MEDCHAIN

FINAL PROJECT REPORT

submitted by

AALAP SAM JACOB
MGP17CS001
ASHISH SHAJI
MGP17CS029
B NAVEEN
MGP17CS036
JAYASANKAR V
MGP17CS052

to

The APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree

of

Bachelor of Technology
In
Computer Science and Engineering

Department of Computer Science and Engineering
Saintgits College of Engineering
Pathamuttom

JUNE 2021

DECLARATION

I, undersigned hereby declare that the final project report “MedChain”, submitted for partial fulfillment of the requirements for the award of degree of Master of Technology of the APJ Abdul Kalam Technological University, Kerala is a bona fide work done by us under supervision of **Er. Tibin Thomas**. This submission represents our ideas in our own words and where ideas or words of others have been included, I have adequately and accurately cited and referenced the original sources. I also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in our submission. I understand that any violation of the above will be a cause for disciplinary action by the institute and/or the University and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Pathamuttom
12-06-2021

Aalap Sam Jacob (MGP17CS001)
Ashish Shaji (MGP17CS029)
B Naveen (MGP17CS036)
Jayasankar V (MGP17CS052)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SAINTGITS COLLEGE OF ENGINEERING, PATHAMUTTOM

CERTIFICATE

This is to certify that the report entitled “**MEDCHAIN**” submitted by **AALAP SAM JACOB, ASHISH SHAJI, B NAVEEN, JAYASANKAR V** to the APJ Abdul Kalam Technological University in partial fulfillment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering is a bona fide record of the project work carried out by them under our guidance and supervision. This report in any form has not been submitted to any other University or Institute for any purpose.

Internal Supervisor	Project In-Charges	Head of the Department
Er. Tibin Thomas	Er. Veena A Kumar	Dr. Anju Pratap
	Er. Jinu Thomas	

ABSTRACT

We live in the midst of a plenitude of information; information is continually reshaping the substance of innovation by making experiences and by lifting norms. With wealth in information there likewise emerge a plenitude of worry about the security of this information, particularly delicate information like individual clinical records. As of now, there doesn't exist a framework that permits people to get to their very own clinical records pre-predominantly. The current framework is a concentrated data set where the pre-predominant access over any clinical records lies with the Hospital [3]. This framework is absolutely uncalled for as it doesn't permit people to screen their own clinical records and could be inclined to any kind of control by the association.

To handle this issue, we propose to utilize a circulated record (blockchain) rather than the current incorporated data set to oversee individual clinical records. The principal benefits of our proposed arrangement are improved information security, straightforwardness, permanence, and sealing.

The key players in this system are:

1. Patient: Patient gives access of the medical record to the doctors so that they can make necessary updates. After updating, the access is revoked.
2. Hospital: Adds and manages patients and doctors in this network. Verification of these entity is also done.
3. Doctors: Doctor should request for access from the patient. Once the access is granted, the doctor makes the necessary updates to the medical records.
4. Pharmacy: Pharmacy can view the prescriptions updated by the doctor. Should request for access from the patient and access is revoked after distribution of medicines.
5. Insurers: Proper and rightful medical claims are ensured by accessing necessary documents of patients with hospitals’ and patients’ consent.
6. Governing Authority: The governing authority acts as the administrator of the whole system. The governing authority checks for any sort of malpractices happening in the whole system.

CONTENTS

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Electronic clinical reports and archives request the requirement for secrecy. Somewhat recently, how patient wellbeing records are put away and gotten today doesn't mirror our specialized advancement in this field, and emergency clinics keep on utilizing age-old patient information the board frameworks [5]. This is incomplete because of rigid clinical information security and assurance laws, which have smothered the utilization of the new advancements to make the treatment of clinical information more straightforward and helpful for the two patients and doctors.

This coding design exhibits a blockchain-fabricated clinical information/access control structure. The application shows the platform from the point of view of 4 stakeholders -

- The Governing authority is the admin of a conglomerate of hospitals, pharmacy, insurers and has the highest of access levels in the hierarchy. They have the ability to onboard a new organization to the conglomerate and assign/de-assign organization admins on their dashboard.
- The organization (hospital, pharmacy, insurer) admin is the admin of a particular organization which is part of the conglomerate/solution. They have the ability to onboard new users with the role of either patient or doctor or remove a user.
- The doctor is a user in the organization with the appropriate role and can upload documents for their patients and download/view documents of their patients to which they have been granted access.
- The patient is a user in the organization with the appropriate role and can upload documents on their own, view them, view the document access logs and also manage access to their documents on their dashboard.

CHAPTER 2

LITERATURE SURVEY

Medical records require a large deal of privacy. So, all the participants are required to be in a mutual agreement with each other. This demands consensus among healthcare providers and regulators, and the creation of agreed policies and procedures [1]. Privacy is the starting point to determining who and whom should be allowed to access personal patient information. In line with this issue, numerous security standards have been developed. This includes managing access control of patient information, security of patient data from unauthorized users, and the modification and destruction of stored data, etc. [4]. As sizes of healthcare data increases, then there is need of security mechanisms to protect the data.

Therefore, data must always be free of threats and secure at all times. If these conditions are not met, the technologies used may not function correctly or be deemed reliable. At present, most healthcare systems use centralized client-server based architectures, where a central authority has full-access to the system. In this scenario, lack of privacy or security flaws may lead to failures in the system, resulting in cyber intruders potentially gaining access to patient data.

