.2.3 Test case ID: 3

Unit that has to be tested: Integrating front-end and API

Assumptions made during testing: Convenient data asset exchange and a user interface that works well.

Data used for testing the specified testcase: Navigate through different entities and easy registration along with passing necessary arguments.

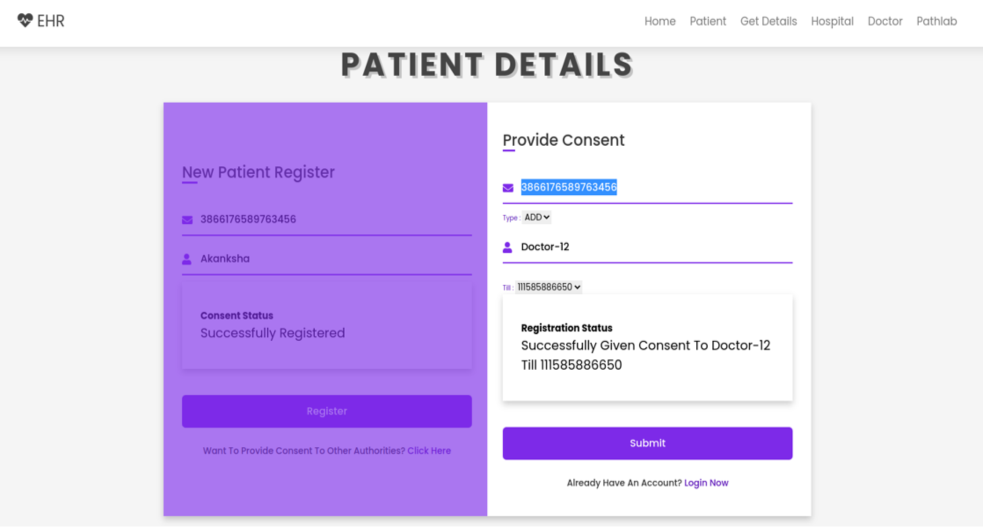
Steps to be executed: Send the front-end request that the back-end successfully processes.

Result obtained: Send request from the front end that the back end has successfully processed.

Pass/Fail: Pass

Comments: After properly registering, new users give their permission to the necessary entity, which then uses the information for subsequent operations.

6.3 Results


EHR
Home
Patient
Get Details
Hospital
Doctor
Pathlab
Register
Want To Provide Consent To Other Authorities? Click Here
Submit
Already Have An Account? Login Now

PATIENT DETAILS

New Patient Register

3866176589763456

Akanksha

Consent Status
Successfully Registered

Provide Consent

3866176589763456

Type : ADD

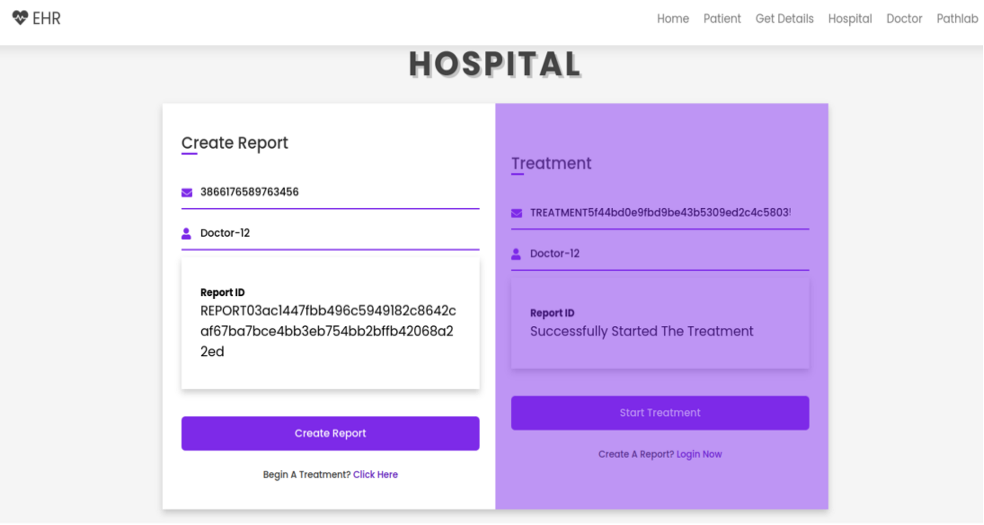
Doctor-12

Till : 111585886650

Registration Status
Successfully Given Consent To Doctor-12 Till 111585886650

Figure 6.1: User interface of patient entity

Figure 6.1 depicts the interface where patients can register themselves if they are new to the application as well as provide their consent to respective authority to access their reports.



HOSPITAL

Create Report

3866176589763456

Doctor-12

Report ID
REPORT03ac1447fbb496c5949182c8642caf67ba7bce4bb3eb754bb2bffb42068a22ed

Treatment

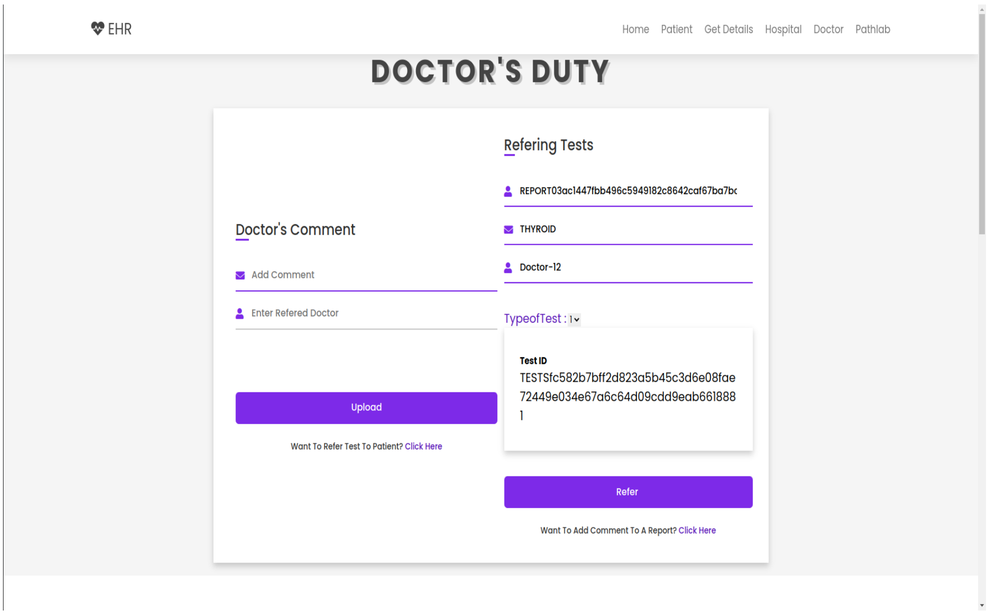
TREATMENT5f44bd0e9fbd9be43b5309ed2c4c5803!

Doctor-12

Report ID
Successfully Started The Treatment

Figure 6.2: User interface of hospital entity

Figure 6.2 shows the hospital's functionalities where, they create reports producing the hashed location of report. Also, hospital assigns the supervisor for starting of a patient's treatment.



