***MID TERM REPORT OF***

**Authentication scheme for Patient-Centric Blockchain**

*A Graduate Project Report submitted to Manipal University in partial fulfilment of the requirement for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

**In**

**Electronics and Communication Engineering**

*Submitted by*

**Nikhil BM**

**160907478**

*Under the guidance of*

|  |  |  |
| --- | --- | --- |
| **Dr Rohini R Rao & Dr Manjuanth V Hegde**  **(External)**  **Assistant Professor- Senior Scale**  **Department of Computer Applications** | **&** | **Dr Rajiv Mohan David**  **(Internal)**  **Assistant Professor- Selection Grade**  **Department of Electronics & Communication** |

**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**MANIPAL INSTITUTE OF TECHNOLOGY**

(A Constituent Institution of Manipal Academy of Higher Education)

MANIPAL – 576104, KARNATAKA, INDIA

**MARCH/APRIL 2020**

A screenshot of a cell phone

Description generated with very high confidence**DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING**

**MANIPAL-56104, KARNATAKA, INDIA**

**CERTIFICATE**

**This is to certify that the project titled PROJECT TITLE is a record of the bonafide work done by STUDENT NAME (*Reg. No. <Register No>*) submitted in partial fulfilment** **of the requirements for the award of the Degree of Bachelor of Technology (BTech) in ELECTRONICS AND COMMUNICATION ENGINEERING of Manipal Institute of Technology, Manipal, Karnataka, (A Constituent unit of Manipal Academy of Higher Education), during the academic year 2019 – 2020.**

**ACKNOWLEDGMENTS**

**This section should contain the acknowledgements due to the Director, Dept HOD, Project supervisor, company personnel, department guide, Laboratory Incharge (where the work was carried out) and faculty members whose assistance was sought during the project work.**

**ABSTRACT**

Modern Healthcare industry has very important requirements related to security and privacy of the users' data. Health data typically includes a record of services received, conditions of those services, and clinical outcomes consequent of those services. Health data are stored in cloud storage or centralised server, making it a very easy target for malicious attacks and private information being illegally shared. Hence this critical information has to share in a secured environment. Therefore, the project’s objective is to provide an authentication scheme for a patient-centric blockchain.

Way back in 2008, the concept of blockchain was introduced has distributed records of money exchanges without the need for a central authority. One of the main advantages of blockchain in healthcare is in interoperability of health records, provide access to medical histories of the patient, doctors prescriptions and hospital assets, all of these in the blockchain architecture. The core properties of blockchain-like decentralised storage, authentication system, privacy and inclusion makes it ideal for our use case. For this project, we have developed a blockchain network providing a secure authentication system in a patient-centric use case.

Firstly, the design of three different levels of privacy between different stakeholders was identified. This has a significant impact in developing the network topology. The network setup and its topology have been obtained. A network between government, primary health centre and government hospitals have been created, and a sample token transaction has been implemented. A static front end user interface has been developed to make the network accessible for an end-user.

The security of health data is a major concern. In this project, a novel authentication system using Hyperledger Fabric based on blockchain technology to make patient-centric transactions. The proposed system solves this by conducting patient record transactions on the blockchain to create a patient-centric healthcare ecosystem. All health records of the patient have to authorised by the patient for any usage of these data. This makes it very difficult for unauthorised usage of health records. We also carried out the implementation of a referral authentication system and demonstrated the usability of the network in terms of throughput, latency and other parameters. Finally, we have used Hypereldger Fabric framework to design and implement the network.

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| **Table No** | **Table Title** | **Page No** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**LIST OF FIGURES**

|  |  |  |
| --- | --- | --- |
| **Figure No** | **Figure Title** | **Page No** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Contents** | | | | | |
|  | | | | | Page No |
| Abstract | | | |  | i |
|  | | | | | |
| **Chapter 1** | | | **INTRODUCTION** | |  |
|  | **1.1** | Introduction | | | 1 |
|  | **1.2** | Security in healthcare and its Importance | | | 2 |
|  | **1.2** | Motivation | | | 3 |
|  | **1.3** | Objective | | | 3 |
|  | **1.4** | Project schedule | | | 3 |
|  | **1.5** | Organisation | | | 3 |
|  | | | | | |
| **Chapter 2** | | | BACKGROUND THEORY | |  |
|  | **2.1** | Literature survey | | | 4 |
|  | | | | | |
| **Chapter 3** | | | **METHODOLOGY** | |  |
|  | **3.1** | Authentication System | | | 7 |
|  | **3.2** | Identity Management | | | 8 |
|  | **3.3** | Network setup and Topology | | | 8 |
|  | **3.4** | Use case scenarios | | | 11 |
|  | **3.5** | Analysis and User Interface design | | | 12 |
|  | **3.6** | Tools and Framework | | | 12 |
|  | | | | | |
| **Chapter 4** | | | **RESULT ANALYSIS** | |  |
|  | **4.1** | Network setup | | | 13 |
|  | **4.2** | User Interface | | | 15 |
|  | | | | | |
| **Chapter 5** | | | **CONCLUSION AND FUTURE SCOPE** | |  |
|  | **5.1** | Work Conclusion | | | 17 |
|  | **5.2** | Future Scope of Work | | | 17 |
|  | | | | | |
| **REFERENCES** | | | | | 18 |
| **PROJECT DETAILS** | | | | | 20 |

**CHAPTER 1**

**INTRODUCTION**

Smart technologies have significantly improved over the last decade. Healthcare systems which are used by hospitals have also adapted to these technologies. These technologies have become increasingly competent in handling large datasets. This section introduces relevant smart technologies which are currently in use in the health industries [1] [2]. Also, it introduces to some of the previous works and its shortcomings. At the end of this chapter, we will have good clarity on what we want to achieve and the importance of the result.

When the healthcare provision started in 1970, the development of measured IT frameworks has been observed. This timeframe was called Healthcare 1.0. During this time, healthcare frameworks were constrained and not facilitated with digital frameworks because of the absence of resources. Also, bio-medical machines had not been developed and integrated into networked devices. Due to which, prescriptions and reports were mainly in written form, which in turn increased the cost and time involved [1]. Next came the Healthcare 2.0 era. In this time, information technologies and health were combined to form the healthcare ecosystem. During this time, digital tracking was introduced, which provided imaging systems for a better understanding of the patient’s health. Simultaneously, new user enabled advancements started to develop in the healthcare industry, surfacing close by the advent of social media. Medicinal services suppliers started to make online networks for information and data sharing, storing health data on cloud servers, and give access to archives and patient records through mobile devices, empowering pervasive access for both the supplier and patient.

Next came the Healthcare 3.0, enabling user customisation of health records where shared. During this time, the introduction of Electronic Health Records (EHRs), wearable and implant systems took place. The era of Healthcare 4.0 started from 2016 to the present day. This time was derived from the idea of Industry 4.0, where Hi-tech and Hi-contact frameworks are being presented, such as cloud computing, big data analytics, blockchain and AI [3]. During this time, EHRs were shared on networks like social media, between clinicians. Interaction and exchange of data had become very simple.

*1.1. Security in healthcare and its importance.*

Introduction to the online exchange of health data and connection to a networked environment created its set of disadvantages. This digital environment created important requirements in the security and privacy of the patient’s health data. Privacy meant that having proper rights to view health records. It is also the point of determining who is allowed to access that information [4]. Due to these, many guidelines have been created to secure the data. Health data are often stored in cloud storage or centralised server, making it a very easy target for malicious attacks and private information being illegally shared. Health data typically includes a record of services received, conditions of those services, and clinical outcomes consequent of those services [5].  Another major challenge facing electronic health record systems (EHR) is to make it interoperable. For a complete picture of the patient, all of the important systems should be able to communicate with each [6] [7].

Security is to protect data from attacks, stealing of data, and it is very much important for addressing privacy [8]. In 2018 alone, there have been many data breaches which have resulted in 13 million healthcare records exposed in the US. Speaking about India, during the period of 1st October 2018 to 31st March 2019, a staggering total of 6.8 million health records were stolen [7]. These databases were sold in the underground. The most common electronic method used by hospitals to transmit health info was via a health information systems provider (HISP). Some of the other methods of information transmission are single EHR vendor, local health information, multi-EHR. Mailing or faxing are some of the common methods of data transmission [9].

