A Project/Dissertation Report

on

Digitalisation of Patients Records using Blockchain

Project Report submitted in partial

fulfillment for the award of the degree of

B.Tech(CSE)

Under The Supervision of

Dr.M Thirunavukkarasan

Assistant Professor

Department of Computer Science and Engineering

Submitted By

AKANKSHA TYAGI – 18SCSE1010145

AVIRAL GUPTA – 18SCSE1010548

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GALGOTIAS UNIVERSITY, GREATER NOIDA, INDIA

DECEMBER - 2021

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING

GALGOTIAS UNIVERSITY, GREATER NOIDA

CANDIDATE'S DECLARATION

I/We hereby certify that the work which is being presented in the project, entitled **" Digitalisation of Patient Records using Blockchain "** in partial fulfillment of the requirements for the award of the **BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING** submitted in the **School of Computing Science and Engineering** of **Galgotias University, Greater Noida**, is an original work carried out during the period of **JULY-2021 to DECEMBER-2021**, under the supervision of **Dr.M.THIRUNAVUKKARSAN, Assistant Professor**, **Department of Computer Science and Engineering** of School of Computing Science and Engineering , Galgotias University, Greater Noida.

The matter presented in the project has not been submitted by me/us for the award of any other degree of this or any other places.

AKANKSHA TYAGI – 18SCSE1010145

AVIRAL GUPTA – 18SCSE1010548

This is to certify that the above statement made by the candidates is correct to the best of my knowledge.

Supervisor

(Dr.M Thirunavukkarsan, Assistant Professor)

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of **AKANKSHA TYAGI – 18SCSE1010145, AVIRAL GUPTA – 18SCSE1010548** has been held on _____and his/her work is recommended for the award of **BACHELOR OF TECHNOLOGY IN COMPUTER SCIENCE AND ENGINEERING**.

Signature of Examiner(s) **Signature of Supervisor(s)**

Signature of Project Coordinator **Signature of Dean**

Date:

Place:

ABSTRACT

Contemporary healthcare information systems are exceptionally fragmented. While growing volumes of personal healthcare data are being created by a plethora of sources – from physicians to pharmacies, laboratories to hospitals, even our mobile phones and smart devices – the information remain, in almost every case, isolated within data silos – segregated and inaccessible from outside the confines of closed and proprietary systems. Not only is this inefficient, but it restricts the ability of a healthcare provider to operate with the most complete set of patient information available in real-time in order to deliver optimal health outcomes. Blockchain technology – and more specifically – a single global blockchain, offers a solution – and healthcare organizations are increasingly taking notice of its transformative potential.

A blockchain-based records system would empower patients to retain full control over their data, choosing when, and to whom, to grant permission to access their information. That could be giving permission to a healthcare provider in a physician-patient setting or could extend to commercial uses – authorizing access to your data by a pharmaceutical manufacturer conducting clinical research in exchange for you receiving micropayments of digital currency.

Putting the patient in control would also make switching between healthcare providers a far simpler process than presently, while ensuring that any information provided is complete and verifiably accurate – a process that could be applied to a variety of scenarios.

TABLE OF CONTENTS

CHAPTER-1

INTRODUCTION

1.1 Introduction:

Blockchain technology – and more specifically – a single global blockchain, offers a solution – and healthcare organizations are increasingly taking notice of its transformative potential.

A single global blockchain can serve as the basis for a universal global electronic health record, offering a secure digital environment, capable of storing and managing patient information in a verifiable manner, publicly accessible in real-time by anyone in the healthcare service provider chain (if authorized by the patient). Each new item of information could be integrated to provide an up-to-date, comprehensive picture of patient health, enabling physicians, pharmacies and other providers to provide better health care guidance to patients. And by using the blockchain, we can iterate and innovate beyond the limitations of existing systems by leveraging its unique features. The same protections applied to prevent the double-spending of digital currency could be used to prevent double-filling of pharmaceutical prescriptions, while blockchain private keys could be implemented as a way to authenticate identity and validate insurance coverage.

Whether patient data is stored directly on the blockchain (with privacy protections) or off-chain (and managed through on-chain access rights), a blockchain-based system of electronic health records would not only enable healthcare providers to take a holistic view of patient information and produce better health outcomes; it would rebalance the information paradigm and put the ‘personal’ back in ‘personal health’.

In a year in which medical jargon and population health figures have become a regular part of our every day (socially distanced) discourse, it’s perhaps unsurprising that for many of us, the year has also brought with it a heightened desire to impart more control over our personal healthcare.

A blockchain-based records system would empower patients to retain full control over their data, choosing when, and to whom, to grant permission to access their information. That could be giving permission to a healthcare provider in a physician-patient setting or could extend to commercial uses – authorizing access to your data by a pharmaceutical manufacturer conducting clinical research in exchange for you receiving micropayments of digital currency.