Modern healthcare systems are characterized as being highly complex and costly. However, this can be reduced through improved health record management, utilization of insurance agencies, and blockchain technology. Blockchain was first introduced to provide distributed records of money-related exchanges that were not dependent on centralized authorities or financial institutions. Breakthroughs in blockchain technology have led to improved transactions involving medical records, insurance billing, and smart con- tracts, enabling permanent access to and security of data, as well as providing a distributed database of transactions. One significant advantage of using blockchain technology in the healthcare industry is that it can reform the interoperability of healthcare databases, providing increased access to patient medical records, device tracking, prescription databases, and hospital assets, including the complete life cycle of a device within the blockchain infrastructure [4].

The security of healthcare records is becoming increasingly important for keeping data safe from security breaches and criminal activity. If unauthorized users are able to gain access to patient data, it can be sold or leaked to the market, with patients' personal information being revealed to anyone with access. This information may include addresses, telephone numbers, full names, etc. The privacy of patients' data is essential in successful healthcare management [1]. In light of these challenges, various countries have proposed or created regulated standards for healthcare systems, to prevent cyber threats, which helps improve confidentiality of patient information and confidence in the provider-patient relationship. At present, most healthcare systems use centralized client-server based architectures, where a central authority has full-access to the system. In this scenario, lack of privacy or security flaws may lead to failures in the system, resulting in cyber intruders potentially gaining access to patient data.

We have studied a few existing papers to study its limitations and perfect our implementation:

1.1 Emergency Access Control Management System for Personal Health Record Based on Blockchain Choi and Kim [1]

Data is constantly re-shaping our daily life, making things easier, faster and more accessible. However, the privacy and integrity of personal data has become a great concern. Personal health records (PHRs) are vital information regarding an individual; hence it requires a high standard of privacy and security. There have been introduced many works on various aspects of managing and organizing the PHRs so far. However, these systems tend to have disadvantages, for instance, in a traditional emergency access system, the patient cannot give consent to emergency staff for accessing his/her PHR. Also, there is no secure record management of patient's PHR, which reveals highly confidential personal information, such as what happened, when, and who has access to such information. In the emergency condition, the medical staff needs some necessary elementary and valuable health information about the patient for increasing the chance to supply appropriate cure to save the patient's life or assuage in perilous conditions. The confidentiality of the PHR restricts even his/her primary doctor from accessing it, also the patient may not be in a conscious state to authorize access to his PHR. So, accessing the PHR in an emergency situation without affecting its safety and integrity is a challenge. This discusses an emergency access control management system (EACMS) based on permissioned blockchain Hyperledger fabric and Hyperledger composer. In the proposed system, we defined some rules using the smart contracts for emergency condition and time duration for the emergency access PHR data items that patient can assign some limitations for controlling the PHR permissions. The performance of the proposed framework was analyzed by implementing it through the Hyperledger composer based on the response time, privacy, security, and accessibility. The experiments confirm that our framework provides better efficiency compared with the traditional emergency access system.

It provides an efficient solution to access an individual's medical records in an emergency situation, where the patient is not in a state to give consent. It provides faster response time and accessibility, as no third party has to be consulted to get access to the patients' health records. Also, it ensures that the confidentiality of the patients' personal records, even in emergency access situations without any privacy breach. The emergency medical staff is given only granular access (defined using smart contracts) over the records.

Also, there are considerable disadvantages. The system works well only if there are a large number of doctors in the system. Senior citizens may not be able to understand and adapt to this system easily, they'll probably be more comfortable with the existing system.

1.2 Secure System for Pervasive Social Network-based Healthcare [2]

The rapid development in the areas of mobile computing, wireless sensing and communicating technique prompts a new concept of pervasive social network (PSN)-based healthcare. The basic idea of the PSN-based healthcare is to enable users to share data collected by medical sensors. Sharing health data benefits people in many ways, including personal applications such as remote medical care and public health services like disease monitor and control. Although this approach has some real conveniences, the biggest challenge is how to securely share health data among the PSN nodes. Health records are vital information regarding an individual's life and health; hence it requires a high standard of privacy and security; therefore, it is important to protect these data from being modified or stolen. In addition, the network of PSN- based healthcare consists of a large number of mobile nodes, therefore, we need a mechanism for these nodes to easily share health data. The proposed PSN based healthcare system mainly relies on two security protocols, they are:
Protocol 1, it is an improvement on IEEE 802.15.6 display authenticated association protocol. Using this protocol, nodes are able to agree on a master key as well as their addresses. It significantly reduces the computational burden on the resource-limited sensor node.

Protocol 2, explains how users can share their health data to other PSN nodes using blockchain techniques. The proposed network is divided into two areas, wireless body area network (WBAN) area and PSN area. The WBAN area aims to establish secure links for sensor nodes and mobile devices through Protocol 1, and the PSN area aims to use the blockchain technique to realize health data sharing through Protocol 2 adding data to the blockchain.

There are several advantages in using this system. It helps the users to easily and more conveniently share medical data. The transactions are carried out very securely using blockchain technology. Fast data sharing improves the quality of peoples' life. Also, the system has some problematic aspects. The large-scale implementation of the proposed system is a very difficult task. Sensors are computationally limited devices. Many sensors touch the skin of users and some even are implanted in the body. Temperature rising caused by executing heavy load computations may cause inconvenience to users.