EHR standards 2016 for India: Current laws regarding data ownership are [10]the physical or electronic records, which are generated by the healthcare provider, are held in trust by them on behalf of the patient. The patient owns the contained data in the record, which are the protected health information of patients. The healthcare provider will own the medium of storage or transmission of such electronic medical record. The “sensitive personal information (SPI) and personal information (PI)” of the patient is owned by the patient himself/herself**.** Security and Privacy Rules: The requirements for privacy and security are given in the following standard. ISO/TS 14441:2013 Health Informatics – Security & Privacy Requirements of EHR Systems for Use in Conformity Assessment [10].

*1.2. Motivation*

Storing of health data in a secured state is very much important. Currently, these data are stored in a centralised server or doctor-client servers. If these servers are not well up to date in terms of security updates, then these networks are prone to hacking and may result in serious data breaches. Storing data in the cloud has become more common in healthcare 4.0 systems. Storing health data with the third party is also dangerous if proper methods are not taken beforehand. All these systems have vulnerabilities. Yup et al. [11] had investigated the approach of using the blockchain framework in healthcare services with regards to security and privacy of the client. They proposed a data access control scheme for maintaining privacy and designed the healthcare data gateway. Zhang et al.[12]also proposed a PSN based system to make a secure healthcare ecosystem. He proposed protocols in sharing and authentication. Xia et al. proposed a blockchain-based system called MedShare [13]. This system had access control, provenance and security of medical records. Jiang et al. [14] proposed a system for the exchange of medical data using blockchain. This system also included off-chain and on-chain methods of storing medical data. There are different projects done by many other researchers addressing the privacy and security concerns of the digital health data, but the very few of it discusses the concepts of ownership of the health data.

The patients are the true owners of their health data, but this is usually not the case. Hospitals and other health data centres own our health data. This project focuses on designing a system which gives this ownership back to the patients. Usually, the main identifiers are removed from the health records and are sold for third parties like research labs and companies. However, with enough attributes put together, these companies can backtrack to the patients. This results in a lack of privacy for the patients and also this can be taken advantage of. This project designs a network keeping the ownership ideas in mind.

To achieve this, blockchain technology is used for the development of the network. The fundamental properties of the blockchain are privacy and security. Using these properties, I am making a patient-centric blockchain network. After completion of the network, the patient has complete ownership of the data. If third parties want to access the data, first the user has to grant permission, only then data will be shared with them.

*1.3 Objective*

To identify the user legality of access permission before getting the data or modifying it. Also, create a secure channel over an insecure network while communicating the data between two entities. By the end of the project, we will implement patient transactions. Transactions between users will be identified while considering the role and maintaining the privacy of the data.

*1.4 Project schedule*

|  |  |
| --- | --- |
| January | Literature survey, review of previously proposed work and study of different cryptosystems and blockchain-based authentication systems was completed. |
| February | Choosing the technology stack, design of the network topology and implemented three organisation blockchain was done. |
| March | Blockchain-based authentication system for two of the use cases mentioned in chapter 3.1 |
| April | Simulate the proposed scheme to study the impact on throughput, latency, load and response time. Along with this documentation will be done. |

*1.5. Organisation*

The rest of the report is as follows: Chapter 2 contains the background theory. Chapter 3 presents the methodology which contains the authentication, identity management and network setup, and topology. Chapter 4 describes the results obtained and, finally, Chapter 5 provides conclusions and suggestions for future research.

**CHAPTER 2**

**BACKGROUND THEORY**

In this section, we review some of the articles in terms of privacy and authentication. In terms of integration of blockchain system with the healthcare industry, there are very few articles which will be useful for the health sector. The major objective is to introduce access control for medical data by using blockchain technology. Comprehensive literature survey of some of the past articles which focus on blockchain in healthcare and some of them in privacy and authentication systems. Table 1 indicates some of the blockchain-based approaches to EHR systems.

There are four main stages for including blockchain technology in the health sector. Firstly, healthcare providers like hospitals have direct access to the blockchain network. That is, all health data are stored in the existing systems. There are many transactions like making appointments or doctor’s prescriptions in the network. All these transactions are done using the patient’s public and relevant data like patient’s IDs are stored in the blocks. The smart contracts bound all the transactions. If any of the third parties want to access the patient’s data, then the patient must authorise it, only then data will be made available. Data made available to third parties will be properly masked, and the data will be confidential for those who do not have access to it [2].

Some of the previous work of blockchain in healthcare in terms of privacy have been listed out. Uddin et al. [15]have implemented system architecture on a continuous patient monitoring system. This uses the patient-centric model. They have increased the security and privacy of the system and implemented them using network simulation. Gaby et al. [16] proposed a blockchain framework called Ancile. The main idea behind this framework was access control and interoperability of health records. Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. It uses Ethereum blockchain and uses smart contracts for access control and uses cryptographic techniques for security. They have followed HITECH and HIPAA guidelines. Abdullah et al. [17] and the team proposes blockchain-based platform names Medibchain. This framework follows patient-centric management and uses blockchain technology as security for storage in the cloud. This helps in maintaining privacy. They have used permissioned blockchain; as a result, anyone who wants to access the network requires permission.

Sundeep et al. [2] have implemented a patient-centric blockchain application for satisfying the needs of the healthcare 4.0. This article proposes algorithms for access control and also shows metrics on experimental analysis. Faisal et al. [18] have implemented a blockchain model for drug supply chain management. The main idea was to make a system such that they can track medicine from the manufacture to the pharmacy and helping in identifying counterfeit drugs. In this, they have discussed network topology, and the experimental analysis has been done. It uses Hypereldger Fabric framework for implementation.

Previous work in blockchain has been divided into five major categories which are architecture, access control policy, algorithms, framework and performance evaluation. The table gives a detailed scenario of the blockchain in healthcare.

Table 2.1: Blockchain-based approaches for an EHR system. Y indicates yes and N indicates No.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Author | Year | Objective | 1 | 2 | 3 | 4 | 5 | Results |
| Abdullah et al. [17] | 2018 | Patient-centric healthcare data management system using blockchain technology. | Y | N | Y | Y | Y | It achieves pseudonymity, privacy, integrity and security. Performance analysis shows good results. |
| Tien Tuan et al. [19] | 2017 | An evaluation framework for analysing private blockchains. | Y | N | N | Y | Y | Hyperledger performs consistently better than Ethereum and Parity across the benchmarks. But it fails  to scale up to more than 16 nodes. |
| Gaby G  Et al. [16] | 2018 | Propose a blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients’ sensitive information. | Y | Y | Y | Y | N | The Ancile framework demonstrates a blockchain system that achieves a high level of decentralisation while acknowledging that  some nodes ought to be of a higher authority. |
| Bhabendu  Et al. [20] | 2019 | The main focus of the survey is to provide a comprehensive analysis of wide applications of blockchain technology for the academic research community. | Y | N | N | Y | N | In this paper, challenges in implementing blockchain and its associated security and privacy issues have been discussed. |
| Wenbo Jiang et al. [21] | 2019 | Analysis of thin-clients into consideration where thin-clients indicate those users who cannot download the entire blockchain due to the limited storage capacity of their equipment. | N | N | Y | Y | Y | It analyses the burden on mobile devices. |
| Sukhwani et al. [22] | 2018 | To develop a permission-based blockchain platform | Y | Y | N | Y | Y | Identified permission blockchain integrity |
| Poslad and Poslad  [23] | 2018 | To suggest access policy to EMR based systems using blockchain | Y | Y | N | N | N | It says about finer granular control, but it's just theoretical only. |
| Guo et al. [24] | 2018 | To propose a secure ABE scheme with multiple authorities for blockchain in EHRs | N | Y | Y | Y | Y | Says about the Immutability of the information ledger |
| Zhang et al. [25] | 2017 | To develop a secure health system for an extensive network. | Y | N | Y | N | Y | Says about how to share the load of the network |
| Fan et al. [26] | 2018 | To strengthen efficient and secured health record sharing with a blockchain network | Y | Y | Y | Y | Y | Record management and sharing from EMR systems and access mechanism. |

1: Architecture 2:Access control policy 3:Algorithms 4:Framework 5:performance evaluation

In conclusion, various journal articles were read and understood to implement our problem statement. Each of the paper helped in understanding what technology stack need to be used, network topology, understanding algorithms, and helping in getting a better picture to achieve our objective.