Putting the patient in control would also make switching between healthcare providers a far simpler process than presently, while ensuring that any information

provided is complete and verifiably accurate – a process that could be applied to a variety of scenarios.

The potential for blockchain technology to impact the healthcare sector extends beyond a purely patient-provider paradigm too. Blockchain solutions can ensure honesty and facilitate transparency in the development of pharmaceutical products, an oft-elongated process subject to strenuous checks for data integrity or 'hygiene'. If data is not properly recorded, or worse, is deliberately fabricated or obfuscated – entire studies, along with potentially billions of dollars and years of time, can be invalidated entirely. Blockchain technology enables easy, auditable tracking of datasets generated by clinical researchers, benefitting government agencies tasked with approving pharmaceuticals and producing better health outcomes for patients.

CHAPTER-2

LITERATURE SURVEY

The review explores the area of electronic health record management systems with a particular focus on the techniques and performances of such systems during catastrophic events and subsequent mass crises. A significant part of the literature, before the introduction of smart contacts on the blockchain, mainly focuses on frameworks and systems for sharing EHRs on cloud infrastructures [39][41]. The introduction of a new approach to express complex logic on the blockchain through a Turing-complete language started a new research path focused on distribution and peer-to-peer communication [52]. In fact, after Ethereum, a new set of frameworks and systems adopting the decentralized philosophy have been studied and proposed both by the academia [3][12][22][29][39][53] and the industry [32]. These frameworks adopt different blockchain models spanning from Ethereum to the subsequent implementations (i.e., Hyperledger, Corda or Tendermint) Before digging into the previous and current work, it is necessary to clarify the difference between Electronic Medical Records (EMR) and Electronic Health Records (EHR). In fact, the two terms might seem to mean the same thing and are often used interchangeably, but they are two different types of digital records. The former can be considered as the digital equivalent of a patient's paper

record used by practitioners. It contains the patient's medical history with diagnoses and treatments given by a particular physician. The latter, instead, is a more general record including the entire patient medical history meant to be shared with other authorized users from across different healthcare providers [45]. Some cloud solutions to the problem of EMR accessibility and sharing have been proposed in [39] and [41]. Patra et al. [39] studied how cloud computing can be employed to facilitate and improve services of the healthcare sector, especially for rural areas. The system must meet a list of requirements including availability, scalability, security, data transmission storage and collection methods. They argue that it is possible to store patient data in the cloud in a cost-effective way. This data can then be shared and accessed by doctors and medical professionals. However, they do not elaborate the concept and limit the scope to a high-level design model without implementation or tests. Starting from the concepts in [39], Yue et al. [54] presented the architecture of so-called data gateway application for healthcare data based on the blockchain. They claim to be the first to propose a system based on the distributed ledger technology and address requirements like EHR sharing and patient control over the data. The architecture expects a private blockchain to run on the cloud, but neither they specify how it should be implemented nor provide performance tests. The firsts to introduce a fully functional prototype, applying blockchain technology to EHRs are Azaria, Ekblaw et al.[3]. They propose a

system called MedRec not only designed to control the access and authenticate the users but also to manage EMRs in a distributed fashion with the aim to address problems like health data fragmentation, slow access, system interoperability, patient agency and improved data quality and quantity for medical research. They attempt to achieve this by describing a system with a modular design meant for integration. In fact, for scalability issues and to facilitate the adoption, the actual medical record is not stored on the blockchain but is kept off-chain on the hospital, provider's relational database. The blockchain holds metadata and references to the EHR location. More precisely, a smart contract manages the interaction between actors and data and defines access rules and pointers to this data. The pointer is a tuple including a query string that shall be executed on the provider's database as well as the location (host port and credentials) where to access the EHR [3]. The prototype is developed using the Ethereum public blockchain: the access control is based on the user's public keys that are Ethereum addresses and the stakeholders participate in the network as "miners" (they run a node). It implies that every party (patient included) must have a blockchain node to interact with it. The main drawback of this implementation is that every actor in the system must have a full copy of the data. Another disadvantage is the poor scalability caused by the consensus protocol. Even though the authors do not mention this possible limit, it is possible to set the upper bound to 60 transactions per second[16] The work that