DOCTOR'S DUTY

Doctor's Comment

Add Comment

Enter Refered Doctor

Want To Refer Test To Patient? Click Here

Refering Tests

REPORT03ac1447fbb496c5949182c8642caf67ba7bc

THYROID

Doctor-12

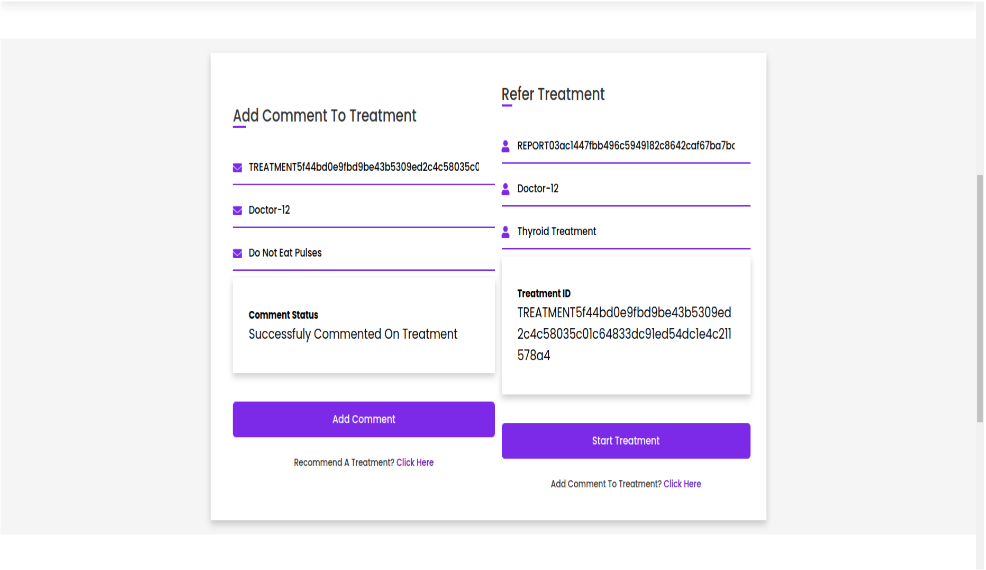
TypeofTest : 1

Test ID
TESTSfc582b7bff2d823a5b45c3d6e08fae72449e034e67a6c64d09cdd9eab6618881

Want To Add Comment To A Report? Click Here

Figure 6.3: User interface of doctor entity to add comments and refer test

Figure 6.3 shows doctor's function to add comment to a patient's report and referring a test for patient which in turn provides a test ID.



Add Comment To Treatment

TREATMENT5f44bd0e9fbd9be43b5309ed2c4c58035c0

Doctor-12

Do Not Eat Pulses

Comment Status
Successfuly Commented On Treatment

Recommend A Treatment? Click Here

Refer Treatment

REPORT03ac1447fbb496c5949182c8642caf67ba7bc

Doctor-12

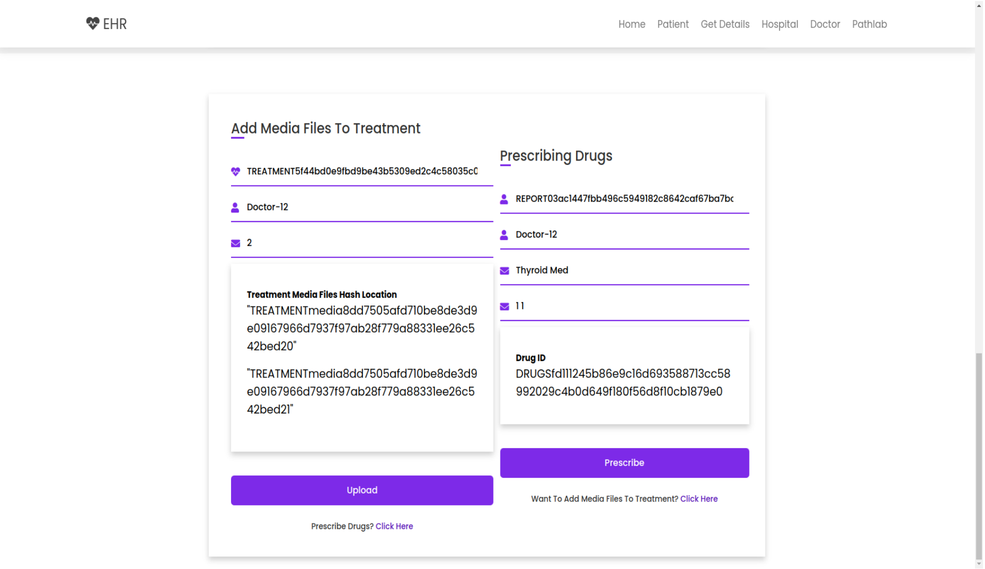
Thyroid Treatment

Treatment ID
TREATMENT5f44bd0e9fbd9be43b5309ed2c4c58035c01c64833dc91ed54dc1e4c211578a4

Add Comment To Treatment? Click Here

Figure 6.4: User interface of doctor entity for referring treatment and adding comment

Figure 6.4 shows doctor's can comment to patient's treatment and refer a treatment providing a treatment ID.



Add Media Files To Treatment

TREATMENT5f44bd0e9fbd9be43b5309ed2c4c58035c0

Doctor-12

2

Treatment Media Files Hash Location
"TREATMENTmedia8dd7505afd710be8de3d9e09167966d7937f97ab28f779a88331ee26c542bed20"

"TREATMENTmedia8dd7505afd710be8de3d9e09167966d7937f97ab28f779a88331ee26c542bed21"

Prescribe Drugs? Click Here

Prescribing Drugs

REPORT03ac1447fbb496c5949182c8642caf67ba7bc

Doctor-12

Thyroid Med

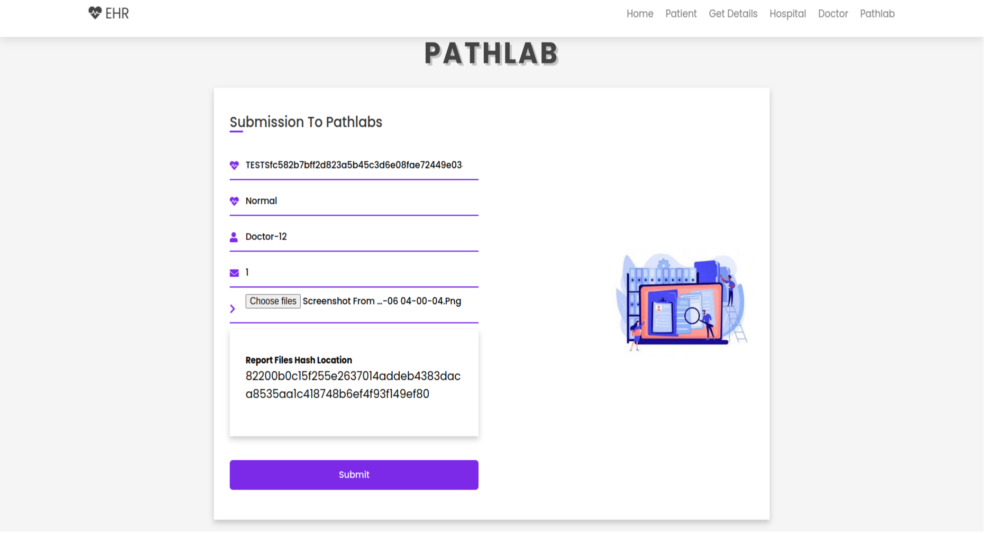
11

Drug ID
DRUGSfd111245b86e9c16d693588713cc58992029c4b0d649f180f56d8f10cb1879e0

Want To Add Media Files To Treatment? Click Here

Figure 6.5: User interface of doctor entity for adding media and referring drugs

Figure 6.5 shows doctors can add media files to a treatment where the hashed location of these media files are reflected. Also, doctors can refer drugs to patient providing a drug ID.