**CHAPTER 3**

**METHODOLOGY**

In this section, we discuss the proposed approaches done to achieve the authentication system in the blockchain system. Firstly, we discuss the two use cases and how authentication for each of them is being done. Next, we talk about identity management in the blockchain system. Next, we talk about network setup and topology. Then we talk about the front end designing part.

*3.1. Authentication System*

The blockchain system architecture is described in this section. There are six participants in the systems: Patient, Private hospital, Government hospitals, Primary health care(PHCs), Insurance provider and research clinics. Since our system is based on patient-centric architecture, we have different levels of privacy and authentication systems, as shown in Fig 3.1. The innermost layer consists of three entities; they are a patient consortium, PHCs and government hospitals. This layer has a private and secure channel in which any of them can communicate. The rest of the two layers, which consists of private hospitals, medical research centres, labs and along with the first layer, are connected with the second channel. The second layer is made to be a public channel.

We have identified two types of use cases. There are mainly two types of transactions can be found in the working scenario. According to that authentication can be performed.

3.1.1. One to One transaction:

Firstly, direct transactions between patient and other organisations. To implement this transaction, authentication will be done using the certificate authority. The user who sending the request must have the digital certificate to get access the service. This is mainly done using three steps. First is the registration of the entities. Whenever the user wants to access the service, he/she should register to the network and must have the valid credentials. Next is login and mutual authentication. In this phase, users can access the system using the credentials which he/she chose during the registration. This phase also builds mutual trust between user and server before exchanging the records. Finally, after authentication, further communication takes place through key agreement. The systematic execution of this is shown in Algorithm 3.1.

|  |
| --- |
| **Algorithm 3.1**: Algorithm for user authentication using certificates. |
| **Input:** Request Q received at the blockchain database server.  **Output**: Access granted or rejected.  1: **if** request == valid certificate **then**  2: **if** login ID & User Signature== valid **then**  3: **if** current index value > Last stored index ^ Hash value ^ Timestamp == Valid **then**  4: Create a New Blockchain node and grant authentication.  5: **else**  6: Access rejected. Exit  7: **end if**  8: **end if**  9: **if** User == Exit in Blockchain Database **then**  10: Add new user Node  11: Initialise index value  12: Allocate current Timestamp value  13: Store Predefined value in Current Hash Value  14: Store Data Value  15: Update user record in Blockchain Database.  16: Add new user certificate  17: **else**  18: **go to** step 1  19:  **end if**  17: **else** Access rejected. Exit. |

3.1.2. Three way transaction:

The second use case is during the Patient-PHCs-Government Hospitals referral program. Here, the patient will be referred to the Government Hospital (GH) through PHC. Government Hospitals and Patients should authenticate each other through PHC before accessing the service because GH should believe that the case information received from PHC is related to the patient who is admitted for treatment. To execute the scenario, a digital certificate will not be sufficient for authentication. Hence there is a need to propose an enhanced authentication system.

Execution of the proposed approach:

This enhanched scheme has the following phases.

3.1.2.1. System Initialisation phase

Before moving in to the registration, the system initializes some parameters. Registration

Center (RC) selects an elliptic curve Ep over the finite field Fp with a large prime number 'p'.

Server also chooses a one way hash function h(.) → Z\* and a point on the elliptic curve 'P’ of order 'n'. Further RC selects 'x' as master key and computes the public key Ppub=x.P and publishes the parameters {Ep, P, Fp, h(.), Ppub }

3.1.2.2. Patient registration phase

In this phase, firstly users introduces their identity and password and wait for the verification process. After successful verification, it generates a concatenated number of the identity and password to compute the pseudo identity of the user. Then, calculates a hash function using number determined in the previous step. Lastly, it sends the registration request to the RC.

Then RC, upon receiving the request, it generates the random number e and uses it to find 100-bit hash using the secret key. Similarly using a hash function, RC generates 100-bit Value and message credentials and passed back to the patient. Lastly, RC generates 100-bit General ID which the patient can use for the transactions. A detail execution of patient registration process is as shown in Fig 3.1.2a .

|  |  |
| --- | --- |
| Patient  1) Patient first introduce his/her identity and password.  2) By using the identity and password, it calculates a pseudo random password called RPW.  3)Calculate hash function  4) User sends the registration requeste to RC | Registration Centre (RC)  1) RC uses the obtained ID and RPW and also the system parameters to calculate registration value V and registration message M. This is done using elliptic curve operations and hash functions  2)RC generates 100-bit General ID(GID) which the patient can use for the transactions  3) Return the M, V and GID back to the patient. |

Fig 3.1.2a

**3.1.2.3. Login and authentication phase**

**In this phase, patient verifies that the inputed ID and PW is correct or not. After verification, it generates a random number and encrypts the patient general ID, message M and timestamp T1 to create a message M1**

*3.2. Identity Management*

Identity management is necessary to map multiple identities with a single patient. If a patient visits different hospitals, he/she will be registered with varying IDs of the patient in the respective hospital. The identity management helps to map all these multiple identities with a single patient. The mapping of IDs makes it easy for the patient to collect his/her health information given by different hospitals.

*3.3. Network setup and topology*

This section describes the network setup of proposed blockchain based EHR system. The Fig. 1 represents the different transaction levels of the proposed system. At the centre of it all is organisation 1, the patient organisation. It is an entity responsible for maintaining peers through which patients can access their medical data. Like all other organisations, it is uniquely identified through the use of a digital certificate issued by a Certificate Authority(CA).

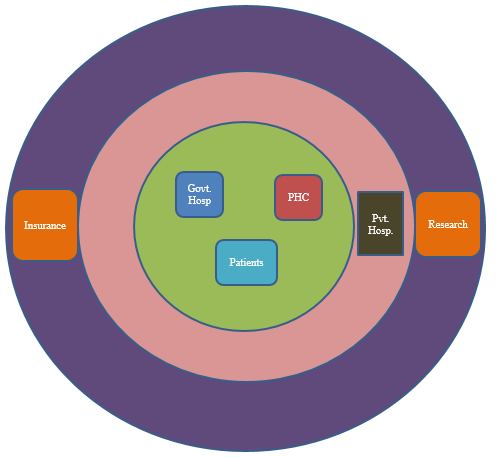


Fig 3.1: Three different privacy layers in the network design.