has been done after MedRec focused on access control, data sharing between health provider and data integration, as suggested by US legislation, HIPAA [11]. A considerable part of the research also focused on the patient agency and control over her information as well as mechanisms to assure privacy and security when the data is aggregated and accessed for research purposes. The different frameworks, architectures, and prototypes, that have been developed until now, can be divided into two different categories depending on the blockchain model that has been used: permissionless [29][22] or permissioned [12][32][53]. For the proposals based on public blockchain implementations, it is worth mentioning the work of Linn and Koo [29] as well as BlocHIE by Jiang et al. [22]. Linn and Koo depart from the work of [3] on MedRec and argue that the EMRs must be stored off-chain in a structure called data lake. This is necessary to achieve scalability in that a blockchain modeled after Bitcoin would result in large files and expansive records replication among all the nodes in the network thereby increasing bandwidth usage and wasting network and storage resources [29]. Their work focuses on the discussion of some key interoperability challenges in the health sector and how blockchain could be used to address these problems. Moreover, they briefly discuss some technical solution on topics like scalability, access security, and data privacy. However, the authors neither propose a new system nor illustrate a design, but rather describe some basic principles for a possible work-

flow. Furthermore, they only mention fault tolerance and disaster recovery characteristics related to replication and lack of single point of failure, without either assessing or describing how it would work. Jiang et al. [22], instead, describe and implement a Healthcare Information Exchange (HIE) platform based on blockchain and working in the cloud. They argue that cloud service providers have taken great responsibility to provide a controlled, cross-domain and flexible HIE platform but they still struggle to provide data sharing services. The authors propose a platform called BlocHIE. The platform's architecture consists of two loosely coupled Blockchains called EMRChain, and PHD-Chain. The former is used to store Electronic Medical Records generated by healthcare institutions and combines off-chain storage and on-chain verification like the other systems mentioned so far. The latter is a separate chain to store Personal Healthcare Data (PHD) generated by the patient. The authors also propose a consensus algorithm based on Proof of Work with a modified mechanism of transactions packing. The transactions are grouped into blocks using a collaborative algorithm to reduce the amount of replicated work and in crease throughput and fairness. Preliminary tests on this new mechanisms show a throughput of 46 transactions per seconds which is higher than both Ethereum and Bitcoin current throughput. The PHD-chain is designed for a considerable amount of data uploaded by the patients. It assumes the use of IoT devices and wearables able to poll data several times during a day.

However, the performances are not enough to be used in real scenarios and have not been tested under stress and crises settings. One of the first attempts was made by Xia et al. [53]. The authors propose a permissioned network running on the cloud and an evaluation of its scalability. In addition, they suggest a new block structure to improve the performances compared to the Bitcoin network. However, it is not clear how the new structure would improve the overall performances as no demonstration is provided. They also attempt to quantify the amount of data shared in a blockchain network per time frame based on different parameters like throughput and transaction size. However, the analysis is just esteem based on assumptions and is not the results of any test run on their proposed system. Dubovitskaya. Xu et al. [12] go forward by proposing a framework and showing different scenarios where the use of shared ledger can ensure privacy, security, availability and fine-grained access control over EMR data. The authors show the design of a prototype of an oncology-specific clinical system to share medical health records for primary patient care. Their solution is meant to facilitate the consent management and speed up the transfer of data between hospitals as well as improve the management of long-lasting treatment and life-time monitoring for patients affected by cancer. The patient data is encrypted and stored off-chain in a cloud repository while the access permissions and EHR metadata are on-chain. The system is built on top of Hyperledger Fabric and runs a PBFT consensus. However,

the scalability of the prototype has not been tested in real a use case. The authors argue that PBFT consensus has excellent scalability properties tested up to tens of nodes and only hint the role of block size. They set the analysis of performances as future work. Finally, Medicalchain [32] is a case taken from the industry with characteristics to the other proposals. The user becomes the owner of its health record and gains full access and control over the data it holds. It also serves to provide transparency between different parties involved in someone's healthcare, in particular hospitals, clinics, and health insurances. The whitepaper is a business plan, with just a few technical details. There is no mention of scalability properties. It is worth mentioning the technique they employ to achieve patient safety: a backup access system for emergency situations. The backup could be particularly helpful during disasters when the patient is unconscious and unable to give consent. The system consists of an emergency bracelet that the user caregivers can scan to obtain the precious information.

CHAPTER 3

PROJECT DESIGN

3.1) Design Goals

Whether functionalities, characteristics or qualities, the literature provides essential insights on the requirements that this system should fulfill to improve the doctors and personnel's operations as well as the security of the healthcare chain. The following list identifies the most relevant requirements, as shown by the literature of blockchain and records.

• Scalability: a record system should be able to scale with the number of users that operate with it. In the context of the blockchain, a system should be able to work seamlessly with any number of nodes and users in the network

• Security: the information shared and stored within the system must remain confidential, correct and available. In case of disasters and disruptions, the system must also be able to resist or recover from the emergency. It is necessary to ensure that hospitals can provide help and assistance when it is needed the most

• Identification: every user that interacts with the record system must be identified, and the access to any piece of information must be granted or restricted based on this identity .This requirement excludes public blockchain implementation because

anonymity and pseudonymity is an inherent characteristic. Ideally, it is possible to map an identity to the corresponding pseudonymous, but this compromises the privacy and confidentiality of the patient-physician relationship.