CHAPTER 3

OBJECTIVES AND PROPOSED SYSTEM

3.1 OBJECTIVE

A significant piece of the wellbeing records the executive’s framework is being dealt with utilizing typical customer worker engineering. This framework, which is being utilized in an enormous scope, has a ton of hindrances. It is strongly suggested by individuals everywhere on the world that their own wellbeing records be kept secure. Thus, by incorporating a safe innovation like blockchain into this case, we could possibly get this framework by an incredible edge. Along these lines, so, our goal is to foster a superior and secure across the board close to home wellbeing records the executive’s framework utilizing blockchain that coordinates the whole clinical records of a person into a solitary stage.

3.2 EXISTING SYSTEMS AND ITS CONS

Regardless of the developing writing on the advantages of different EHR functionalities, some have distinguished potential impediments related to this innovation. These incorporate monetary issues, changes in the work process, transitory loss of usefulness related to EHR selection, protection, and security concerns, and a few potentially negative side-effects [6]. Pre-prevailing access over records lies with the medical clinic. Burdens happen when people can't get to their records when he/she needs. Less straightforwardness and security. Hence, making a major degree for control by the specialists.

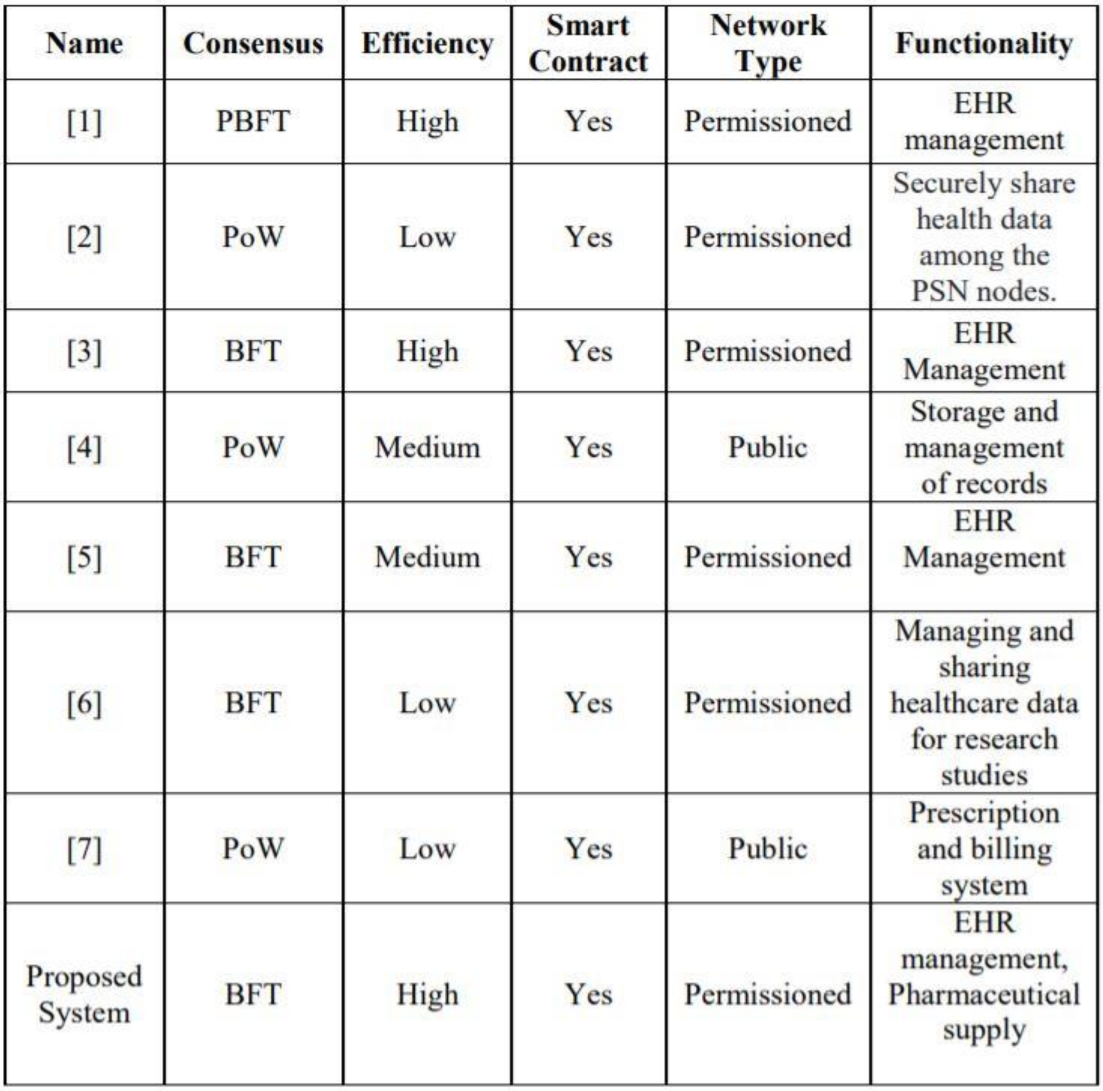
Current EHRs frameworks may cause a few unseen side-effects, like expanded clinical blunders, negative feelings, and changes in the power structure. Another significant issue is that a great deal of undesirable access in regards to the wellbeing records is likewise generally be accounted for. Such occasions ought to be significantly kept away from because abuse of individual wellbeing records can be of incredible outcomes. Another primary objection that resounds across a wide range of medical services associations includes drops in efficiency identified with current concentrated EHR frameworks use[6]. Usefulness drops can emerge from a few causes. The first and most regular identifies with usefulness drops because of the work process or EHR plan that cause clinicians or managerial staff to take additional time than typical to achieve errands. The second reason for efficiency misfortune identifies with deficient preparation on the EHR framework which normally emerges when new clients are acquainted with a framework or a framework is redesigned or changed and the applications are too intricate to even think about utilizing. Issues identified with the interoperability of medical care information have tormented endeavors to modernize the Global medical services framework. One of the essential obstructions to interoperability rests in the way that the many exclusive EHR frameworks or clinical gadgets available don't handily share data.[3]

