

# A Decentralized Blockchain-Based Model to Secure Confidential Medical Information

by

Tahmid Chowdhury

19201115

Tabassum Nusrat Jahan

19201027

Golam Rabbani Rifat

19201041

Sadman Sakib Nahid

19201029

A thesis submitted to the Department of Computer Science and Engineering  
in partial fulfillment of the requirements for the degree of  
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering  
School of Data and Sciences  
Brac University  
September 2023

© 2023. Brac University  
All rights reserved.

# Declaration

It is hereby declared that

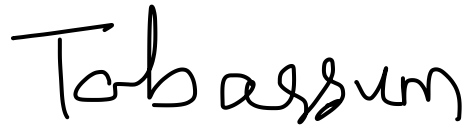
1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

## Student's Full Name & Signature:



---

Tahmid Chowdhury  
19201115



---

Tabassum Nusrat Jahan  
19201027



---

Golam Rabbani Rifat  
19201041



---

Sadman Sakib Nahid  
19201029

# Approval

The thesis/project titled “A Decentralized Blockchain-Based Model to Secure Confidential Medical Information” submitted by

1. Tahmid Chowdhury (19201115)
2. Tabassum Nusrat Jahan (19201027)
3. Golam Rabbani Rifat (19201041)
4. Sadman Sakib Nahid (19201029)

## Examining Committee:

Supervisor:  
(Member)



---

Dr. Muhammad Iqbal Hossain  
Associate Professor  
Department of Computer Science and Engineering  
Brac University

Program Coordinator:  
(Member)

---

Dr. Golam Rabiul Alam  
Professor  
Department of Computer Science and Engineering  
Brac University

Head of Department:  
(Chair)

---

Dr. Sadia Hamid Kazi  
Chairperson and Professor  
Department of Computer Science and Engineering  
Brac University

## Abstract

Nowadays in the current situation security in preserving data, keeping credentials is essential. Everytime a patient goes to a different healthcare institute that patient needs to go through checkup, most of the times same medical tests repetitively. Because of this inefficiency, the cost in the healthcare sector keeps increasing thus proper health care is not ensured for general people. Though in many healthcare institute a centralized data server(EHS) is used which is a problem because of single point of failure. In a centralized data storing system hacker can deploy cyber attack that's why a decentralized data storing system is needed. Though a decentralized data storing system is expensive comparing to centralized system it can provide security, privacy,transparency and interoperability. For deploying decentralized system blockchain can ensure privacy as well as data integrity because if any data is added to the block chain it would be immutable(can't be changed). In our proposed model medical records are encrypted and stored outside a blockchain and location of the records and other transaction information are stored in the blockchain where repetitive cost will be reduced and accountability among healthcare providers will be established.This thesis paper propose a blockchain based healthcare system where access of patient data is controlled effectively.

# Table of Contents

<b>Declaration</b>	<b>i</b>
<b>Approval</b>	<b>ii</b>
<b>Abstract</b>	<b>iii</b>
<b>Table of Contents</b>	<b>iv</b>
<b>1 Introduction</b>	<b>2</b>
1.1 Background . . . . .	2
1.2 Statement of Problem . . . . .	3
1.2.1 Data Security . . . . .	3
1.2.2 Privacy Protection . . . . .	3
1.2.3 Interoperability . . . . .	3
1.2.4 Scalability . . . . .	3
1.2.5 Cost-Efficiency . . . . .	4
1.3 Research Objectives . . . . .	4
1.4 Significance of the Study . . . . .	4
1.5 Limitations . . . . .	4
1.6 Thesis structure . . . . .	5
<b>2 Related Work</b>	<b>7</b>
2.1 Literature Review . . . . .	7
2.2 Characteristics of Blockchain . . . . .	24
2.2.1 Block Structure . . . . .	24
2.2.2 Consensus Mechanism . . . . .	25
2.2.3 Hashing Algorithm . . . . .	26
2.2.4 Distribution . . . . .	26
2.2.5 Accessibility . . . . .	26
<b>3 Threat Modeling &amp; Requirement Analysis</b>	<b>28</b>
3.1 Threat Modeling . . . . .	28
3.2 Requirement analysis . . . . .	28
<b>4 System Design</b>	<b>30</b>
4.1 Methodology . . . . .	30
4.2 Scenarios . . . . .	31
4.3 System Architecture . . . . .	33
4.3.1 Data Structure . . . . .	33