PATHLAB

Submission To Pathlabs

TESTSfc582b7bff2d823a5b45c3d6e08fae72449e03

Normal

Doctor-12

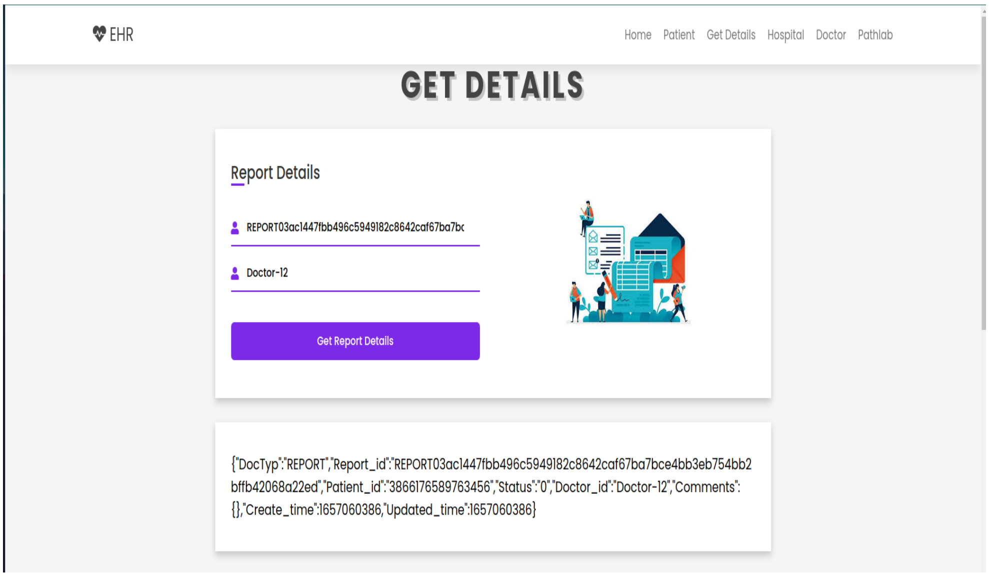
1

Screenshot From ...-06 04-00-04.Png

Report Files Hash Location
82200b0c15f255e2637014addeb4383daca8535aa1c418748b6ef4f93f149ef80

Figure 6.6: User interface of pathlab entity

Figure 6.6 shows the results of a test conducted by pathlab are provided which are stored in the blockchain consequently and provide us the file location of the test report.



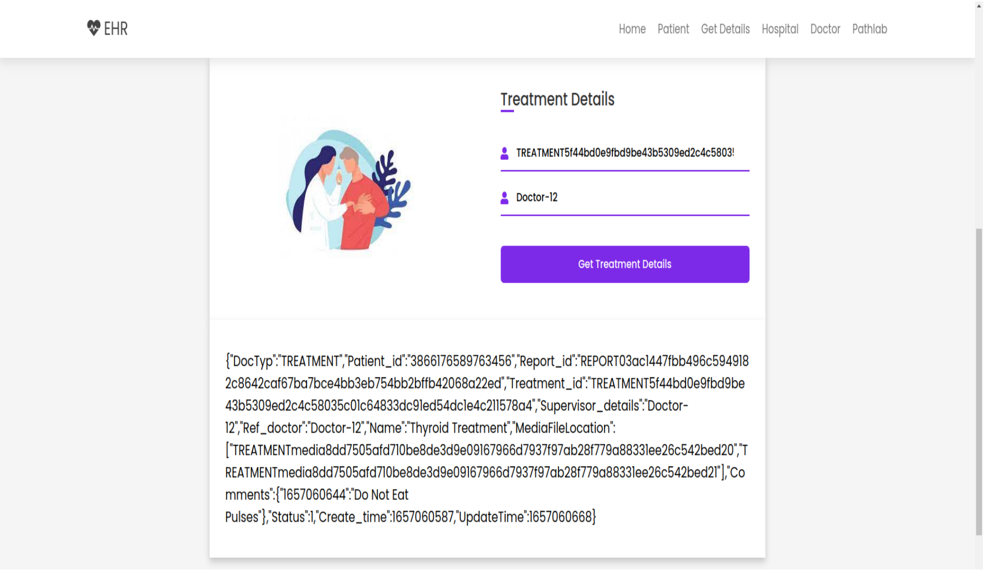
REPORT03ac1447fbb496c5949182c8642caf67ba7bc

Doctor-12

```
{"DocTyp":"REPORT","Report_id":"REPORT03ac1447fbb496c5949182c8642caf67ba7bce4bb3eb754bb2
bffb42068a22ed","Patient_id":"3866176589763456","Status":"0","Doctor_id":"Doctor-12","Comments":
{},"Create_time":1657060386,"Updated_time":1657060386}
```

Figure 6.7: User interface to review report details

Figure 6.7 depicts the interface where concerned authority can view their report details by providing their report ID and their supervisor's ID.



TREATMENT5f44bd0e9fbd9be43b5309ed2c4c5803!

Doctor-12

```
{"DocTyp":"TREATMENT","Patient_id":"3866176589763456","Report_id":"REPORT03ac1447fbb496c594918
2c8642caf67ba7bce4bb3eb754bb2bffb42068a22ed","Treatment_id":"TREATMENT5f44bd0e9fbd9be
43b5309ed2c4c58035c01c64833dc91ed54dc1e4c211578a4","Supervisor_details":"Doctor-
12","Ref_doctor":"Doctor-12","Name":"Thyroid Treatment","MediaFileLocation":
["TREATMENTmedia8dd7505afd710be8de3d9e09167966d7937f97ab28f779a88331ee26c542bed20","T
REATMENTmedia8dd7505afd710be8de3d9e09167966d7937f97ab28f779a88331ee26c542bed21"],"Co
mments":{"1657060644":"Do Not Eat
Pulses"},"Status":1,"Create_time":1657060587,"UpdateTime":1657060668}
```

Figure 6.8: User interface to review treatment details

Figure 6.8 depicts the interface where concerned authority can view their treatment details by providing their treatment ID and their supervisor's ID.

Chapter 7

Conclusions and Future Scope

7.1 Conclusion

As the earth moves forward, all aspects of life are measured in terms of time and energy. To keep up with the current situation, the medical system needs to be improved. Another form of health care improvement is to facilitate access to and retrieval of data assets between patients, physicians, and caregivers while at the same time maintaining a secure protocol for access to private data assets.

For this project, we use a medical data asset management system using a blockchain. This project focuses on providing an easy way to facilitate the retrieval and maintenance of a personal health record using a blockchain data structure that makes the data stored on each block unchangeable.Since each block in a blockchain contains a copy of the entire chain and is linked to the preceding block by a hash value, it should be difficult to mathematically break a block that has been modified. And which leads to the blockchain becoming a highly secure data archive for keeping medical records.

Limiting who can update or add data to the blockchain also helps provide security or resistance to any type of impersonation. This is done using public and private keys, where private keys only limit users who are authorized to update records. In the case of medical data, only hospitals and physicians are allowed to review the results of tests, recommendations, or treatment analyzes.

Ultimately, this project aims to play a key role in health care and data management of patient assets so that they can update their new reports and receive the required report analysis and instructions from a physician while also ensuring the integrity of their data. is saved.

7.2 Future Scope

- **Scalability:** Prospectively, this application can be used by multiple hospitals and medical professionals. The scalability of hyperledger can be broadened by increasing the number of nodes for each user interface in the future as well.

- **Off-chain storage:** An off-chain storage could be used to store media files in order to enhance the performance of blockchain as well as reduce the cost of storage.

Chapter 8

Published Paper

The paper named “Blockchain Based Medical Data Asset Management System” has been presented at “Thirteenth International Conference on Advances in Computing, Control, and Telecommunication Technologies - ACT 2022” in the special issue of the GRENZE International Journal of Engineering and Technology - GIJET on 26th June 2022.

Bibliography

[1] Fan, K., Wang, S., Ren, Y. et al. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J Med Syst 42, 136 (2018). https://doi.org/10.1007/s10916-018-0993-7.

[2] Griggs, K.N., Ossipova, O., Kohlios, C.P. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42, 130 (2018). https://doi.org/10.1007/s10916-018-0982-x.

[3] V. M. Harshini, S. Danai, H. R. Usha and M. R. Kounte, "Health Record Management through Blockchain Technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1411-1415, doi: 10.1109/ICOEI.2019.8862594.