3.3 PROPOSED SYSTEM AND ITS PROS

A decentralized organization offers a wide scope of advantages over the more customary unified organization, including expanded framework dependability, scale, and security. Quite possibly the main advantages of decentralized organization the executives is the way that there is no genuine single mark of disappointment. What's more, a decentralized organization design takes into consideration more prominent protection, as data isn't going through a solitary point and rather goes through various focuses [7]. This makes it considerably harder to follow across an organization. The system is designed in such a way that there are six major players in it. These are:

- Patient: First, the patient has to login into the system through the user interface. Once the patient has logged in, they have the options to grant the access of the medical records to the other players present in the system. That is, if a patient visits the hospital, the doctor may ask the patient for the permission for accessing their medical record. Once the patient has accepted the request, the doctor can do the necessary prescriptions and update the medical record of the patient.
- Doctor: As mentioned in the above case, the doctor can ask for the permission for accessing the medical record of the patient when they visit the doctor. Once the permission is accepted, the doctor can make the necessary updates to the records. Both the doctor and patient entities are under the hospital node.
- Hospital: The hospital node can add new health records with the patient’s consent. The patient and doctor nodes are under the hospital node. This node can also verify the identity of the doctors.
- Governing Authority: The governing authority acts as the administrator of the whole system. The governing authority checks for any sort of malpractices happening in the whole system. i.e., the whole network is being governed by this authority (preferably by the government medical authority).

- Pharmacy: Pharmacy can view the prescriptions updated by the doctor. Should request for access from the patient and access is revoked after distribution of medicines.



Name	Consensus	Efficiency	Smart Contract	Network Type	Functionality
[1]	PBFT	High	Yes	Permissioned	EHR management
[2]	PoW	Low	Yes	Permissioned	Securely share health data among the PSN nodes.
[3]	BFT	High	Yes	Permissioned	EHR Management
[4]	PoW	Medium	Yes	Public	Storage and management of records
[5]	BFT	Medium	Yes	Permissioned	EHR Management
[6]	BFT	Low	Yes	Permissioned	Managing and sharing healthcare data for research studies
[7]	PoW	Low	Yes	Public	Prescription and billing system
Proposed System	BFT	High	Yes	Permissioned	EHR management, Pharmaceutical supply

CHAPTER 4
DESIGN AND METHODOLOGY

4.1 ARCHITECTURE

The proposed blockchain based medical data storage system use the following architecture. The system consists of the players namely governing authority, hospitals, pharmacies, insurance providers, patients interact with blockchain network and the off-chain organ donation database. The primary aim of the blockchain network is to preserve the patient data securely without any data leakages by providing a global medical record to the patient.

Governing authority is one of the key players in the entire system which verifies and authorizes the players which comes under it. Hospitals, pharmacies, insurer are the nodes controlled by this player. This authority will verify the when a new hospital or pharmacies or insurer is added to the network and validate its functioning.

Hospitals are the node in which the patients are directly interacting. Here in this network, we are included a network hospital in a region. When a patient approaches a hospital for the treatment, he gives the corresponding hospital to access his medical records stored in the permissioned blockchain network. Therefore, the hospital can use this data for the treatment purpose with patient's permission. Hospital node will help the patient to interact with the doctors in the hospitals. After completing the treatment, the patient can revoke the hospitals access to medical data, thus the privacy and security is ensured.

The pharmacies are allowed to get the prescription of the patient when he/she is allowed from the network. Here also we are using the same access and revoke mechanism mentioned in the patient-hospital section. Thus, after buying the medicines the patient will revoke the access permission of the pharmacies. We are also included insurance providers to this network. The user can access the same medical record for taking the insurance. All the three interactions of the patient is allowed only by the permission of him/her.

All the data other than organ donation related records are stored in a permissioned blockchain network. This is begin updated when there is transaction occurs in the network.

By using this system, the patient will get proper treatment and follow up hence we are using a same medical record everywhere, also able to continue the treatment in any of the hospitals in this network.