4.3.2	Mechanism . . . . .	35
<b>5</b>	<b>Implementation</b>	<b>38</b>
5.1	Window Navigation Diagram . . . . .	38
5.1.1	Full Procedure of Window Navigation Diagram . . . . .	38
5.2	Blockchain Account . . . . .	39
5.3	Smart Contract Description . . . . .	39
5.4	Medical Record . . . . .	42
5.5	Front End . . . . .	45
5.5.1	Patient . . . . .	45
5.5.2	Doctor . . . . .	46
<b>6</b>	<b>Discussion</b>	<b>48</b>
6.1	Validation of Model . . . . .	48
6.2	Hardware Cost . . . . .	48
6.3	Security Impact to secure Confidential Medical Information . . . . .	51
6.3.1	Data Integrity and Immutability . . . . .	51
6.3.2	Enhanced Security . . . . .	52
6.3.3	Consensus Mechanism . . . . .	52
6.3.4	Resistance to DDoS Attacks . . . . .	52
6.3.5	Interoperability and Data Sharing . . . . .	52
6.3.6	Data encryption . . . . .	52
6.3.7	Data privacy . . . . .	52
6.4	Comparison With Other Models . . . . .	53
<b>7</b>	<b>Conclusion</b>	<b>54</b>

# Chapter 1

## Introduction

### 1.1 Background

Medical data security is an essential part of the healthcare industry for protecting confidential healthcare information in personal health record data management, electronics health records data management, diagnostic laboratories, and pharmacy firms. For making patient data more secure and in relevant form we are using blockchain for monitoring patient record or EHR (electronic Health Record) in medical sector. We choose this factor because blockchain performs for security and transparency of sharing medical data in the healthcare system. In this thesis, we abstract a blockchain based model in healthcare system for sharing medical data purpose where blockchain performs as protector of data in healthcare and block specific threats. We are supposed to hope that using blockchain in healthcare can generate a new technology where patients can be treated as securely and easily. Any illegal activity, third party intermediary removed by blockchain. We are going to accomplish by using public blockchain in EHR or patient monitoring system in purpose of security of data and the transparency of records. We are going to use some features like: decentralization, immutability, security, privacy and transparency. This paper concludes the emerging and innovative technologies in the healthcare system by using blockchain.

We all have read about DNA and RNA from our childhood. We also know that DNA/ RNA inherit all kinds of information of a human characteristic. Generic information can be the most private and crucial things of a human being as it contains all kinds of information of disease, health situation, successively got diseases etc. This information must remain secure for the sake of securing a human. Additionally, other medical issues such as a patient's record of diseases, patents of medicines, formula to make medicines etc are also very important to remain secure.

Patient information is too sensitive and private for someone to ever want to divulge. Maintaining the confidentiality of sensitive data and providing appropriate security and protection measures should therefore be given the utmost priority. By enforcing data privacy regulations, several nations around the world oblige hospitals and healthcare providers to uphold all of this. Many nations have laws or acts specifically for healthcare data. Bangladesh doesn't even have a healthcare data law,

which should have been implemented long ago given the obvious necessity.

In recent times, securing medical data is a blessing. However, still there remain some security breaches in the medical system like leaking patients personal reports or leaking the data of the formula to make medicines. To solve this problem, implementing Blockchain in the medical system to secure data would be very beneficial. So let's first know, what is blockchain?