[4] S. Hasavari and Y. T. Song, "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), 2019, pp. 71-75, doi: 10.1109/SERA.2019.8886792.

[5] Y. Yu, Q. Li, Q. Zhang, W. Hu and S. Liu, "Blockchain-Based Multi-Role Healthcare Data Sharing System," 2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM), 2021, pp. 1-6, doi: 10.1109/HEALTHCOM49281.2021.9399028.

[6] L. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla, "Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-7, doi: 10.1109/CAMAD.2019.8858469.

[7] Hannah S Chen†, Juliet T Jarrell†, Kristy A Carpenter, David S Cohen, Xudong Huang* Department of Psychiatry, Massachusetts General Hospital and Harvard Medical School, USA.

[8] M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem, “MedAccess: A Scalable Architecture for Blockchain-based Health Record Management,” 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257720.

[9] R, Lokesh N, Suhail Khan, Saifulla. (2021). Block Chain Based Supply Chain Management for Counterfeit Drugs in Pharmaceutical Industry. International Journal of Scientific Research in Computer Science, Engineering and Information Technology. 100-108. 10.32628/CSEIT217122.

Project Planning AY-2021-22

Activites	No.Of Weeks	Plan/ Actual	Septmeber				October				November			December				January			Feb		March			April				May				June				July		
			1	2	3	4	1	2	3	4	1	2	3	1	2	3	4	1	2	3	1	2	1	2	3	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3
Problem Identification and Literature Survey	6W	Plan	🟦	🟦	🟦	🟦	🟦	🟦																																	
		Actual	🟥	🟥	🟥	🟥	🟥	🟥																																	
Software Requriments and Specifications	3W	Plan							🟦	🟦	🟦																														
		Actual							🟥	🟥	🟥																														
Architecture, Design and Prototype	4W	Plan										🟦	🟦	🟦																											
		Actual										🟥	🟥	🟥	🟥																										
Implementation	10W	Plan																		🟦	🟦	🟦	🟦	🟦	🟦	🟦								🟦						
		Actual																			🟥	🟥	🟥	🟥	🟥	🟥								🟥						
Testing and Validation	3W	Plan																								🟦	🟦	🟦						🟦	🟦	🟦			
		Actual																								🟥	🟥	🟥						🟥	🟥	🟥			
Project Closure - **Results Observations** **-Demonstration** **-Report Writing**	3W	Plan																											🟦	🟦	🟦						🟦	🟦	🟦
		Actual																											🟥	🟥	🟥						🟥	🟥	🟥

Cost Estimation

Project cost estimation is the process of predicting the quantity, cost, and price of the resources required by the scope of a project. Since cost estimation is about the prediction of costs rather than counting the actual cost, a certain degree of uncertainty is involved. The cost estimate is used to determine the size of the required investment to create or modify assets. It is also during the early phases that alternative plans are considered that need to be priced. It covers activities such as resource planning, cost estimating, budgeting and cost control. These activities are repeated in a closed loop and take place during the whole project life cycle.

Name	**Cost**
Internet Charges	5000
Report	4000
Travelling Cost	1000
Miscellaneous	1000
Total	11000

PO ATTAINMENT

Programme Outcomes (POs):		Task Preformed	Attainment				
			Excellent 5	Very Good 4	Good 3	Fair 2	Poor 1
PO1	Engineering knowledge	1. Applied the knowledge of Development, Programming and Software Engineering.		✓			
PO2	Problem analysis	1. Literature Survey done on "Chat-bot methodology" 2. Behaviours of students during course and quiz. 3. The objectives of the project were set. 4. Knowledge of Development, Programming and Software Engineering was found to be useful in implementing the project		✓			
PO3	Design/development of solutions	1. Solutions are developed for the following: Monitor the behaviour of students with the way they talk. 2. Decreasing the dependency of other websites used by students during course. 3. Monitor the applications and system processes running on the client systems.	✓				
PO4	Conduct investigations of complex problems	1. Requirements for chatbot is gathered through Literature Survey. 2. Behaviour patterns of students indulged in other activities is also studied. 3. Suitable solutions to meet the requirements are developed.		✓			
PO5	Modern tool usage	1. Visual studio, Flutter, Firebase, Android Studio, Git, Technology is used	✓				
PO6	The engineer and society	1. This project helps to reduce dependency on other websites and monitor students so that they concentrate on the assigned work.		✓			

Programme Outcomes (POs):		Task Preformed	Attainment				
			Excellent 5	Very Good 4	Good 3	Fair 2	Poor 1
PO7	Environment and sustainability	1. This project meets some of the current requirements of admin to help him maintain ethical standards of study work in academic institutions. 2. This project is upgradable with additional monitoring features required for the changing generation of students and is thus sustainable.			✓		
PO8	Ethics	1. This project is useful to teach students and prepare them for examinations. 2. It is also useful to take care that the students concentrate on studies, work and do not get distracted towards non-academic websites when internet facility is provided. 3. References are quoted. 4. Report is prepared by students and plagiarism check is made with turnitin software.		✓			
PO9	Individual and team work	1. Each student took up the responsibility of executing one module of the project. 2. The report content was contributed by each of the team members. 3. Integration of the modules was done as a team work. 4. Incorporating the suggested changes was done in a 5. As a team presentations and demo of the project was given	✓				

Programme Outcomes (POs):		Task Preformed	Attainment				
			Excellent 5	Very Good 4	Good 3	Fair 2	Poor 1
PO10	Communication	1. Phase-wise presentation and Demo of progress of project work before the panel. 2. Presentation and Demonstration of project before Industry Experts. 3. Preparation of Report spread across the entire Semester. 4. Regular interaction with Guide and Panel members to incorporate the suggestions given during evaluations 5. Answering queries during presentations and Demos.			✓		
PO11	Project management and finance	1. Project Scheduling using Gantt Chart. 2. Maintaining Project Diary. 3. Estimating Man Hour Requirement			✓		
PO12	Life-long learning	1. Working on Flutter technology. 2. Reading papers and articles on Chatbots.		✓			

medical data asset final report

by Akanksha S

Submission date: 15-Jul-2022 10:12AM (UTC+0530)
Submission ID: 1870738885
File name: major_plag_B2.pdf (2.69M)
Word count: 8514
Character count: 44687

medical data asset final report

ORIGINALITY REPORT

7 %	2%	0%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Visvesvaraya Technological University, Belagavi Student Paper	4%
2	github.com Internet Source	1 %
3	Submitted to RMIT University Student Paper	1 %
4	Submitted to SIM Global Education Student Paper	<1 %
5	Submitted to University of Bridgeport Student Paper	<1 %
6	Submitted to British University in Egypt Student Paper	<1 %
7	Submitted to WorldQuant University Student Paper	<1 %
8	"OMD: A Compression Function Mode of Operation for Authenticated Encryption", Lecture Notes in Computer Science, 2014. Publication	<1 %

9	Submitted to Yeditepe University Student Paper	<1 %
10	coek.info Internet Source	<1 %
11	Joseph Holbrook. "Blockchain Development", Wiley, 2020 Publication	<1 %

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	Off		

VITAE

Name: Akanksha Srivastava USN: 1SI18CS007 DOB: 26/10/2000 Permant Address: 56, ward no. - 09, Dumwaliya, Bagaha-2, Bihar - 845105 Phone No.: 9166894355 Email: akankshabsrivastava@gmail.com CGPA: 8.78(Upto 7th Sem) Placed: Yes CTC: 10	
Name: Khalid Farooq USN: 1SI8CS046 DOB: 14/05/1999 Permant Address: dragmullah, ahlan gadool, anantnag, J&K - 192202 Phone No. 9797436494 Email: wandererkhalid@gmail.com CGPA: 8.1(Upto 7th sem) Placed: Yes CTC: 12	
Name: Rakshitha B EUSN: 1SI18CS085 DOB: 12/11/2000 Permant Address: Dhavalagiri house, Vijayanagar Layout, Bannur p/o, Padil, Puttur, D.K., Karnataka - 574203 Phone No. 8722072545 Email: rakshitabantwal1@gmail.com CGPA: 8.58(Upto 7th sem) Placed: Yes CTC: 12	