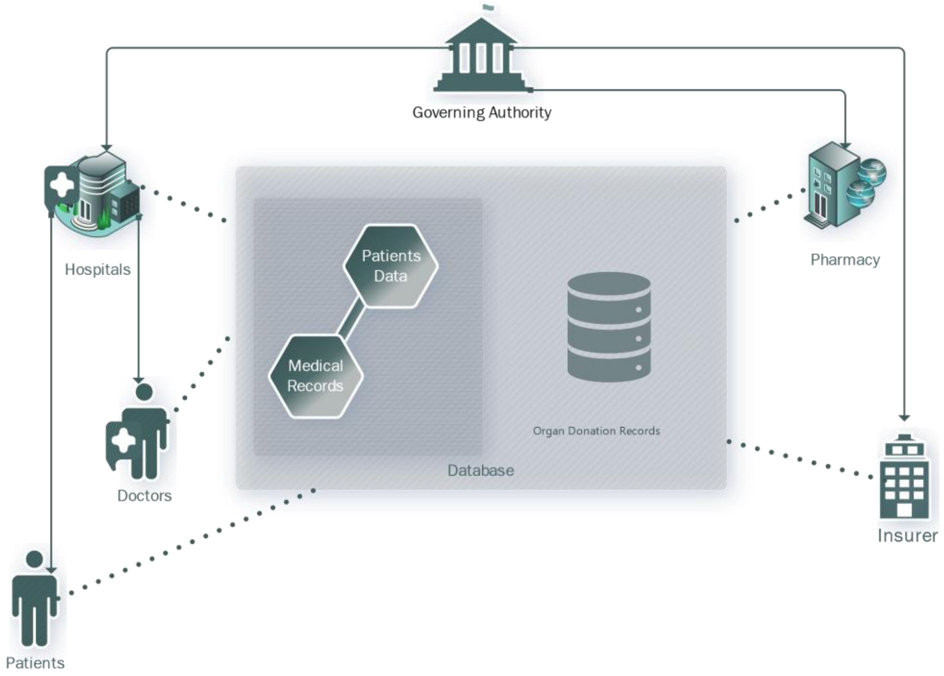


Fig 4.1 Architecture

4.2 FRAMEWORKS AND ITS IMPLICATION

The permissioned blockchain is built to permits a person, an organization or a group of organizations to transfer information and record transactions efficiently [5]. It adds a layer of privileged to decide who can participate in the network system, with the identity of each participant known to all participants. In the permissioned blockchain network system, the participant does not have a chance to fraud as their identity is exposed to the management server. In the permissioned or private blockchain network, usually, apply an algorithm such as Byzantine Fault Tolerance

(BFT). While in the permissionless blockchain system has used proof of work algorithm.

The Hyperledger Fabric (HF) is an implementation of a permissioned blockchain system and open source blockchain initiative hosted by the Linux Foundation [5]. It is one of the prime permissioned blockchain structures presently. Because it is based on the permissioned blockchain, it allows just concerned stakeholders as participant members and confines anyone to meet the network, temper the ledger, or invoke the transactions. The HF Network consists of several kinds of nodes, client nodes, peer nodes, and ordering nodes relating to the various organization. Every node's identity on the HF network which is presented by a membership service provider (MSP), typically correlated with an organization. All nodes in the HF network have distinctness to the identities of all parties and approve them. The MSP issues the enrolment and transaction certificates to the client. The fabric has smart contract functionality, chaincode, which enables participants to execute complex transactions as per defined permissions [10].

IBM® Blockchain Platform provides a managed and full stack blockchain-as-a-service (BaaS) offering that allows you to deploy blockchain components in environments of your choice. Clients can build, operate, and grow their blockchain networks with an offering that can be used from development through production. Key features are:

- **Simplified DevOps** allows you to move from development to test to production in a single environment by scaling up your Kubernetes resources to add more components.
- **Up-to-date Fabric key features**. Choose which version of Hyperledger Fabric you want to use when deploying peers or ordering nodes. Leverage the latest features of Hyperledger Fabric v1.4.9 and v2.2.1.