## **1.2 Statement of Problem**

In the modern healthcare environment, the growing use of digital technology has resulted in the production and storage of enormous volumes of private medical data, such as patient data, electronic health records, and diagnostic findings. These developments provide substantial hurdles in terms of data security and privacy, even though they have the potential to transform healthcare delivery and enhance patient outcomes. Traditional healthcare systems' existing centralized storage and handling of medical data is vulnerable to a number of security flaws, including data breaches, illegal access, and single points of failure. The integrity and accessibility of medical data, as well as patient confidentiality, are all seriously jeopardized by these flaws. Concerns about patient permission and data ownership are also raised by the opaqueness of the systems used to handle and share data. Accordingly, the primary issue addressed in this research is the need for a secure, decentralized blockchain-based system that can successfully shield private medical data from unwanted access, alteration, and data breaches. The system has to address the following major issues:

### **1.2.1 Data Security**

Create a strong system to guard against unwanted access and tampering while ensuring the confidentiality, availability, and integrity of medical data.

### **1.2.2 Privacy Protection**

Use privacy-preserving strategies to safeguard sensitive patient data, limiting access to only authorized parties and, when appropriate, safeguarding patient anonymity.

### **1.2.3 Interoperability**

To facilitate effective communication between different healthcare providers and organizations while protecting data security and consistency, interoperability standards should be established.

### **1.2.4 Scalability**

Create a blockchain-based solution that is able to process the enormous amount of real-time medical data that is created without sacrificing performance or transaction throughput.



### **1.2.5 Cost-Efficiency**

Determine whether the proposed decentralized system is economically feasible and whether it provides a cost-effective substitute for the current centralized healthcare data management solutions.

By addressing these issues and developing a decentralized blockchain-based system that provides improved security, privacy, and interoperability for private medical data, it may be possible to significantly alter healthcare procedures and increase patient and provider confidence.

## **1.3 Research Objectives**

This research aims to come up with a system that ensures security and privacy in the medical system while no other parties, just the related person with that objective will know about the full information.

- 1.To understand if Blockchain can provide privacy with proper security.
- 2.To experiment if people with less knowledge do not scam in the medical sector.
- 3.To test medical data do not leak or hack while securing using Blockchain.
- 4.To evaluate the proposed model

## **1.4 Significance of the Study**

The study shall offer a decentralized, immutable ledger system, which greatly increases its security by using blockchain technology. The risk of data breaches and unauthorized access is decreased by the encryption and distribution in the blockchain system.

The study shall introduce a system where patients have greater control over their health data and they can grant permission to healthcare providers and other authorized parties to access specific portions of their records, ensuring privacy and consent.

The study shall demonstrate a trust and accountability system within the healthcare ecosystem, as all transactions and activities recorded on the blockchain are transparent and auditable. This transparency can help mitigate fraud, improve accountability, and reduce errors and discrepancies in healthcare processes.

## **1.5 Limitations**

It can be said that Blockchain is a very new decentralized technology which is used to secure confidential information. The implementation of Blockchain is very rare in this world till now. If there is any popular implementation on blockchain that is present then that is some cryptocurrencies such as Bitcoin, Ethereum etc. In Fact the consensus mechanism of these two is different from each other. One uses

Proof of Work(PoW) and another one uses Proof of Stake(PoS). To talk about implementation of blockchain in the medical sector then it will be very rare. There are few companies who work to implement blockchain in the medical sector. Due to this it was very hard to collect the real data existing related to this work. Also we face PC storage for implementing the project. As storing patient's data in every private blockchain in each doctor's PC needs a lot of repository which is the most challenging part of this project. That's why this project needs a supercomputer with a lot of storage.

So, to solve this problem, we have read multiple research papers and online journals to know the existing technologies which have been used and come up with a new idea to secure confidential patients' medical information by using blockchain.

## **1.6 Thesis structure**

By this section we can get a quick glimpse of understanding about the whole thesis.

### **Chapter 1: Introduction**

Here we discuss the objectives and problems that occur in Bangladesh in terms of the medical health record and how we can develop the medical health record or EHR by using blockchain.