Name: Rishika Kumari USN: 1SI8CS087 DOB:13/10/1999 Permant Address: Phase 1, Vaishnow Devi Nagar, Kathal more, Ratu, Ranchi, Jharkhand - 835303 Phone No. 9955140780 Email: rishikaojha1310@gmail.com CGPA: 9.29(Upto 7th sem) Placed:Yes CTC:12	

Blockchain Based Medical Data Asset Management System

[1]Akanksha Srivastava, [2]Khalid Farooq, [3]Rakshitha B, [4]Rishika Kumari, [5]Shruthi K, [6]A. S. Poornima, [7]M. B. Nirmala
[1-4] UG student, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: {akankshabsrivastava, wandererkhalid, rakshitabantwal1, rishikaojha1310}@gmail.com
[5] Assistant Professor, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: shruthik@sit.ac.in
[6]Professor, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: aspoornima@sit.ac.in
[7]Associate Professor, Computer Science and Engineering, Siddaganga Institute of Technology
Tumkur, India
Email: mbnirmala@sit.ac.in

***Abstract*—In today's health care management, medical health records are in the form of electronic medical record (EHR/EMR) systems. These systems store a patient's medical history in a digital format. However, a patient's medical data being acquired in an efficient and timely manner is proven to be difficult through these records. Health management is always hindered by the inability to acquire information, less usage of information acquired, unmanageable privacy controls, and poor data asset security. In this paper, we are introducing an efficient as well as a secure medical data asset management system using blockchain in order to resolve these issues. Blockchain technology eases the accessibility of all such records by maintaining a block for every individual patient. This paper proposes an architecture using an off-chain solution that will enable doctors, and patients to access records in a safe way. Blockchain makes medical records immutable and encrypts them for data integrity. Users can observe their health records, but only patients own the private key and can only share it with whom they desire. The smart contracts also help our data owners to manage their data access in a permissioned manner. The final result will be viewed as a web and mobile interface to easily access, detect as well as ensure high-security data.**

***Index Terms*—Medical data, Management, Blockchain, Web and mobile application.**

I. Introduction

One of the biggest issues faced worldwide in the healthcare and medical sector is the incapacity for medical data to be acquired in an efficient and timely manner. All electronic medical record or electronic health record (EMR/EHR) systems presume that each patient approaches medical practitioners in one clinic or in the common state or province. These systems are only centered around the same practitioner and the use of such information is not useful nor accurate. Patients visit multiple doctors per year for various reasons. The broader aspect of practitioners that usually aren't taken into account are chiropractors, pharmacists, etc. Patients also travel for vacation, work, and even relocate for a longer duration. In the present day, a large number of patients are vastly interested in recording their health status using wearable health devices. This health data generated by patients is easily acquired by the service providers or devices but never by medical practitioners. Therefore it is proven hard for a patient to get their multiple records accessed through a summarized EMR because of security and privacy concerns. Thus, regardless of patients being the rightful owners of their medical data assets, and in spite of practitioners, health facilities, and the government providing large medical investments, health management is always hindered by the inability to acquire information, less usage of information acquired, poor data asset security and unmanageable privacy controls. These are the key reasons for developing a health care management system using blockchain. For these security reasons, blockchain is implemented in this healthcare management system.

Blockchain is considered to be the immutable ledger which is decentralized, distributed and stores data in blocks. Each block of the blockchain is connected with its preceding block through the link. Since each header of the block has the hash value of the preceding one, it becomes computationally infeasible for a third party to change any data in the blockchain as it needs to be reflected on every node of the blockchain. This makes blockchain an immutable and secure database to store private information. As every node is independent in the blockchain and no node is superior to others, it technically forms a decentralized system that is robust for handling such big data-like medical records. In order to implement hashing of pointers, we use Merkle tree. Merkle tree on the other hand are cryptographic hash pointers represented as a binary tree. The construction of a Merkle tree is done by taking the hash of a pair of data as the leaf node, and its output is hashed till the root node. The usage of Merkle trees makes transaction verification easier and faster in the blockchain. But since permissionless blockchains are susceptible to being disruptive, permissioned chains are being implemented as they steer clear from expensive consensus mechanisms and work in environments that are trusted.

This paper implements a hyper ledger-based blockchain architecture that is more extensible and scalable. In this paper, we include mainly three components - an application user interface, an access control module as blockchain, and data storage based as off-chain. Any medical data being shared by an individual for their convenient exchange with the doctors needs to be secured from any sort of third-party intrusion. The data might hold crucial information regarding the patient's history which might affect them, thus any sort of change in the data by a third party intentionally or not may cause severe damage to the individual. Also at the time of emergency, a doctor might need all of the patient's history where an efficient database is required. Therefore, all medical data must be secured and efficiently available, which in this case is done using blockchain. All data assets like medical reports, prescriptions, treatment plans, drugs, etc. are kept in a safe cloud-based repository to maintain the level of performance and keep it economically feasible. The application interface makes the system smoothly available to access for doctors, patients, distributors, and manufacturers. The on and off-chain data are securely linked through the patent-pending method without any storage load in the blockchain architecture. Smart contracts provide data owners access to their records in a permissioned and safe manner.

II. Literature Survey

One research paper by Kai Fan, Shangyang Wang, Yanhui Ren, Hui Li and Yintang Yang titled "MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain" [1] aims to provide a familiar method of storing patients' information at hospitals. For a common patient, data is stored in multiple hospitals. Thus for a patient to get their multiple records accessible through a summarized EMR is proven hard because of security and privacy concerns. This paper provides a solution to the above problems by giving a blockchain-based information management system called 'MedBlock'. Here MedBlock's distributed ledger provides easy retrieval and access of data in electronic medical records. This paper also achieves an improved consensus mechanism and high data security by utilizing symmetric cryptography and customized access control protocols.

Catering to the needs of issues that arise in remote patient monitoring systems, Kristen N. Griggs, Olya Ossipova, Christopher P. Kohlios, Alessandro N. Baccarini, Emily A. Howson and Thaier Hayajneh published a paper titled "Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring" [2] for resolving security concerns related to exchange and recording of data transactions. In order to resolve these issues, this paper proposed a blockchain-based smart contract to ensure safe analysis and medical sensor management. The paper used the Ethereum protocol and created a system where the smart device is communicating with the sensors and calls smart contracts while at the same time logging every event on the blockchain. This benefits patients with real time tracking and intervention in the medical field by notifying patients and practitioners, while simultaneously providing security. This paper resolves all security issues in medical smart devices health management in a HIPAA compliant manner.

Highlighting flaws in the centralized approach to maintaining health records, the research paper "Health Record Management through Blockchain Technology" by V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte [3] brings out the issue of a data breach. There is a huge loss for institutions as well as patients when a data breach happens, in terms of monetary as well as health loss. Moving forward, this paper also reveals the flaws in institution-centralized data control and gives a decentralized system using blockchain as a solution. In health care, smart contracts help to make things simpler. Where Blockchain will be used for invocation, record production, and validation. The solution proposed could be used as a solution for various problems in the medical domain such as record maintenance, record sharing, billing, medical research, etc. It lays the theoretical base for a model of maintaining records with the help of blockchain, further research and practical implementation.