4.1 PROPOSED DATAFLOW

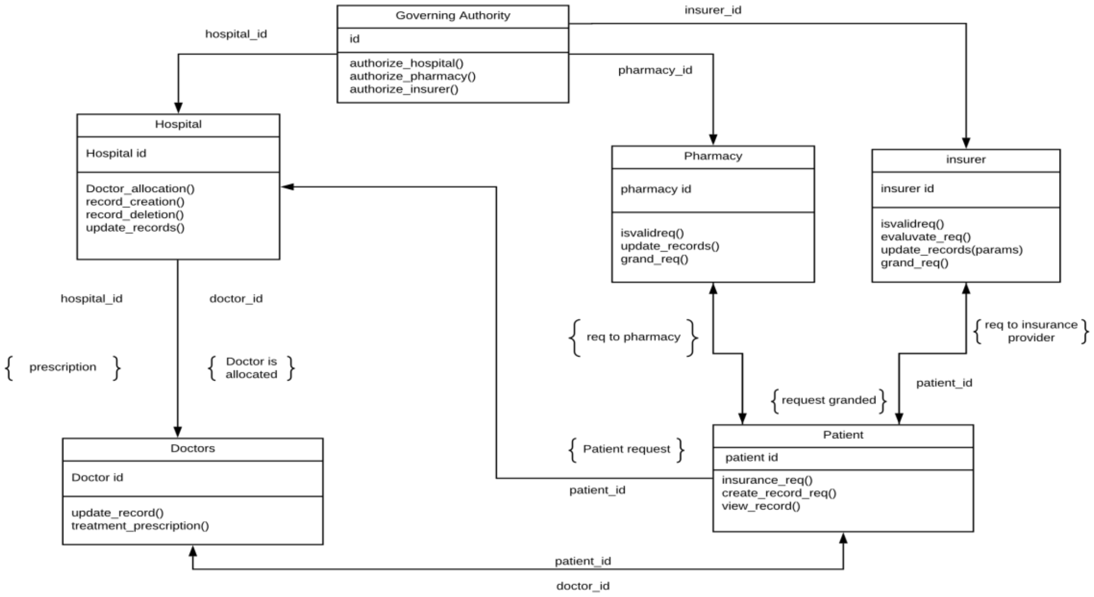


Fig 4.2 Proposed Data Flow

LOGIN FLOW

- All the players of the application (patient, hospital, governing authority, pharmacy and insurer) begin the user flow by logging into their respective dashboards.
- Clicking the login button leads to their respective login portal.
- In the dashboard, several options according to the role of the player are present.
- These options are executed by transferring the id of the player across the required areas, storing and retrieving them from the blockchain database.

PLAYER FLOW

- All the players follow these steps to exchange and handle data between them.
- The player should first login, upon which they will be going through the login flow.
- After successful authentication, the user can access the respective dashboard. They are able to create a medical record, download any of their medical records, give prescriptions, view the access logs of their documents, and view/manage permissions to their documents.
- The users are connected to the blockchain to process the queries.

CHAPTER 5

RESULT AND DISCUSSION

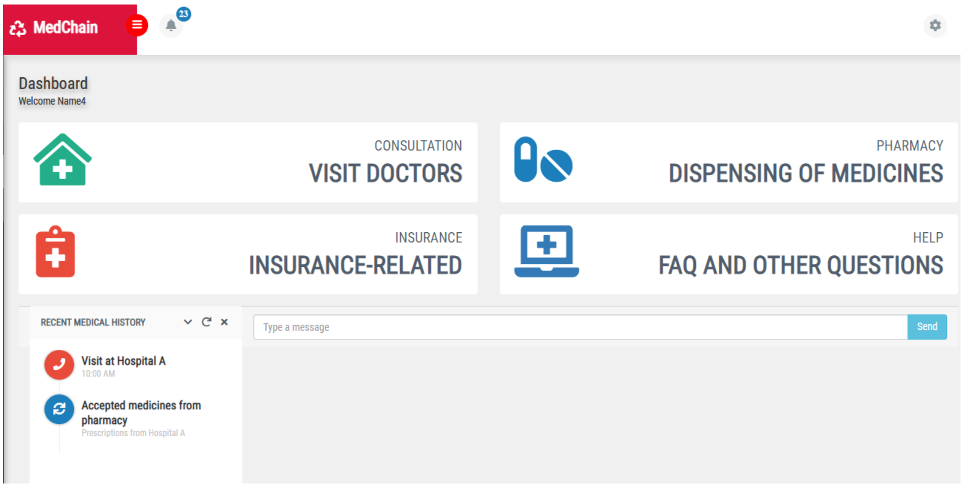
5.1 Web App

Our project uses a web-app for the uploading and modification of medical records, prescription and for insurance claims. Each player in the network will have a corresponding login.

On logging in, each player is authorized by a unique token, and are redirected to their corresponding dashboard.

5.1.1 Patient

Different functionalities included in the patient dashboard are; consultation, pharmacy, insurance and help. A screengrab of the dashboard is given below.



Visit at Hospital A
10:00 AM

Accepted medicines from pharmacy
Prescriptions from Hospital A

Fig 5.1 Patient Dashboard

- Upon selecting consultation, the patient can grant access to doctor to view his/her medical records by specifying the doctor's id.