• Privacy and access control: as mentioned in the background, identification enables access control and privacy. The information is restricted to only those who can access it: a doctor may access and modify a record only with the patient consent. In addition, every interaction between the user, either a patient or a doctor, and the health record must be traced.

• Patient control: the patients should be able to access their personal record. Not only it enables the patient to integrate the records with notes and additional information, but also to make them aware and more engaged in their own healthcare, especially for patients with chronic diseases .Blockchain could also allow full control and ownership of the personal record, thereby granting access and sharing information only upon consent or emergency situation.

• Data sharing: as a patient can seek treatments in different hospitals and clinics; the healthcare facilities must put in place a system to share data securely .

• Data analysis for the research: a large part of the literature emphasizes the importance of research on medical data. Provide anonymized clinical information is essential to advance the investigation of new treatments and cures. Therefore, an

EHR system must take into account mechanisms to aggregate and transmit anonymized information to research laboratories .

• Integration: finally, a new system that provides all the capabilities above, must be designed for integration. In fact, EHR management systems on blockchain are not meant to replace current systems completely, but to integrate and provide the features that were missing .

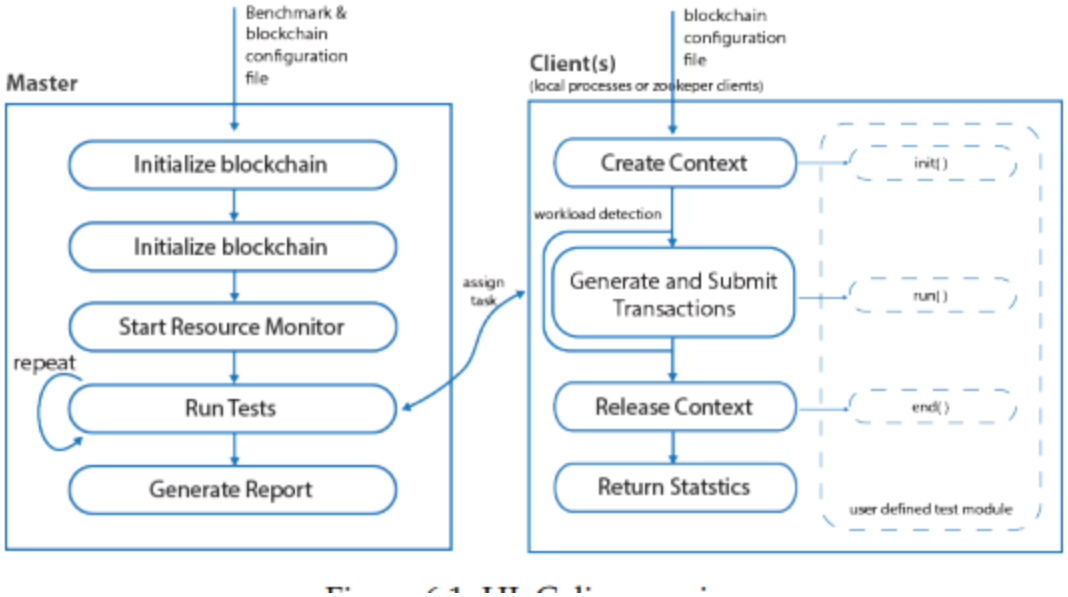
3.2) Tools

Hyperledger Caliper: HL Caliper is an open-source framework, under the Hyperledger umbrella and supported by various companies (IBM, Oracle, Huawei et al.), that provides users and developers with a tool to evaluate the performance of different blockchains. One of its declared purposes is to cope with the lack of source code of benchmark solutions that make it hard to both validate the results and to perform the same evaluation on different projects. It also attempts to cope with a lack of a common definition of performance indicators by relying on the definitions provided by the Performance & Scalability Working Group. In order to understand the validity of the results produced by HL Caliper, it is important to mention the modules that compose the benchmark tool. The architecture consists of three layers:

• Adaptation Layer: is used to integrate HL Caliper with different blockchain implementations and use cases. It contains a set of adaptors to interface with a particular use case.

• Interface and Core layer: is formed by different modules that allow monitoring the resources, analyzing the performances, invoking and installing smart contracts on the blockchain, and generating the final report.

• Application/Benchmark Layer: contains scripts implemented by the user to test a particular blockchain use case. These scripts form the test suite that is used to measure the performances. This layer holds a benchmark engine that executes the tests using a master-workers strategy as shown in figure, the master node generates worker threads to which it assigns tasks. Each task is in charge of one operation on the blockchain, that can be either smart contact initialization, execution or cleanup.