Similarly, research titled "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology" is a paper that focuses on the poor management and causes of failure of Emergency Medical care, written S. Hasavari and Y. T. Song [4] A lot of pre-hospital deaths are caused due to the lack of medical history of patients. A lot of patients' data is generated in some other hospital and later is relevant to some other hospital. It is very difficult for a different healthcare system to retrieve a patient's medical history from the previous healthcare system. In this paper, a safe filing system and blockchain is proposed as the remedy to emergency access to patients' records. All medical record concerns like authentication and privacy have been taken care of in this approach. With the help of the practical implementation of this paper, the ambulance crews can access patients' medical history and avail high-quality pre-hospital care which leads to a much less death rate.

Blockchain in the medical system has few healthcare systems that provide targeted sharing protocols for medical data and personal health data. The paper titled "MedBlock: Blockchain-based Multi-role Healthcare Data Sharing System" by Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, [5] proposes a data management system for multiple users by combining blockchain and the InterPlanetary File System (IPFS).

Another work in similar literature, "Blockchain-based approach for e-health data access management with privacy protection" by L. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla [6] provides a design where blockchain is used in the healthcare system for the storage of information in clinics, and hospitals based on the patients' access policies. The paper shows 2 types of chains i.e. a private sidechain and a public main chain, which either keeps information of the patients' real ID or information with a temporary ID.

Research, "Blockchain in Healthcare: A Patient-Centered Model", by Hannah S Chen, Juliet T Jarrell, Kristy A Carpenter, and David S Cohen, Xudong Huang [7] proposes a technology that could be utilized in many places for sharing and storing health records for both hospitals and application interfaces. After blockchain gained popularity in software research, it started providing data authority over to patients. This project thus created a change in authority for patients resulting in a patient-centered model.

A similar work titled "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management" by M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem, [8] aims for a decentralized medical structure using blockchain, though the price of storing information and records is overpriced on the blockchain. This price is due to the high amount of computaion required in a transaction prior to committing on the blockchain. Cost of managing patient's electronic health records (EHRs) is not feasible and costly on a blockchain service. Here, a project design solution is provided to reduce the high expenses on a blockchain. Furthermore, the usage of watermark as a way to store patients' media results in addition to the usage of encryption on IPFS objects stored in the network.

III. Methodology

A. Blockchain

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a cryptographic hash of the previous block, a timestamp, and transaction data (generally represented as a Merkle tree) [9]. The timestamp verifies that the transaction data was there at the time the block was released, allowing it to be hashed. The blocks form a chain, with each new block reinforcing the preceding ones as it contains the information of the previous block. As a result, blockchains are resistant to data tampering since the data in any given block, once recorded, cannot be changed retrospectively without affecting all subsequent blocks.

Hyperledger Fabric, an open-source project from the Linux Foundation, is the modular blockchain framework and de facto standard for enterprise blockchain platforms [10].

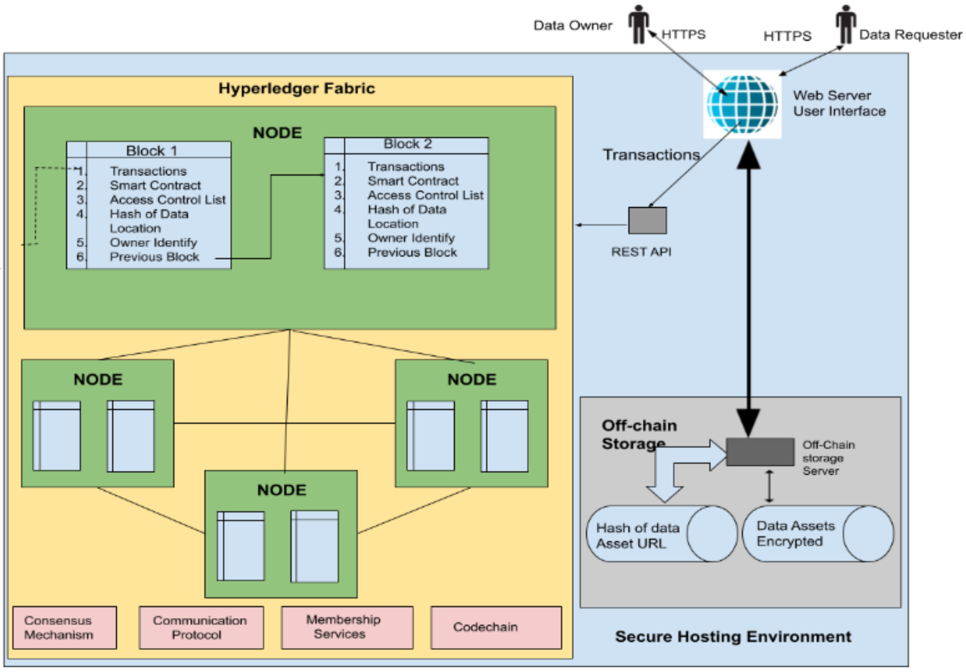


Fig. 1: Architecture

As shown in Fig. 1, We have two main entities, the data owner and the data requester who would be handling the data. The purpose of the project is to give the owner total control over their data, hence we will be using Discretionary Access Control (DAC) policy. The architecture is based on Hyperledger Fabric, which contains different nodes to store medical history. Hyperledger Fabric is a distributed ledger platform that is permissioned where all nodes in the network have an identity. Each node has a hash key which is used to securely access data from off-chain storage.

Each patient (the data owner) has its own blockchain and access to the blockchain can be given to the data requester, like doctors, pharmacies, and hospitals for a specified period of time. The patient can give permanent consent as well to a requester in order to facilitate emergency access to retrieve data. To maintain the integrity of the data, the patient will have the option to check consent details given till a certain point in time. The application would also facilitate the fetching of reports and prescriptions both by the patient as well as the data requestors.

The data requestors who have consent from the patient will have permission to add the blocks to the chain. The doctor can refer to tests and treatments which the patient has to go through and also prescribe drugs using the blockchain. In addition to this, the doctor can add comments and media to the blocks.

When a patient visits a hospital a new prescription is made. In a similar way, hospitals will have the permission to create a new report inpatient blockchain. In addition, hospitals will have the functionality to register a patient for the treatment recommended by the doctor and start the treatment.

B. Consensus

The model presented in this paper is patient-centric, and hence the patient holds the power of decision making in order to reach consensus. Once a patient gives permission, other entities like doctors, hospitals, and pharmacies can access the patient's data and participate in the consensus to agree upon a single, stable, and uniform state of the blockchain.

The technical freedom to create channels between the entities to further ensure safe and secure flow of data across entities allowed to participate in the channel. This in turn helps in creating a private network inside the blockchain between the chosen entities.

C. API Workflow

The following flow chart shown below in Fig. 2 displays the API workflow of the system. The description of each entity within the system is as explained.
Patient: The patient user registers to the network requiring their Aadhar number (a 12 digit individual identification number of India) and a consenter ID. This provides temporary consent to the doctors based on their ID.
Hospital: The hospital user creates a report for patients about their tests, details etc, using the patient ID.
Doctor: The doctor user refers tests to patients, along with the type of tests and treatment to be conducted.
PathLab: This user tests based on supervisor's ID and prescribes drugs to the patient
Pharmacies: Pharmacies give drugs along with a recommendation message. The refer treatments to patients accordingly.
Hospital: This user begins treatment based on the supervisor ID. Doctor further adds comments and media files to the patient's records.