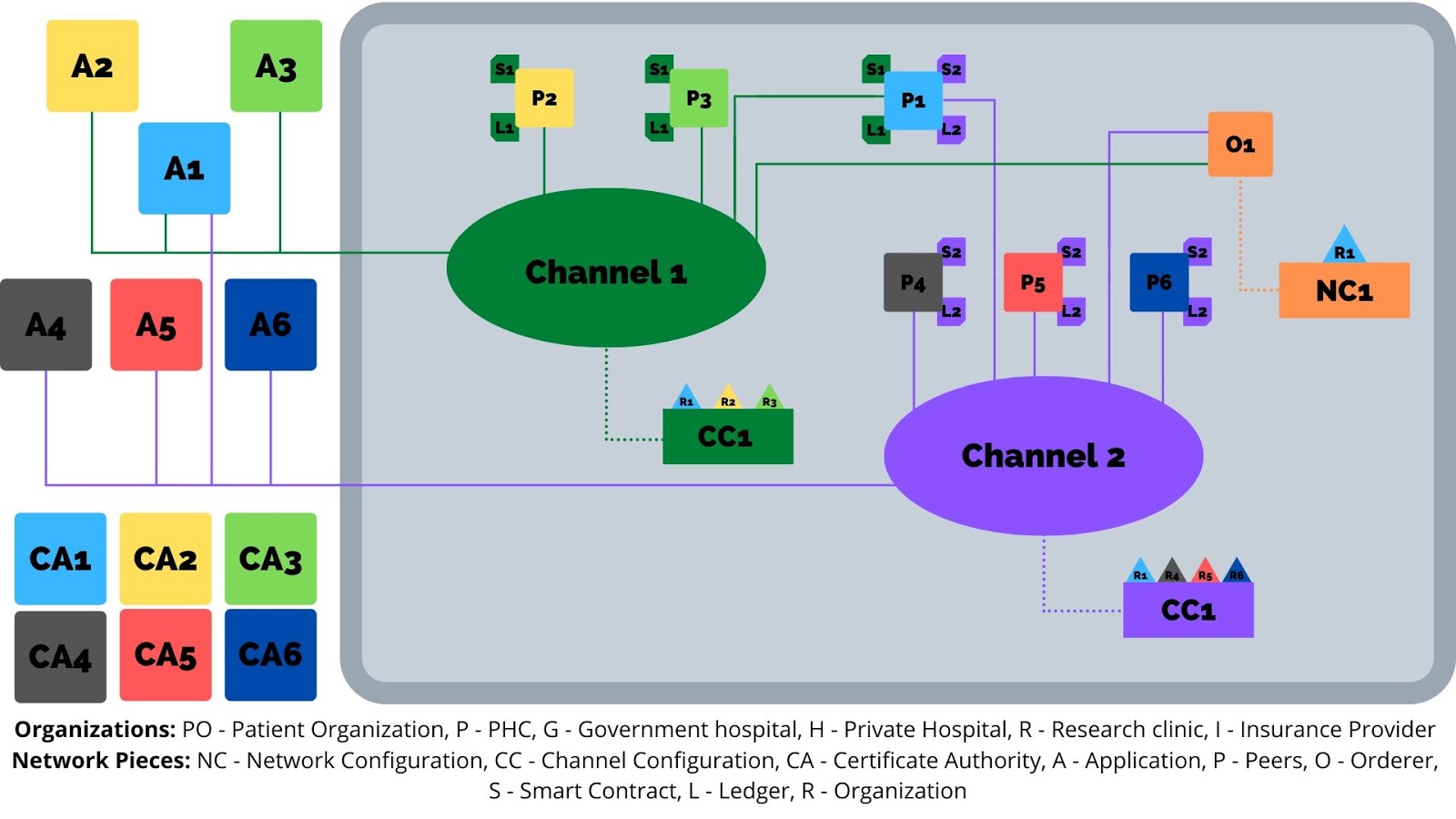


Fig. 3.2.1 System diagram for the implementation of our framework.

Network Configuration(NC), which contains the information about the system channel and several other details like the block size, ordering service and orderer information. It also defines access permissions such as who has the rights to create a channel, which is currently only given to the patient organisation. Likewise, the channel configurations comprise the details of the respective channels. Each organisation has its application interface to communicate through the use of a UI. They also have their own set of peers (one per organisation for now as per the diagram) with each peer having their own dynamically updated ledger and the respective smart contracts installed. Since we are using just one peer per organisation, for now, the peer is an anchor peer, and depending on the endorsement policy of the smart contract, it will be an endorser peer as well. The patient organisation owns the orderer, but during the deployment stage, there will be a shift from the Solo ordering mechanism to include orderers from other organisations and to increase the decentralisation.

Channel 1 is for the referral mechanism involving the writing of patient data on the blocks. The patient would initially go to the PHC (organisation 2). After their checkup, the patient medical data is written onto the blockchain. The patient may be referred to a government hospital (organisation 3), where further updates take place on the patient’s medical record on the blockchain. As a result, this channel is private. Channel 2 comprises all the remaining organisations who mostly have just read permissions. This channel is public that is all the organisations are connected to a single channel, and all of these can interact between themselves. This channel is for the second and third layers in the privacy layers of Fig 3.1. These read access are enabled through the use of smart contracts. An important point to be kept in mind is that the patient has complete control over who gets access to read, write or update his/her medical data, which enables privacy. Initially, we will be using the default settings for

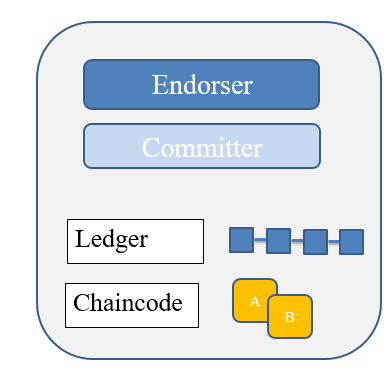


Fig 3.2.2. Diagram of a peer.

authentication, which involves the use of PKI and the default consensus mechanism.

Each of the peers has some of the components depicted in Fig 3.2.2. Firstly, they have the endorser peer, which endorses the transactions. There will be a copy of the ledger in each of the peers, and this ledger depends on the channel to which the peer is connected. Each peer will have a chaincodes installed on them. Chaincodes are smart contracts that are the set of rules and regulations.

Transaction Flow: Let us consider channel 1, with every transaction, requires endorsement from every peer in the channel.  
Step 1: A client initiates a transaction. Anyone of the organisations will first initiate a transaction through the use of their application SDK. An example of a transaction could be the writing of medical data for a new patient. When a proposal is made, a request is made for invoking the smart contract. This chaincode says what data can be read and/or written into the ledger (i.e. write new key-value pairs for the assets).

Step 2: Endorsing peers verify signature & execute the transaction. The endorsing peers verify that: transaction proposal is valid by checking the signatures and it also checks if the submitter is authorized to make the request. If each of this is valid, then it submits the request. During this time no updates to the ledger take place. If everything is valid, a “proposal response” which contains the signature of the endorsing peer’s is passed to the SDK.

Step 3: Obtained proposal response is inspected by comparing it with the endorsing peer’s signature to check if it is a valid response. If it is valid, the client makes the transaction. This is then broadcasted to the ordering services and other anchor nodes. Orderer receives all transactions and orders them according to the timestamp of the transaction. The orderer proposes a new block. World state gets updated. Each peer appends the new block to its a copy of the ledger.

*3.3. Analysis and User Interface design*

Analysis of the security is done using formal security proof. This is simulated using software named AVISPA. For practicality and user interaction, a user interface is being designed. This UI acts as the front end part of the network, and it is used mainly for the login/logout to/from the network and do transactions on the network.

*3.4. Use case scenarios*

Out of all the stakeholder scenarios mentioned as part of the different levels, the most important ones are as follows:

1. A patient visits the PHC for one or more checkups. For example, considering a pregnancy, a woman will be going for antenatal visits, for the delivery as well as postnatal visits. In case the PHC does not have enough resources, it may refer the patient to a government hospital. This referral would be a transaction. In the second part of this scenario, the government hospital will either accept or not accept the referral within 15 days depending on the priority flag. In this level, no privacy policies are required considering the nature of transparency required here.
2. A patient goes to a government hospital and the hospital refers the patient to a private hospital. Here, an authentication system needs to be designed keeping in my the privacy requirements.
3. A patient requires to go to a private hospital directly. The UI will list out all the hospital for a specific problem based on location, reputation and cost. In this case, the doctor and patient do not know each other, and hence, a different authentication system is needed to be designed, same as that used in point 2.

A third-party research clinic or the government may require to extract data (read only) for research purposes such as creating statistics

*3.5. Tools and Framework*

The blockchain-based framework, called Hypereldger Fabric, is used for developing the proposed project. Hyperledger Fabric is open-source software. It is developed b group called a Linux foundation. They support different blockchain projects and provide various support for different types of smart contract and different application. Fabric provides permissioned, and a consortium managed blockchain. It works on the assumption that the participants in the network are trusted and known to each other. This framework supports various coding languages like Java, Node JS, Go. and its mainly used to develop business networks. Fabric makes use of Docker engine for setting up the network. Docker is an operating system level container which is used by fabric. It helps in developing, creating and running fabric network by making each peer in the network as a separate container.

Automated Validation of Internet Security Protocols and Applications short known as AVISPA tool is used for providing the security proof of the authentication scheme. This tool provides a range of application for building and analysing formal models of security protocol. All the protocols are written in High-Level Protocol Specification Language or HLPSL.

The simulation PCs have the following configuration:

* 6 core CPU (Intel Core i5 8th Gen with turbo boost up to 2.8GHz)
* 16GB memory
* 1 Gbit/s network
* 250GB SSD

This section says about the methodology adopted for achieving the objective. It gives a detailed report on authentication schemes and why they are required. It also says about the setting up of the network and its configurations. At last, it says about the interface design, the tools and framework used.