The caliper architecture composed by a master node that orchestrate a pool of client that communicate invoke and query the blockchain implemented for the particular use case.

The test were executed on three different machines with the following characteristics:

• Operating system: Mac OSX;

• HL Fabric components run in Docker container with the following resource allocation: – 8 CPUs; – 16GB of memory.

• The HL Fabric network setup was the following:

– HL Fabric version v1.1.0;

– The peers storage was the default LevelDB database;

– The ordering service based on Kafka: 3 Zookeeper servers and 4 Kafka brokers

The prototype was tested in two scenarios: the normal state and the emergency state.

Ruby on rails:

Ruby on Rails is known as an MVC (model-view-controller) full-stack framework. The code is separated into three interconnected layers:

Model contains the logic of an application, all the essential data, and high-level classes.

View is the UI representation of the data present in Modal. It's what users interact with and see on their screens.

Controller connects Model and View, receives user input, and decides how to handle the input.

Ruby on Rails centers around two main principles, also known from other programming frameworks.

Do Not Repeat Yourself (DRY)

This first principle states: *"Every piece of knowledge or logic must have a single, unambiguous representation within a system."* The logic behind it is straightforward. Coding the same things repeatedly, in different parts of an application, clutters the codebase, slows down development, and makes maintenance a lot harder.

When developing in RoR, you split the application's logic into smaller, reusable units. You then reuse them throughout the code by simply calling them. When you need to update either piece, you update once, and the change applies across the entire codebase.

Convention over Configuration (CoC)

This second principle is also about simplifying development and cutting down on time needed to ship the code. Convention over Configuration means that the RoR assumes various logical situations for you, by using the underlying, native functions, classes, variables and procedures.

In this way, it decreases the number of decisions you make, and cuts down on the complexity usually associated with configuring each application area. And if you're unhappy with the default settings, you can overwrite them with your code and adjust the environment to your needs.

CHAPTER 4

MODULES

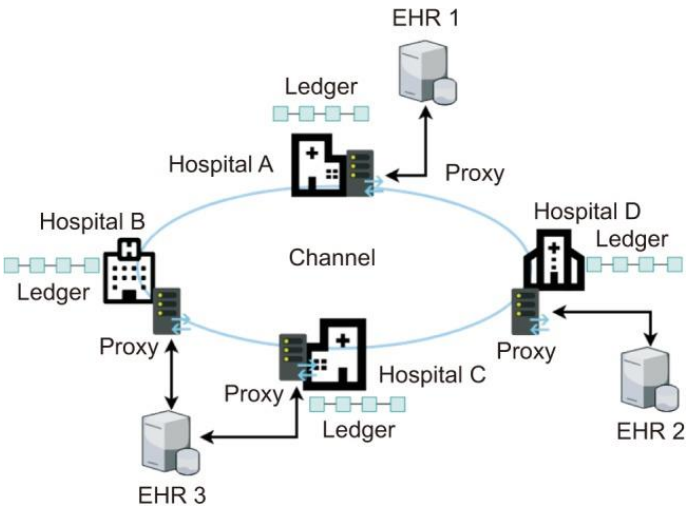
Hyperledger Fabric

In HLF, there are several key that play pivotal roles in the system. In addition, it provides three phases of consensus to validate transactions before uploading them to the ledger. HLF provides a variety of special designated chaincodes called system chaincodes to perform certain privileged tasks. Examples of system chaincodes are Configuration, Life Cycle, Query, Endorser, and Validator system chaincodes. In our study, we designed several prerequisite chaincodes and implemented them in our prototype system.

System Conceptual Design

We built a private subnet of an HLF network where the same ledger is shared among the hospital members ,which is called a channel. Organizations or departments within them can constitute independent channels with relevant ledgers according to their needs. In practice, medical data is usually too big to handle directly in a ledger; therefore, data is kept in an records, and only the address is recorded in the ledger. Such storage type is called on-chain or off-chain according to whether the data is in a ledger or not. A ledger also contains the hash values of