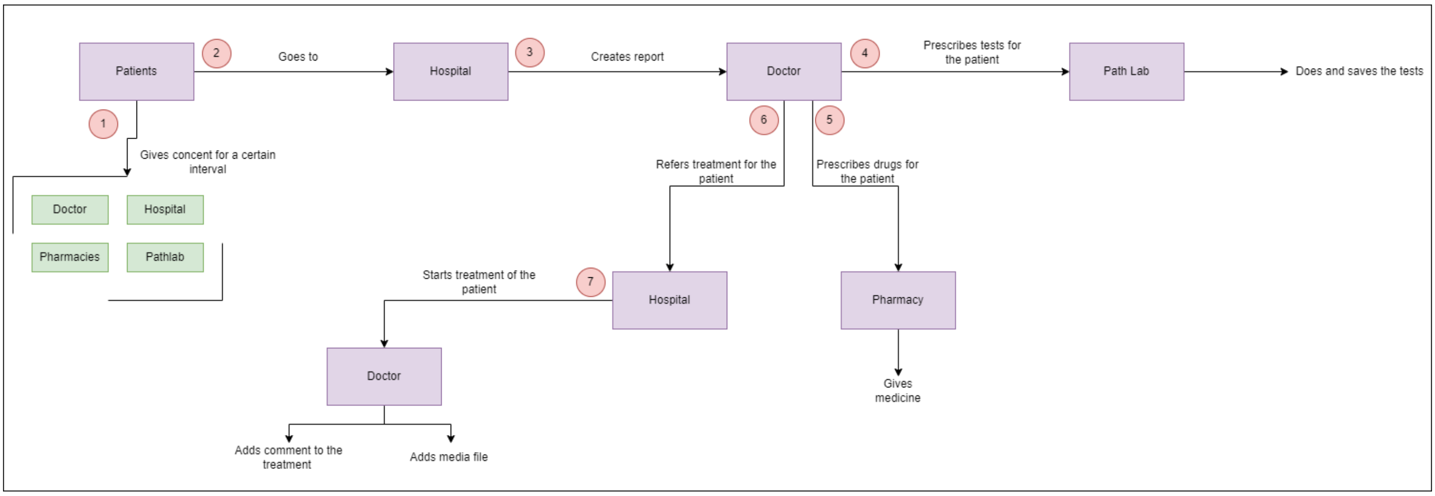

Patients
2
Goes to
Hospital
3
Creates report
Doctor
4
Prescribes tests for the patient
Path Lab
Does and saves the tests
1
Gives concent for a certain interval
Doctor
Hospital
Pharmacies
Pathlab
6
5
Refers treatment for the patient
Prescribes drugs for the patient
Starts treatment of the patient
7
Hospital
Pharmacy
Doctor
Gives medicine
Adds comment to the treatment
Adds media file

Fig. 2: Data Flow within the system

D. Off-chain Storage

The medical data management system will contain a huge amount of data which could not be accommodated on the block itself. In order to scale the system we would need storage off the blockchain. This storage is called off-chain storage. The off-chain storage can be a structured or unstructured storage which can contain a variety of data ranging from text to images.
There are various issues with current on-chain storage : access issue, performance issue, security issue, success issue, and cryptographic issue. In order to avoid all these we can use an off-chain storage which is shared and secure. To harness the advantages of distributed systems, the project will be using a nosql database named couchDB. CouchDb is a document based database which facilitates both structured as well as unstructured data. It also is highly compatible with hyperledger and highly responsive to HTTP requests which makes the transaction easier and faster. The couchDB also has a feature of replication and follows ACID property which prevents any kind of data loss and maintains the atomicity of each and every transaction happening in the chain.
The blocks in blockchain will contain a hash value which will refer to the partition where the data is stored in the database.

E. UI Description

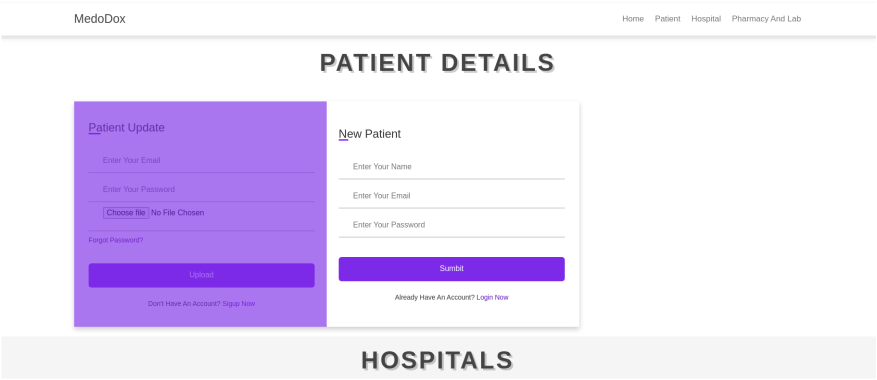


Fig. 3: UI for patient registration

The user interface of the medical data management system will have five activities, one for the data owner (the patient) and another 4 for the data requestors (doctor, hospital, pathLabs, and pharmacies). Each activity will have a registration and sign-in functionalities. During the time of registering each entity will be provided a unique id which will be referenced while accessing the blockchain.
The patient will have a page where they can view their medical records. On the other hand, the other entities (doctors, hospital, pathLab, and pharmacies) will have access to view as well as upload the designated details in the form of a new block to the blockchain.
In order to give a flawless experience to the users, a mobile application will be developed using a cross platform tool named flutter. This will make sure that the user outreach is not only limited to android or iOS users but to both.

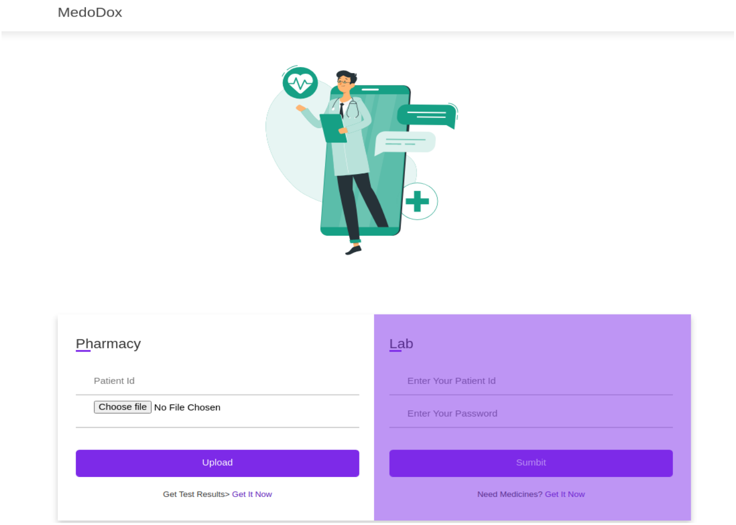


Fig. 4: UI for updation in patient blockchain by pharmacy and Lab

The undergoing UI of the working system is shown. As displayed in Fig. 3, it is the user interface for our patients to register themselves if they are new to the site and updating their new medical health records to the database through their ID and password. The hospital entity is where patients update their latest test results or prescription for any further comments from the doctor assigned. As shown in the Fig. 4, it is the phamacy and laboratory section where the respective departments function according. As the pharmacy provides the medicine as per the prescription provided and the laboratories perform the tests mentioned in the form submitted.

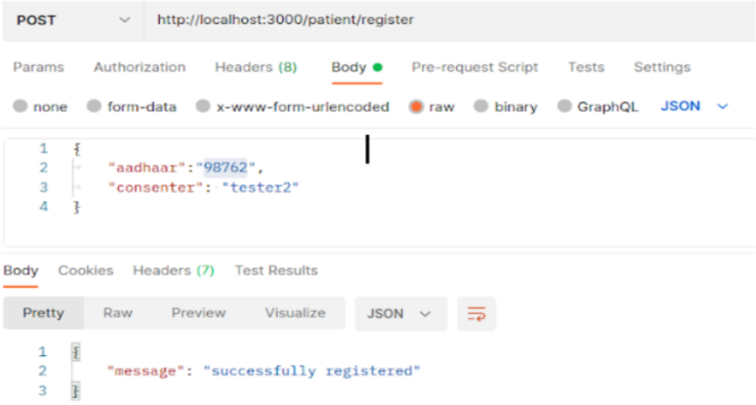
IV. Results

A. Secure an Enhanced Protocol for the Storage of Private Health Data

Implementing a blockchain data structure provides immutability of data and authenticity to the users accessing the data. The data stored can only be updated or inserted by the authority that owns the private key while others could access their own data for viewing. This ensures the authenticity that only authorized people like hospitals, caregivers and laboratories could update the data of a patient. The blocks in the data chain are linked to previous blocks using the hash of the block, thus any change in a block needs to be updated in every block to acquire an enhanced secure protocol for the storage of private health data as every block holds a copy of the entire blockchain. This makes our project a secure structure to store the medical data of every individual.