**CHAPTER 4**

**RESULT ANALYSIS**

This chapter discusses the preliminary result obtained. As the project is in its midway, the analysis and simulation results [2] [1]have not been included since they are yet to be determined. The inner-circle present in privacy layers, which is patient, govt hospital and PHC organisation setup have been completed.

*4.1. Network Setup for single channel*

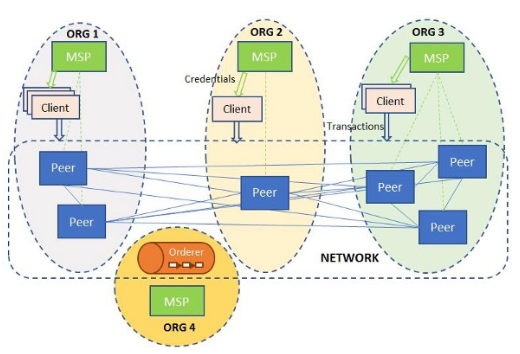
 [28]

Fig 4.1. The network setup for the innermost circle of the privacy layers.

First. We have created channel one has shown in fig 3.2.1. Once the channel has been created, the peers of three organisation, i.e. patient, govt hospitals and PHC are connected to the channel.

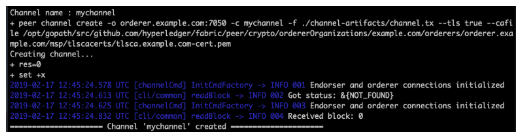


Fig 4.2: Creation of channel one.

After the joining of the peers, we need to configure the anchor peers. Anchor peers are the peers who are connected to other anchor peers of other organisation. Whenever a transaction has to be submitted, we use anchor peers for informing all the other nodes in the network.

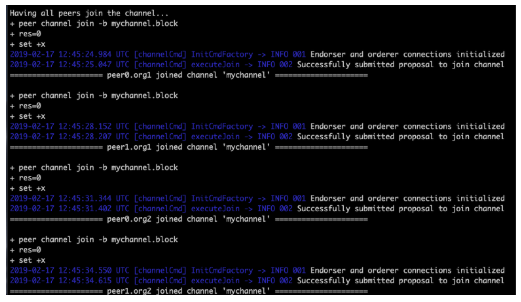


Fig 4.3: All the peers connecting to the channel.



Fig 4.4: Anchor peers are configured and joined to the channel.

When the user initiates the transactions, the peer first has to install the chaincode. That is the peer should be aware of the rules and regulation before handling the transaction. After installing the chaincode, in fabric, the chaincode must be instantiated on the peer. Only after instantiating the peer will be ready for the transaction.

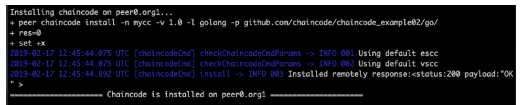


Fig 4.5. A chaincode is being installed in peer0 of the first organisation.

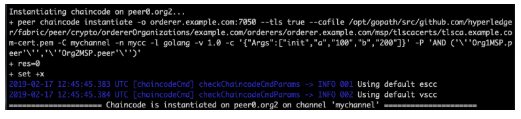


Fig 4.6. A chaincode is being instantiated on peer0 of the first organisation.

To simulate the transaction, we have assumed a scenario in which Party A has 100 tokens and Party B has 200 tokens. Now we make a transaction between A and B by sending ten tokens from A to B. Once the transaction is being completed, there will 90 tokens with A and 210 tokens with B.

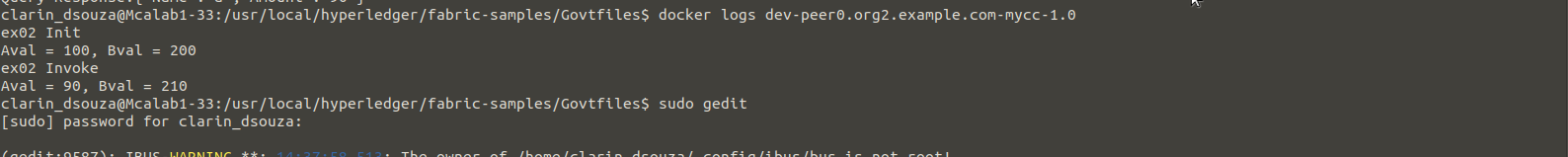
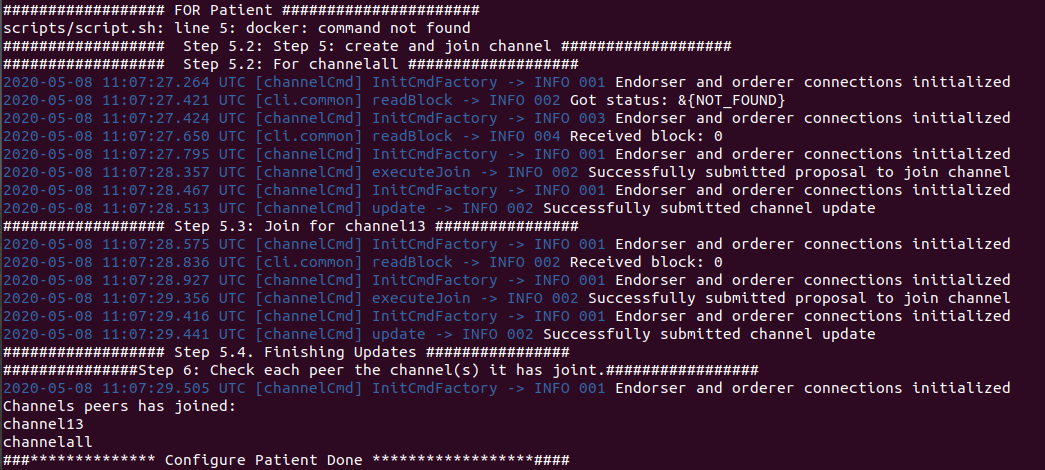


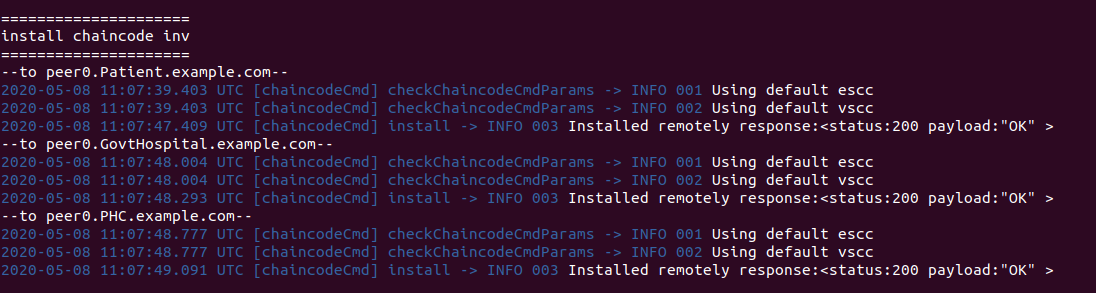
Fig 4.7. The values of token before and after the transaction.

4.2. *Network Setup for multi-channel*

First, we setup the network as show in Fig 3.2.1. We create channel one has shown in fig 3.2.1. Once the channel has been created, the peers of three organisation, i.e. patient, govt hospitals and PHC are connected to the channel. Then we create channel two which is the public channel, to which we connect all the seven organisations. After the joining of the peers, we configure the anchor peers.