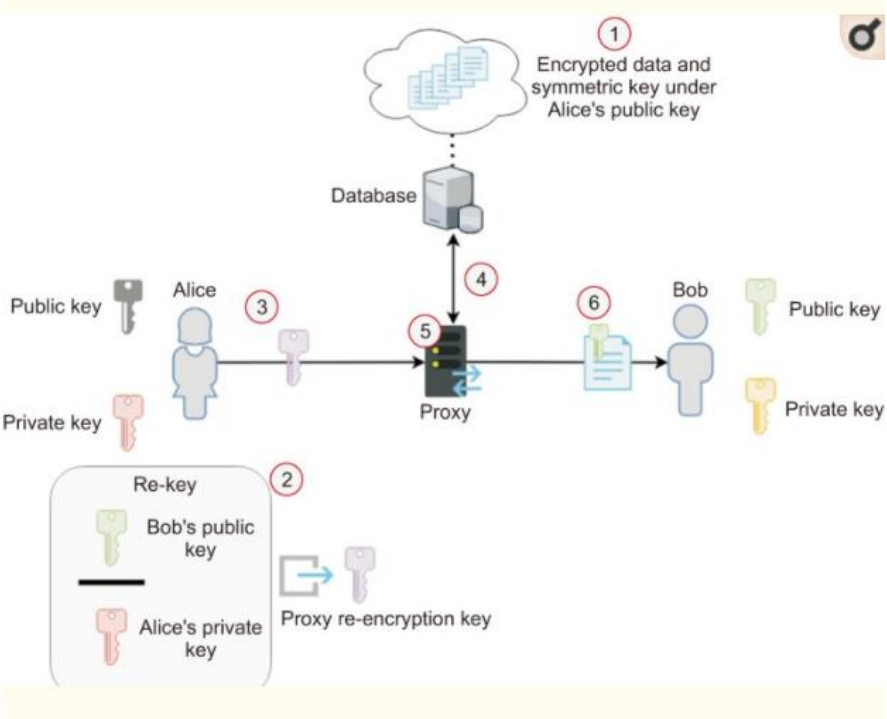
data. This guarantees data integrity because once a piece of data is written in a ledger, it becomes immutable, and this allows the user to check whether the data has been altered or not.



Cryptographic Scheme

Before patient data is uploaded to the records with the patient's consent, the data is encrypted using an adequate symmetric key. Then the symmetric key is asymmetrically encrypted using the patient's public key and attached to the encrypted data. This hybrid encryption makes the procedure efficient in terms of both speed and convenience because the encryption of large data can be done faster by symmetric-key than asymmetric-key, while the latter is more convenient in the encryption of small-size cryptographic key.

To read patient data, a proxy downloads it from the relevant record and sends it to the receiver. However, in case the receiver is different from the patient, the encrypted symmetric key at the data should be transformed, so that it can be decrypted by the receiver's private key. To do this, we use a proxy re-encryption scheme in which the patient generates the proxy re-encryption key by mathematically combining their private key and the receiver's public key using the AFGH algorithm. After receiving the newly made re-encryption key, the proxy re-encrypts the symmetric key for the receiver. In that process, the symmetric key is not disclosed to the proxy. Otherwise, the proxy must send the data to the patient to make it encrypted using the receiver's public key.