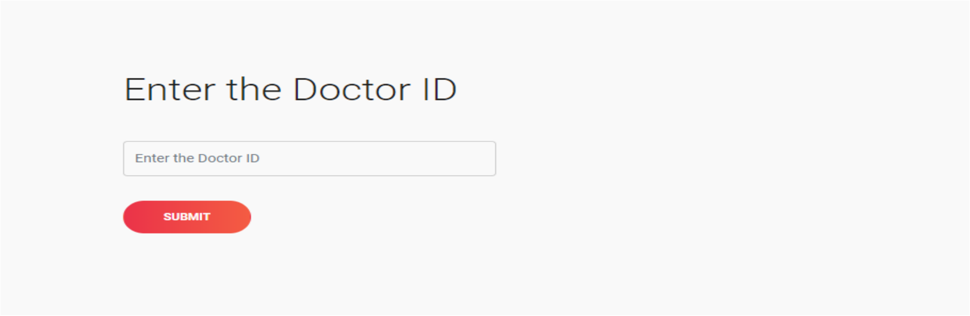


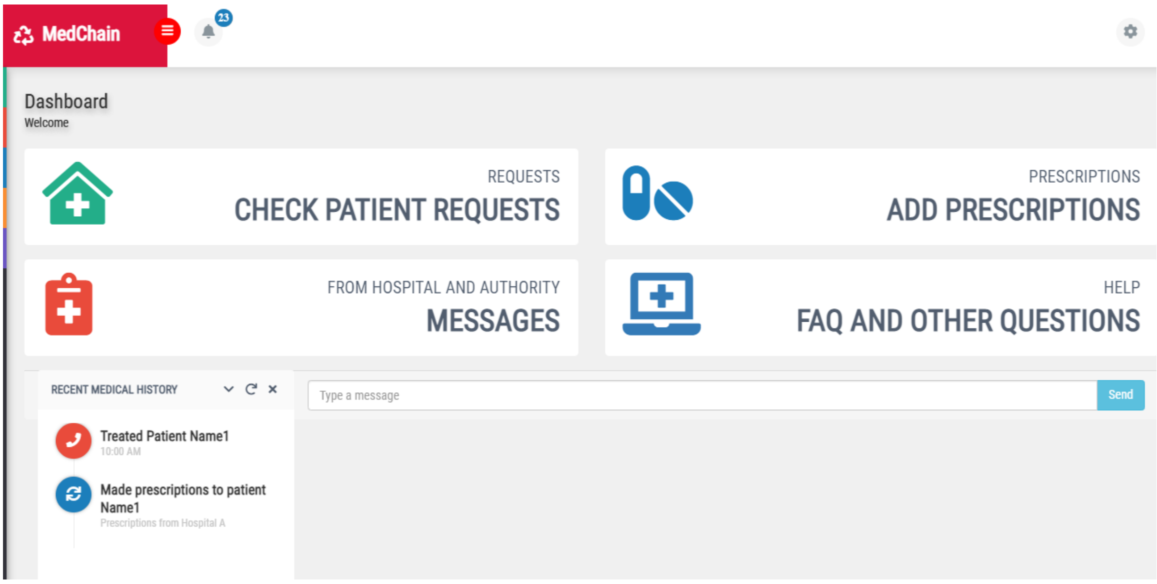
Fig 5.2 Doctor verification by patient

- Upon selecting pharmacy, the patient can view the prescriptions given by the doctor and see whether its delivered or not.

- Patient can make direct insurance claims by submitting the required documents to the insurer.

5.1.2 Doctor

The different functionalities in the doctor dashboard are;

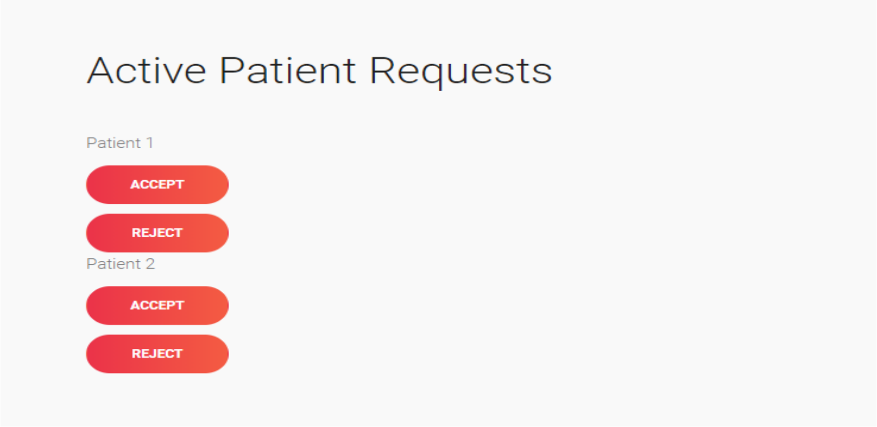


Treated Patient Name1
10:00 AM

Made prescriptions to patient Name1
Prescriptions from Hospital A

Fig 5.3 Doctor Dashboard

- The doctor can check patient request and choose to accept or reject them accordingly.


Active Patient Requests

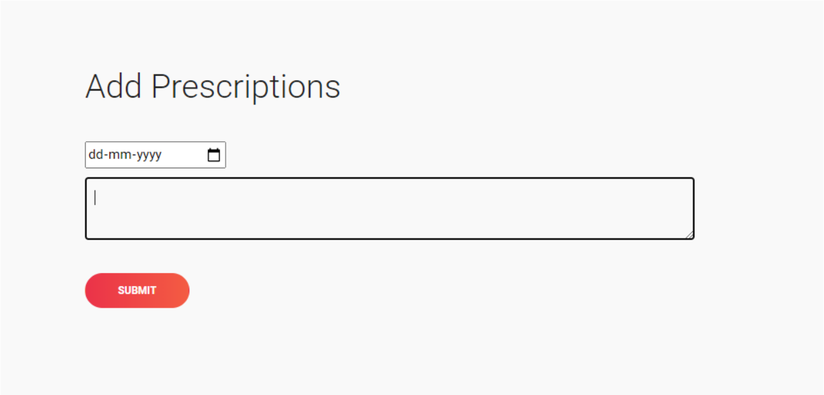
Patient 1

Patient 2

Fig 5.4 Patient requests

- Upon authorization by the patient, the doctor can view the medical record and perform diagnosis.

- Can add medical prescriptions after diagnosis.