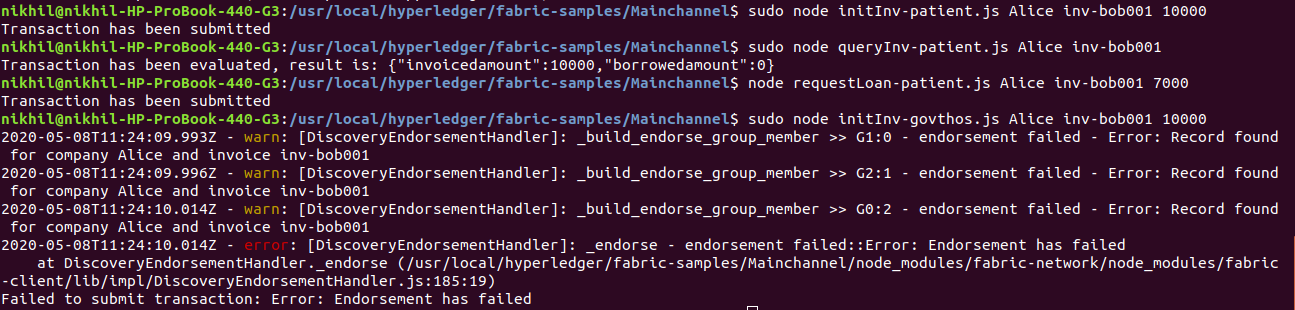
Fig: The patient organisation is connect to two channel as the network design i.e channel13 and channelall.

After this, we install a chaincode on two of the organisation i.e patient and government

Fig: Shows the installing of chaincode on the Patient, Govt. Hospital and PHC organisations.

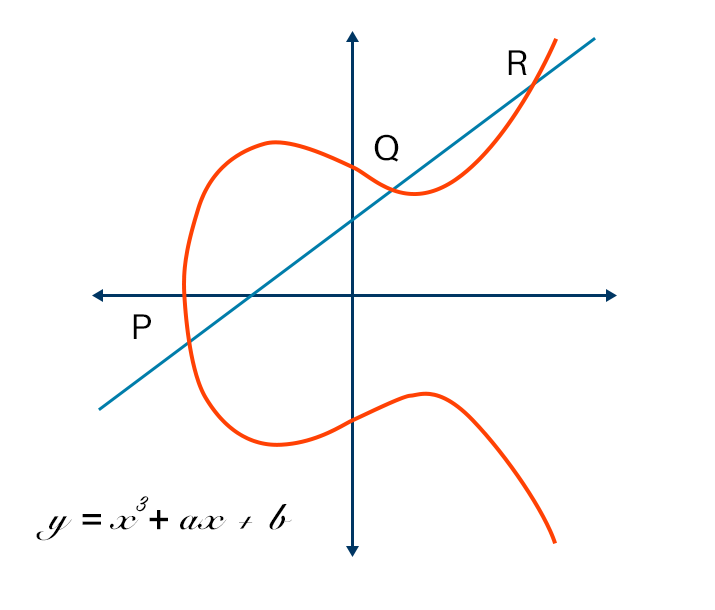
hospital. This chaincode is written to make transaction between two of these entities. Then, we create one patient user and one government hospital user to simulate a real life transaction.

For making a this transaction, we consider a banking example. We submit a transaction from the patient named Alice asking for money of 10000 from bank A. So bank A provides loan of 7000. This transaction is recorded in the blockchain. So if the Alice again asks for a loan of 10000 from bank B, then it will give error saying that money has been already been submitted by bank A. This transactions shows the working of the network.

Fig: Shows the registration of the patient Alice and asking for loan of 10k from bank A.

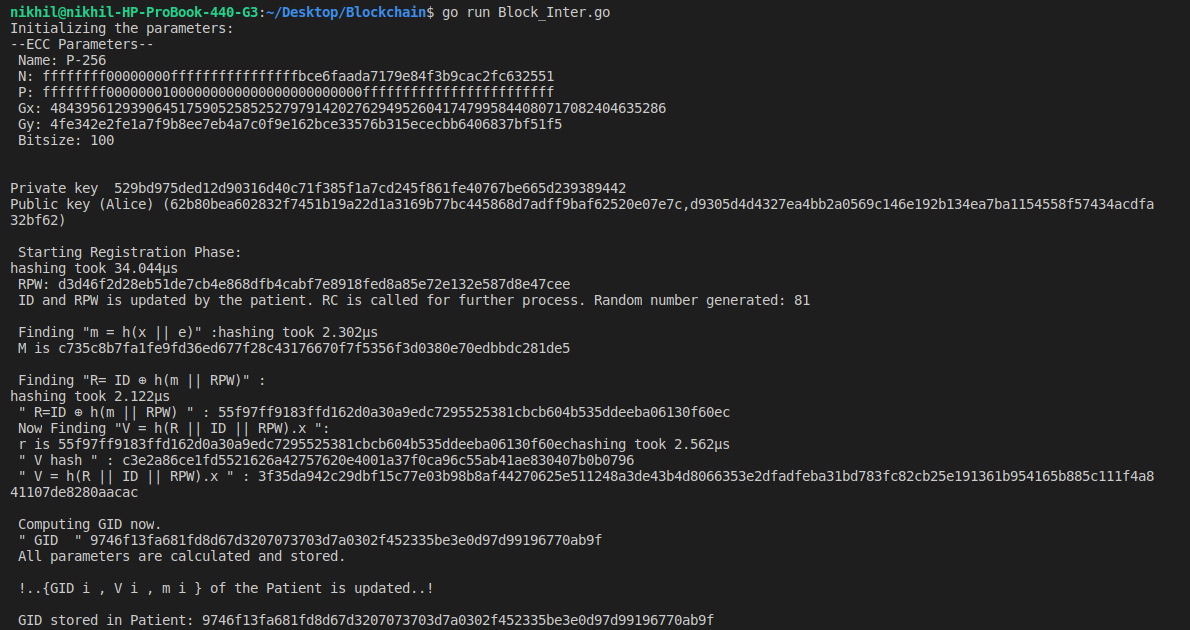
4.3 Implemententation of the three-way authentication algorithm

Firstly, For the implementation using elliptic curve, elliptic curve parameters had to be choosen. The elliptic curve has the form y2=x3+ax+b where a and b are defined parameters. A point on the curve is first picked and marked it has G- the generator points and we perform all the operations with in a finite set of field called as modulus of p. The final parameters are defined by *n-* the size of subgroup and *h-the cofactor.*  There are diiferent standards of elliptic curve which includes secp256k1, p192, p224, p256, and p384. All these standards are defined by parameters: (p,a,b,G,n,h)