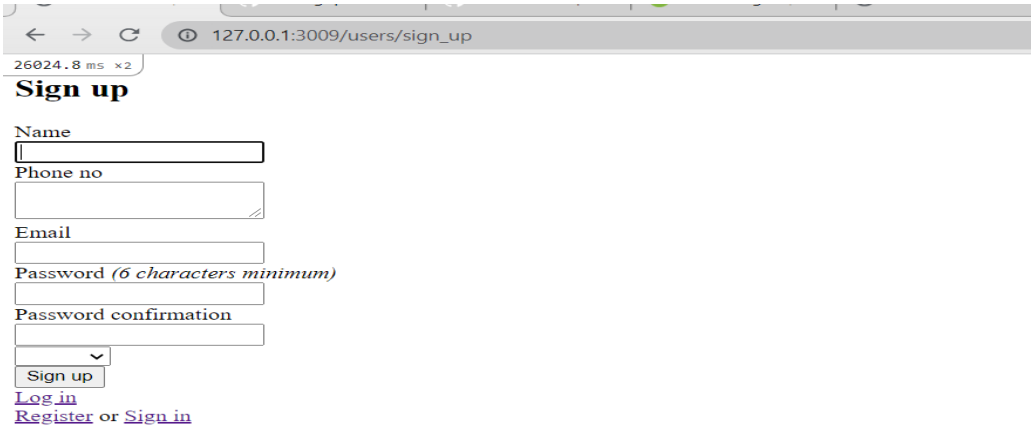
Web-Based Application

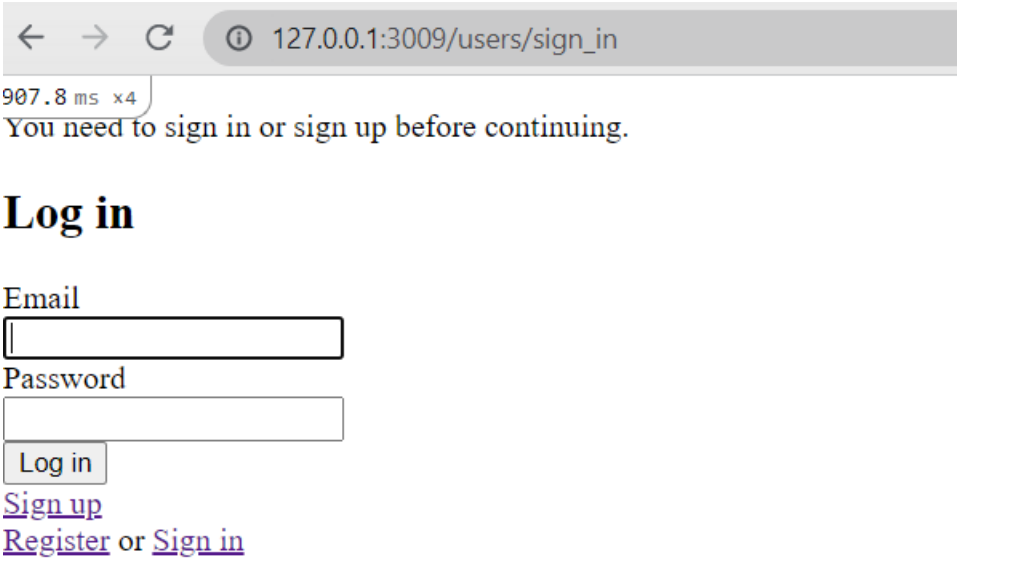
Our system provides web-based application for clients in each hospital to make access requests to the ledger or record. Web-based application is the front-end side application program available in a hospital or clinic. A hospital can have a single peer or many peers according to their scale, while a small clinic functions as a client without peer. For identifying participants across the system, doctors in each hospital are assumed to have their ECerts.

Web-based application offers web-based user interfaces and essential interactive functions in communication between participants in the system. Patients use it to

generate key pairs to register and enrol their identities to the system to obtain ECerts. In addition, they can generate proxy reencryption keys and send them to the proxy. On the other hand, the client uses this web-based application to create a transaction proposal and submit it to the blockchain system for the tasks such as identifying a patient's identity and creating, uploading, and sharing medical records, metadata and so forth.

1.)Login/Sign Up





2.)Appointments

7008.1 ms ×3

Welcome! You have signed up successfully.

Welcome Aviral gupta !! Have a nice day .

Recent appointments

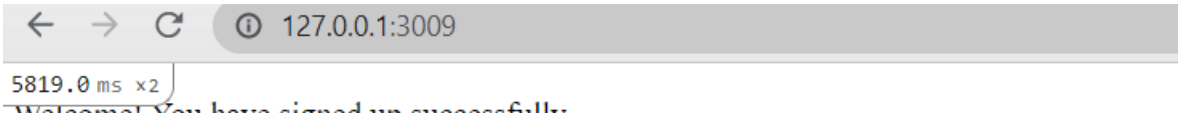
Book Appoitnment
Signed in as aviralgupta222@gmail.com. Sign out

5841.4 ms ×2

Details of Dr. Bansal

Name : Dr. Bansal
Qualifications :-
Specializations :-
Certifications :-
Book Appointment
Signed in as aviralgupta222@gmail.com. Sign out

3.)Prescription



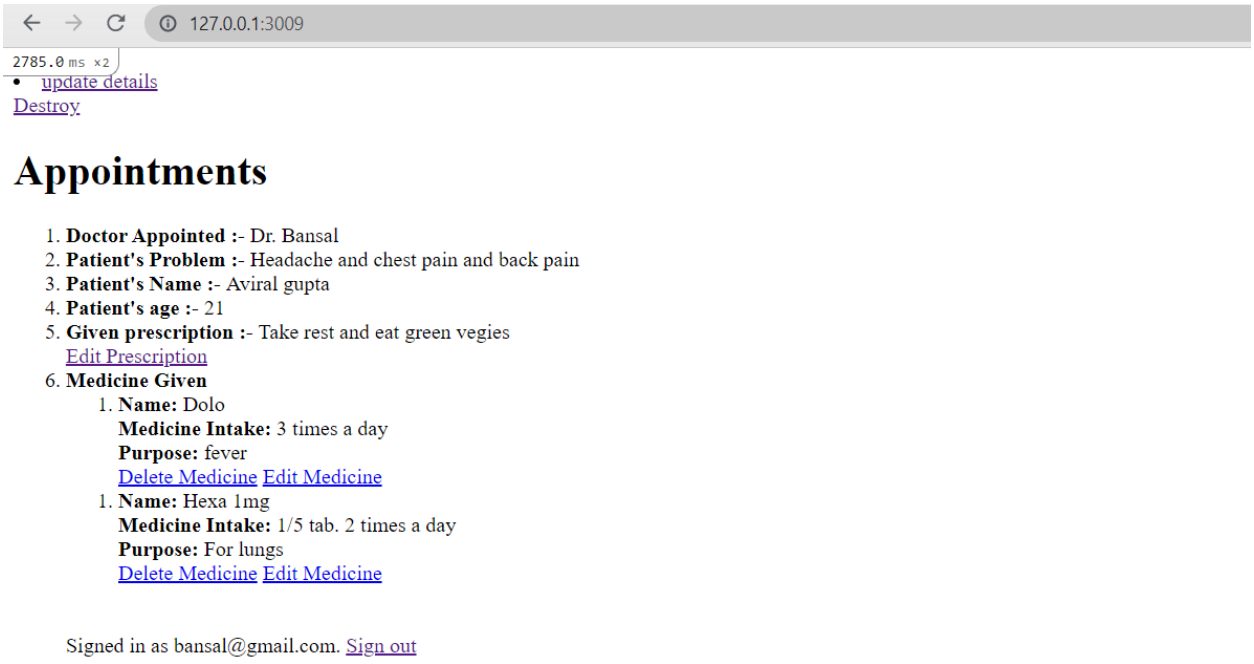
Welcome! You have signed up successfully.