B. An Economically Feasible Health Data Management System

Maintaining an entire database that includes all medical records of every patient requires a large amount of space which directly requires a vast amount of storage thus increasing the cost of maintaining the blockchain exponentially. To reduce the cost of storage and provide an economically feasible health data management system, we have maintained an off-storage database where we keep the actual data of every individual, whereas the actual blockchain holds the link to the cloud storage where the medical assets are stored.

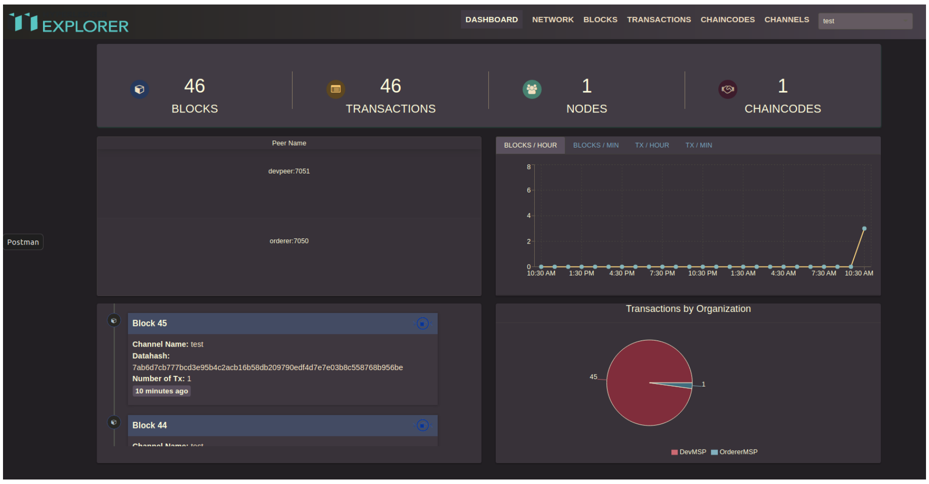


POST http://localhost:3000/patient/register

```
{
    "aadhaar":"98762",
    "consenter": "tester2"
}
```

```
{
    "message": "successfully registered"
}
```

Fig. 5: API response for patient entity



Block 45
Channel Name: test
Datahash: 7ab6d7cb777bcd3e95b4c2acb16b58db209790edf4d7e7e03b8c558768b956be
Number of Tx: 1
10 minutes ago

Block 44
Channel Name: test

Fig. 6: Hyperledger Explorer for the blockchain

After the implementation of the solution proposed in the paper, we were able to give the data requesters (the hospital and doctor) a temporary access and it was tested using Postman, as shown in Fig. 5.

As shown in Fig.6, the changes in the blockchain can be visualized using Hyperledger-fabric explorer and secure the data within different channels.

The existing system of healthcare is centralized and not secure while the proposed system provides decentralisation and gives appropriate amounts of security to the crucial medical data using consensus mechanisms. The decentralisation helps the access of medical data from any part of the world which would help in solving data loss problems during relocation and lack of input during treatment.

VI. Conclusion

As the world is moving forward, every aspect of life is measured in terms of time and energy consumption. In order to keep up with the status quo, the medical system needs to be upgraded. One form of healthcare upgrade is to facilitate efficient access and retrieval of data assets between patients, doctors, and caregivers while parallelly maintaining a secure protocol for the accessibility of private data assets.

This paper focuses on providing a convenient way of easing the retrieval and storage of an individual's health record using a blockchain data structure which makes data stored in each block to be immutable. In the blockchain, the blocks are linked to the previous block with a hash value and every block has a copy of the entire blockchain, and thus any change or update on any block needs to be reflected on every block which makes it computationally impossible to breach and resulting in blockchain to be a very secured data structure to store medical records.

Restricting who can update or add data to the blockchain also helps in providing security or resistance from any sort of impersonation. This is facilitated using public and private keys, where the private keys restrict only authorized users to updating the records. In the medical data asset, only the hospitals and doctors are allowed to update the test results, recommendations, or treatment analysis.

Ultimately, this paper aims to play an important role in the health care and management of data assets for patients to be able to update their new reports and get the needed report analysis and prescriptions from the medical practitioners while also ensuring that the integrity of their data is maintained.

References

[1] Fan, K.,Wang, S., Ren, Y. et al. MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain. J Med Syst 42, 136 (2018). https://doi.org/10.1007/s10916-018-0993-7.

[2] Griggs, K.N., Osipova, O., Kohlios, C.P. et al. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. J Med Syst 42, 130 (2018). https://doi.org/10.1007/s10916-018-0982-x.

[3] V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte, "Health Record Management through Blockchain Technology," 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), 2019, pp. 1411-1415, doi: 10.1109/ICOEI.2019.8862594.

[4] S. Hasavari and Y. T. Song, "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), 2019, pp. 71-75, doi: 10.1109/SERA.2019.8886792.

[5] Y. Yu, Q. Li, Q. Zhang, W. Hu, and S. Liu, "Blockchain-Based Multi-Role Healthcare Data Sharing System," 2020 IEEE International Conference on E-health Networking, Application & Services (HEALTHCOM), 2021, pp. 1-6, doi: 10.1109/HEALTHCOM49281.2021.9399028.

[6] L. Hirtan, P. Krawiec, C. Dobre and J. M. Batalla, "Blockchain-Based Approach for e-Health Data Access Management with Privacy Protection," 2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2019, pp. 1-7, doi: 10.1109/CAMAD.2019.8858469.

[7] Hannah S Chen†, Juliet T Jarrell†, Kristy A Carpenter, David S Cohen, Xudong Huang* Department of Psychiatry, Massachusetts General Hospital and Harvard Medical School, USA.

[8] M. Misbhauddin, A. AlAbdulatheam, M. Aloufi, H. Al-Hajji and A. AlGhuwainem "MedAccess: A Scalable Architecture for Blockchain-based Health Record Management," 2020 2nd International Conference on Computer and Information Sciences (ICCIS), 2020, pp. 1-5, doi: 10.1109/ICCIS49240.2020.9257720.

[9] "Blockchain", 22:47, 11 April 2022, Wikipedia [Online]. Available: https://en.wikipedia.org/wiki/Blockchain

[10] "Hyperledger fabric", 22:57, 1 April, 2022, [online]. Available: https://www.ibm.com/topics/hyperledger

Thirteenth International Conference on
Advances in Computing, Control, and Telecommunication Technologies
ACT 2022

Jun 27-28,2022; Hyderabad, India.

CERTIFICATE OF PRESENTATION & PUBLICATION

This is to certify that *Akanksha Srivastava* *of* *Siddaganga Institute Of Technology, Tumkur, Karnataka, India* *author of a Research Paper titled* *Blockchain Based Medical Data Asset Management System* *has submitted the paper which has been approved and presented for publication in the Thirteenth International Conference on Advances in Computing, Control, and Telecommunication Technologies, ACT 2022, which is organized by the Association of Computer Electrical Electronics and Communication Engineers (ACEECom) – a division of The IDES.*

Dr. Janahanlal Stephen
General Chair, ACT 2022

Prof. K U Abraham
General Co Chair, ACT 2022

http://act.theides.org/2022/