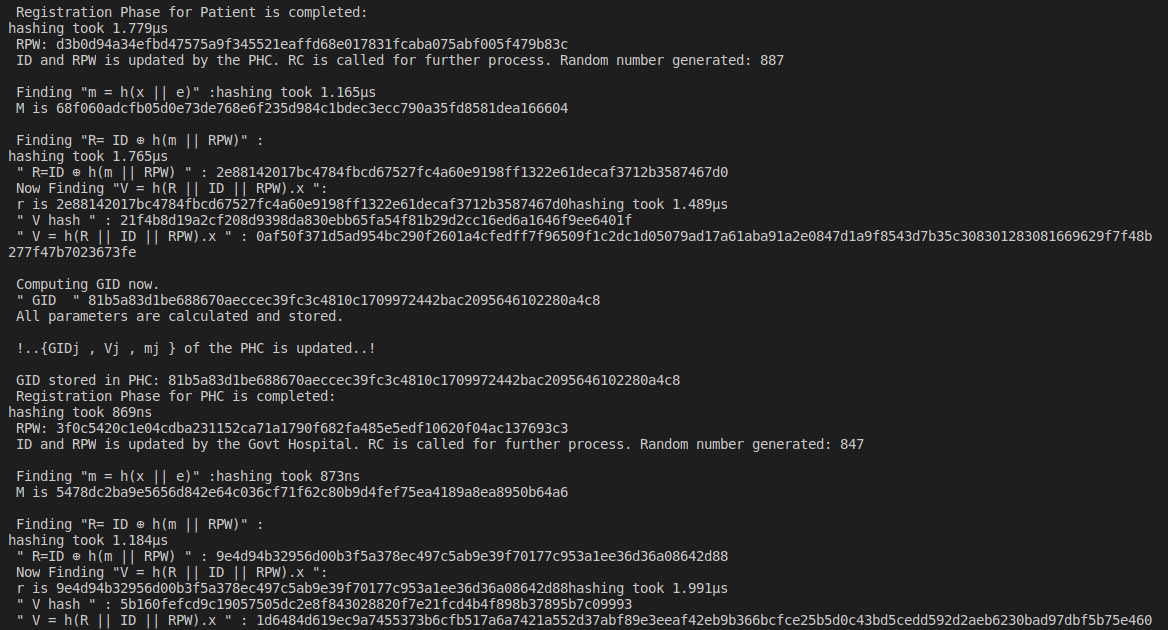


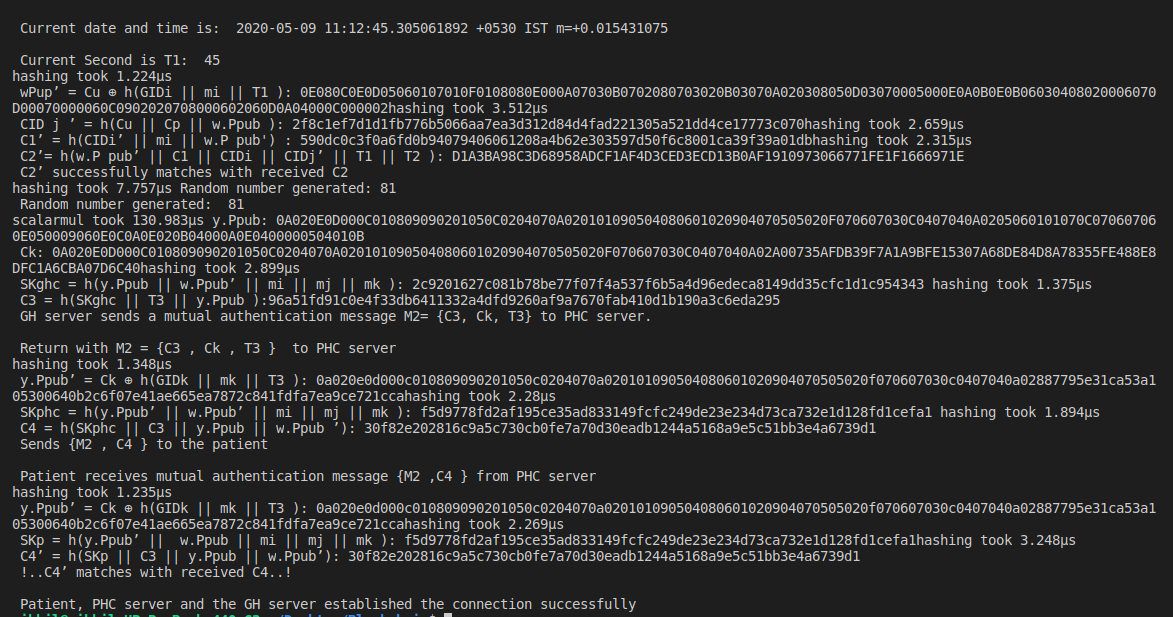
*Fig: Shows the general form of the elliptic curve.*

As described in section 3.2.1, first we define the elliptic curve parameters (p,a,b,G,n,h). After defining the parameters, we generate the private and public keys from the elliptic curve. After this generation, patient server initiates a login request by sending a login details and authentication parameters to the PHC server.

*Fig: Shows generated* elliptic curve parameters (p,a,b,G,n,h), public and private keys. It also shows the ECC operations performed by the patient and computing dynamic ID.

After the patient sends the login request message to the PHC server, PHC computes a set of mutual authentication parameters by using the set of parameters obtained from the patient login request. These parameters are obtained using ECC operations and are send the Govt.Hospital server. Government hospital calculates its own authentication parameters and send back the computed parameters to PHC. PHC uses this to recompute some of it’s parameters and sends it to the patient server. The patient server recomputes the authentication parameters obtained from the PHC server and check if the computed parameter is the same has it’s own calculated parameter. If those parameter matches, then the authentication is established between Patient, PHC and Government Hospital server. Further communication is done using the token which are generated during the computation.

*Fig: Shows the login request obtained from the patient server and is being proccessed by the PHC server.*

*Fig: Shows that the authentication parameter from patient server and the parameters obtained from the government hospital matches. This makes the authentication complete and a three way secure network is obtained.*

In order to calculate the efficiency of the code, timings of some major ECC operations like calculating hash, ECC scalar multiplication was calculated. These operations are the most time consuming operations. These timings are shown in Table 2.

|  |  |
| --- | --- |
| Table 2  Approximate time required for various operations | |
| Description (Time to compute) | Approximate computation (in seconds) |
| Hash Function | 8.051µs |
| ECC scalar multiplication | 100µs |

*4.3. Network simulation.*

Blockchain network is simulated to obtain the send rate, min max latency and throughput.

*For 10:*

*| Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| open | 100 | 0 | 49.9 | 2.32 | 1.36 | 1.92 | 25.6 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| query | 100 | 0 | 96.3 | 0.14 | 0.01 | 0.04 | 95.3 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| transfer | 50 | 50 | 50.4 | 2.51 | 1.29 | 1.88 | 12.3 |*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*for 5*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*| Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| open | 100 | 0 | 51.7 | 2.27 | 1.29 | 1.80 | 26.6 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| query | 100 | 0 | 102.2 | 0.14 | 0.01 | 0.04 | 99.4 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| transfer | 40 | 60 | 51.6 | 2.14 | 1.23 | 1.72 | 10.9 |*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*for 1*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*| Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| open | 100 | 0 | 50.7 | 2.18 | 1.21 | 1.69 | 26.1 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| query | 100 | 0 | 102.1 | 0.09 | 0.01 | 0.03 | 99.7 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| transfer | 36 | 64 | 50.1 | 1.82 | 1.27 | 1.59 | 10.4 |*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*for 15*

*| Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| open | 90 | 0 | 59.8 | 6.65 | 4.53 | 5.57 | 13.5 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| query | 90 | 0 | 95.8 | 0.53 | 0.01 | 0.23 | 94.6 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| transfer | 38 | 52 | 51.7 | 2.53 | 1.71 | 2.18 | 9.2 |*

*for 20*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*| Name | Succ | Fail | Send Rate (TPS) | Max Latency (s) | Min Latency (s) | Avg Latency (s) | Throughput (TPS) |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| open | 100 | 0 | 56.3 | 10.17 | 7.31 | 8.80 | 9.8 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| query | 100 | 0 | 98.6 | 0.16 | 0.01 | 0.07 | 93.0 |*

*|----------|------|------|-----------------|-----------------|-----------------|-----------------|------------------|*

*| transfer | 41 | 59 | 53.3 | 3.01 | 2.33 | 2.63 | 9.3 |*

*+----------+------+------+-----------------+-----------------+-----------------+-----------------+------------------+*

*4.2. User Interface*

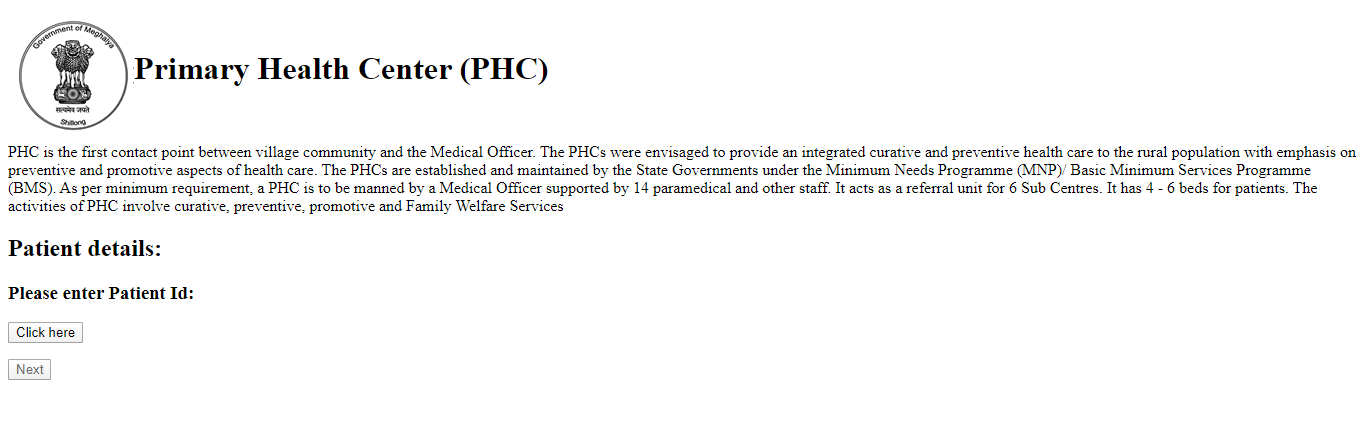
As a part of developing the user interface, some of the user interfaces have been developed. Fig 4.8 shows the user interface for the PHCs. In this page, the PHC has to enter the patient ID for the referral scheme. If the patient has to be referred to other government hospitals, PHC has to enter the patient ID, which results in displaying the patient details. After confirming the details, they select the govt. hospital to be referred to and submit the application.