- update details

Destroy

Appointments

Signed in as bansal@gmail.com. Sign out



Source Code:

```
class Medicine < ApplicationRecord

  belongs_to :appointment

 validates :name, presence: true

 validates :purpose, presence: true

 validates :medicine_intake, presence: true
```

```
end


class Patient < User
  has_many :appointments, :class_name => "Appointment"
  has_many :doctors, through: :appointments


end


class UsersController < ApplicationController
  before_action :authenticate_user!, except: [:create, :new]


    def show
        @user = current_user
        @patient=current_user
      end
```

```
 def new
    @user=User.new
 end


def create
 @user=User.new(user_params)
 if @user.save
  redirect_to edit_user_path(@user)
 else
  render :new
  end
 end
 def edit
  @user = User.find(params[:id])
```

```
end

def update
  @user= User.find(params[:id])

  if @user.update(user_params_second)
    redirect_to root_path
  else
    render :edit
  end
end

def destroy
  @user = User.find(params[:id])
  @user.destroy
```

```
    redirect_to root_path
  end
  private
  def user_params
    params.require(:user).permit(:name, :phone_no, :type)
  end

  def user_params_second
    params.require(:user).permit(:specialist_in, :qualifications, :certifications)
  end

end
```

CHAPTER 5

RESULTS

We developed a prototype system to implement our concept and tested its performance including chaincode logic. The results demonstrated that our system can be used by doctors to find patient's records and verify patient's consent on access to the data. Patients also can seamlessly receive their past records from other hospitals. The access log is stored transparently and immutably in the ledger that is used for auditing purpose.

CHAPTER 6

CONCLUSIONS

We developed a prototype system to implement our concept and tested its performance including chaincode logic. The results demonstrated that our system can be used by doctors to find patient's records and verify patient's consent on access to the data. Patients also can seamlessly receive their past records from other hospitals. The access log is stored transparently and immutably in the ledger that is used for auditing purpose.

Our system is feasible and flexible with scalability and availability in adapting to existing EHRs for strengthening security and privacy in managing patient records. Our research is expected to provide an effective method to integrate dispersed patient records among medical institutions.

CHAPTER 7

REFERENCES

[1]S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri

Blockchain technology in healthcare: a comprehensive review and directions for future research

Appl. Sci., 9 (9) (2019), p. 1736

[2]T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula, M. Ylianttila

Blockchain utilisation in healthcare: key requirements and challenges

In2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom), IEEE (2018 Sep 17), pp. 1-7

[3]G. Moona, M. Jewariya, R. Sharma

Relevance of dimensional metrology in manufacturing industries

MAPAN, 34 (2019), pp. 97-104, 10.1007/s12647-018-0291-3

[4]M.H. Kassab, J. DeFranco, T. Malas, Giuseppe Destefanis Laplante, V.V. Neto

Exploring research in Blockchain for healthcare and a roadmap for the future

IEEE Trans. Emerg. Top. Comput. (2019)

1-1

[5] B. Shen, J. Guo, Y. Yang

MedChain: efficient healthcare data sharing via Blockchain

Appl. Sci., 9 (6) (2019), p. 1207

[6] U. Chelladurai, S. Pandian

A novel blockchain based electronic health record automation system for healthcare

J. Ambient Intell. Humanized Comput. (2021)

[7]P. Zhang, D.C. Schmidt, J. White, G. Lenz