Add Prescriptions

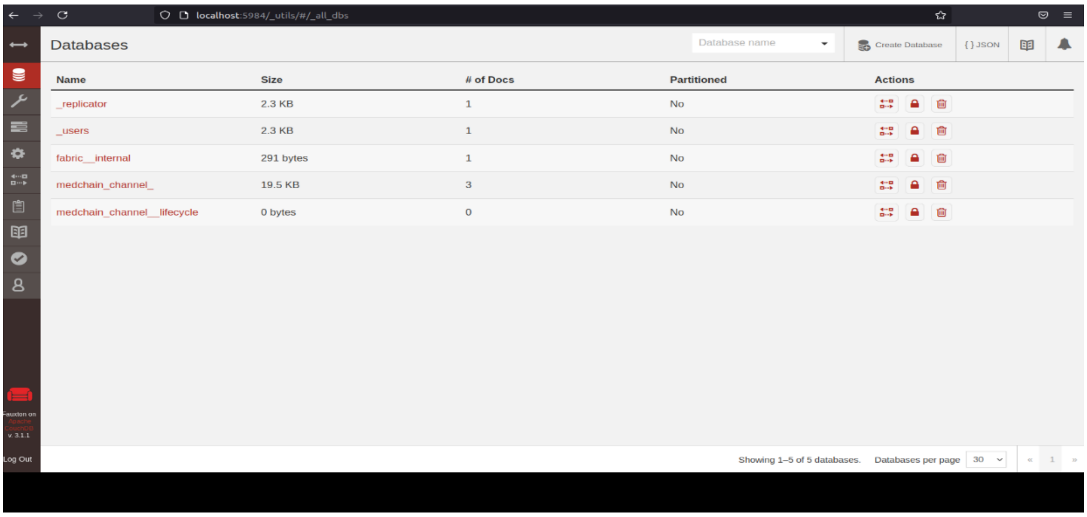
dd-mm-yyyy

Fig 5.5 Prescription Window

- Can send/receive messages from hospital and authority.

5.2 Network

Once a patient is consulted by a doctor, the updates made for the first ever time is uploaded into the blockchain database as a new record. Further modifications are made into the same record in case of future consultations. The blockchain network is used mainly as the storage for health records. The database system used is CouchDB. CouchDB is a JSON document datastore rather than a pure key-value store, therefore enabling indexing of the contents of the documents in the database. Other functionalities like login, register etc. are handled using MongoDB, Node and Express. The network is handled using Hyperledger Fabric. The database state is shown below.


localhost:5984/_utils/#/_all_dbs
Databases
Database name
Create Database
{ } JSON
Fauxton on Apache CouchDB v. 3.1.1
Log Out

Name	Size	# of Docs	Partitioned	Actions
_replicator	2.3 KB	1	No	
_users	2.3 KB	1	No	
fabric__internal	291 bytes	1	No	
medchain_channel_	19.5 KB	3	No	
medchain_channel__lifecycle	0 bytes	0	No	

Showing 1–5 of 5 databases. Databases per page 30

Fig 5.6 CouchDB dashboard

CHAPTER 6
CONCLUSION

Individual clinical records are amazingly delicate information and must be dealt with outrageous alert. Blockchain has a ton of highlights that help in the improved, productive and secure administration of records, it can extraordinarily balance out the administration of records in various areas. Subsequently, by utilizing a particularly refined framework, treatment of wellbeing records can be significantly settled.

Right now, customary customer worker situation is being utilized for the capacity of wellbeing records. There is a great deal of impediments for this framework. This framework exclusively confides in the worker, hence if the worker fizzles, the entire framework falls flat. Thus, when we acquaint blockchain with oversee wellbeing records, the dispersed idea of blockchain assists us with beating large numbers of the burdens of the customary customer worker framework [9]. The wellbeing records are made more straightforward, secure and a ton of controls can be stayed away from.

However, since blockchain is an innovation that appeared as of late, the clients are very little mindful about the idea of blockchain innovation. In this way, the framework ought to be executed steadily with outrageous alert while assigning access and authorizations.

REFERENCES

[1] Sudeep Tanwar, Karan Parekh, Richard Evans - Blockchain-based electronic healthcare record system for healthcare 4.0 applications, 2019.

[2] Chen L , Lee WK , Chang C-H , Raymond Choo K-K , Zhang N . Blockchain based searchable encryption for electronic health record sharing. Fut Gener Comput Syst 2019;95:420–9 .

[3] Kabra N , Bhattacharya P , Tanwar S , Tyagi S . Mudrachain: blockchain-based framework for automated cheque clearance in financial institutions. Fut Gener Comput Syst 2020;102:574–87.

[4] Dai, Yueyue, et al. "Blockchain and deep reinforcement learning empowered intelligent 5G beyond." *IEEE Network* 33.3 (2019): 10-17.

[5] Dai, Yueyue, et al. "Hyperledger Fabric and permissioned blockchain for content caching in vehicular edge computing and networks." IEEE Transactions on Vehicular Technology 69.4 (2020): 4312-4324.

[6] Mistry I, Tanwar S, Tyagi S , Kumar N . Blockchain for 5g-enabled IoT for industrial automation:a systematic review, solutions, and challenges. Mech Syst Signal Process 2019;135:1–19 .

[7] Kang, Jiawen, et al. "Toward secure blockchain-enabled Internet of Vehicles: Optimizing consensus management using reputation and contract theory." *IEEE Transactions on Vehicular Technology* 68.3 (2019): 2906-2920.

[8] W. Li, S. Andreina, J.-M. Bohli, and G. Karame, "Securing proof-of-stake blockchain protocols," in Data Privacy Management, Cryptocurrencies and Blockchain Technology. Cham, Switzerland: Springer, 2017, pp. 297–315.

[9] S. Apte and N. Petrovsky, “Will blockchain technology revolutionize excipient supply chain management?" J. Excipients Food Chem., vol. 7, no. 3, pp. 76–78, 2016.

[10] 0. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," IEEE Internet Things J., vol. 5, no. 2, pp. 1184–1195, Apr. 2018.