Fig 4.8: User interface for the PHC.

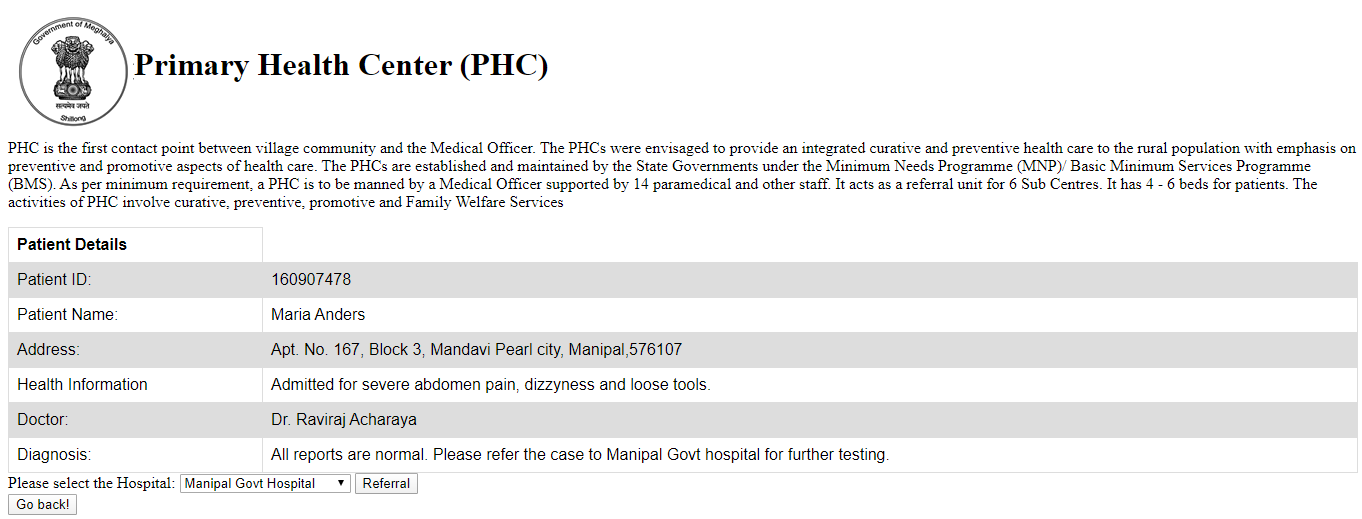


Fig 4.9: User interface for the referral application.

Similarly, the government hospital has its user interface, as shown in Fig 4.9. When they get the referral from other PHC, the govt hospital gets the option for viewing the patient details, accepting the patient and rejecting the patient. These user interfaces are currently static, but during the completion of the project, these will be dynamic and integrated with the blockchain network.

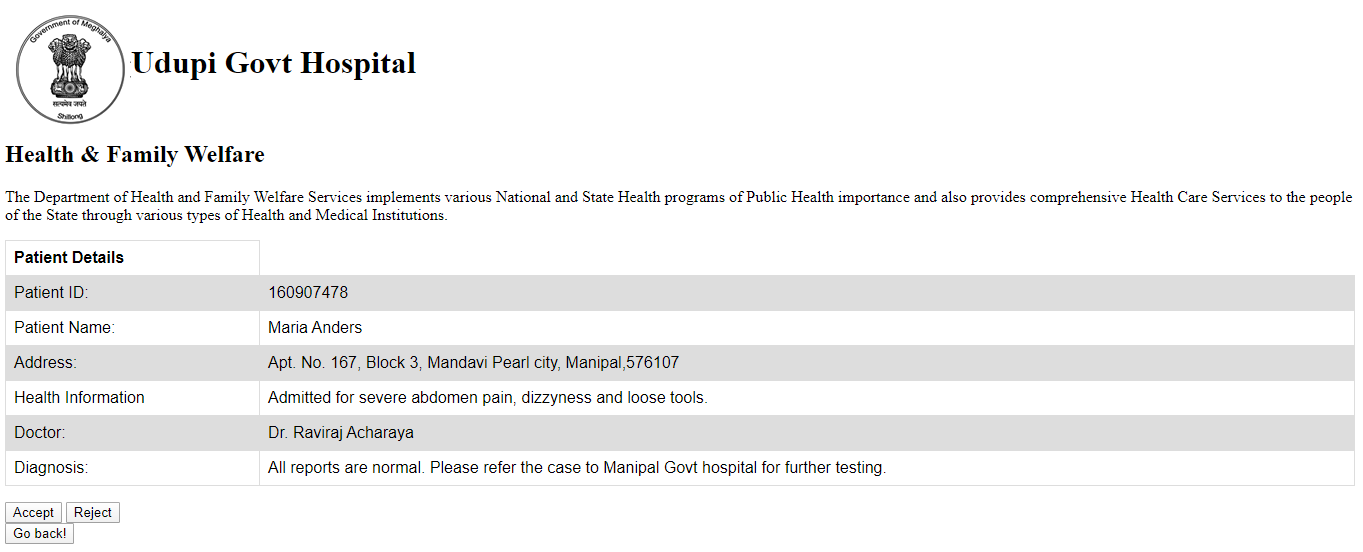


Fig 4.10. A user interface for the Govt. hospitals for accepting or rejecting the referred patient from the PHCs.

The result obtained for the network setup of the inner circle shows the working of the blockchain. The only things which are required to be added are another channel and three more organisations. The working of the above-simulated network is done using the default authentication system. This is a deviation since we have to implement our authentication system instead of the default. Since there are two use cases which required two types of authentication methods, as mentioned in the methodology section, only one use case has been simulated. Rest of the results will be completed by the end of the project.

**CHAPTER 5**

**CONCLUSION AND FUTURE SCOPE OF WORK**

*5.1 Conclusion*

In the era of Healthcare 4.0, privacy and security of health data have become important factors. Use of blockchain technology plays an important role in terms of security. This helps in reducing cybercrime, data theft, tampering of health data and makes the data immutable. In this project, we intend to make a patient-centric authentication scheme. Usually, the health data is not being owned by the patient; they are owned either by hospitals or big companies. By using blockchain, we give the ownership rights back to the patient. We are using hypeledger fabric for the development of the project. Security is achieved through immutable ledger technology. Using access control, we can make all the transaction patient-centric. This project shows the capabilities of blockchain technology in the healthcare and how it will revolutionise the health sector.

*5.2 Future Scope of Work.*

For future scope, we have to implement the transaction for the referral case. For example, considering a pregnancy, a woman will be going for antenatal visits, for the delivery as well as postnatal visits. In case the PHC does not have enough resources, it may refer the patient to a government hospital. This referral would be a transaction. In the second part of this scenario, the government hospital will either accept or not accept the referral within 15 days depending on the priority flag. In this level, no privacy policies are required considering the nature of transparency required here. For this use case we need to build an authentication scheme.

We also have to build an authentication scheme for direct communication between patient and other organizations like private or govt. hospitals. This will be done by the help of certificates.

Lastly, we need to measure the performance of the network. This will be done in order to compare our proposed authentication scheme. We will be comparing mainly four parameters: they are latency, throughput, load and response time. All of these metrics will compared with different network scenarios. All these will be done in the coming one and half months accordingly.

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  | |  |  |  |  | | --- | --- | --- | --- | |  | | | | |  |  | | | |  |  |  |  | |  |  |  |  | |  | | | | |  | | | | |  |  | | | |  |  |  |  | |  |  |  |  | |  |  | | | |  | | | | |  |  | | | |  |  | | | |  |  | | | |  |  | | | |  |  | | | |  | | | | |  |  | | | |  |  | | | |  |  | | | |  | | | | |  |  | | | |  |  | | | |  |  | | | |  |  | | | |  |  | | | |  | **References** | | | |