### **Chapter 2: Literature Review**

The theoretical concepts relevant to this study are discussed in this chapter. The evolution in this chapter, the theoretical concept discusses the evolution of blockchain in the medical sector from traditional to new concepts. The overall theory of blockchain used in medical health records and mechanisms previously used in EHR systems are discussed here.

### **Chapter 3: Threat Modeling & Requirement Analysis**

In these chapters, we investigate the threats which can attack our model and gave solutions.

### **Chapter 4: System Design**

In these chapters, we investigate the research objectives and try to give an idea and way to develop the model.

### **Chapter 5: Implementation**

Here we tried to implement some of the parts of our model.

### **Chapter 6: Discussion**

Here we discuss the problems in chapter 1 to the finding of the study and meaning information is drawn from the data presented in the results section.

## **Chapter 7: Conclusion**

From the study, this chapter we summarize the whole thesis in together neatly and recapping the crucial part.

# Chapter 2

## Related Work

### 2.1 Literature Review

Bangladesh is on the way to using top technological instruments [1]. The nations around the world who have expertise in new technologies can tackle barriers and take advantage of any opportunity. Blockchain technology is among those technologies which can bring a new era of security systems around the world. In fact the developed countries have already started to research about solving security problems with the help of Blockchain. In this paper there is also a discussion, the Public and Private Blockchain which is, anyone can contribute to a public blockchain by creating and validating blocks and participating in the network. Nobody in this room has access to the network. As a result, all parties continue to have access to, and transparency over, the transactions and the corresponding data. Since control is evenly distributed within the network, no single person is able to modify the data.

On the other hand, only approved and trusted entities are permitted to participate in system operations on a private blockchain, which can be restrictive in that regard. In this way, Private blockchain can give the guarantee of security. This paper also talked about Smart Contract where people can save their transactional information, their property information etc. There is also a road map in this article which talks about where and in which domains blockchain can be implemented. Among these there is Health and Application domain.

There is lots of data including personal information saved in medical reports [2]. This paper suggests to use attribute based access control and Hyperledger Fabric based storage together for the solution of healthcare information security. This solution can be near to Smart Contract. Now various technological sectors are using blockchain technology such as smart cities, finance, education etc. The ABAC model for access control is also established at this time to guarantee that users may access them effectively and safely. Additionally, due to the volume and complexity of medical data, we combined the interstellar file system with blockchain which is Interplanetary file System(IPFS) which has a better resource network than HTTP to achieve blockchain slimming and further enhance user access efficiency. This helped to relieve some of the storage burden on the system. There is also a talk about PKI public keys by which people will authenticate themselves. Moreover, this paper also gave information about Attribute based access control model which can be useful for adding, updating and deleting.

The paper has talked about Ring signature which is basically a privacy protection scheme or method which is used to remain anonymous [3]. Blockchain is a distributed ledger system that uses cryptographic algorithms and calculations. Now-a-days the privacy of a user seriously gets threatened by using a public blockchain ledger. To solve the problem, The Ring signature algorithm comes to give anonymity to a person. In fact in case of vote or take review this Ring technology techniques is very helpful. While using public blockchain the other users in contract can see the location through IP address or can get a lot of information which is already causing several problems around the world. In this case Ring signature can help to remain anonymous in case of sensitive issues. Mainly, Ring signature uses lots of encryption which builds anonymity. Ring signature technology was introduced by Rivest et al by using Ring signature algorithm. In this technology there is a ring signature system, where the user uses a combination of random integers, various technologies and the public keys of several group members while completing the signature process. The verifier of signature can not identify the user of that signature. But in this way they can confirm that the user is among the signature set or not. As I said before, it is very efficient to use electronic currency, voting in elections, reviewing and complaint recording.

Blockchain introduces open and transparent transactions as well as data privacy leaks because it is a public and visible record ledger. To maintain the user's complete anonymity and defend their right to privacy, this approach uses a ring signature transaction signing scheme. This study suggests privacy protection in blockchain by applying ring signature . The authors also wrote about blind signature technology which is also a technology that can save privacy of a user and in this technology, there remains the connection between input address and output address hide.

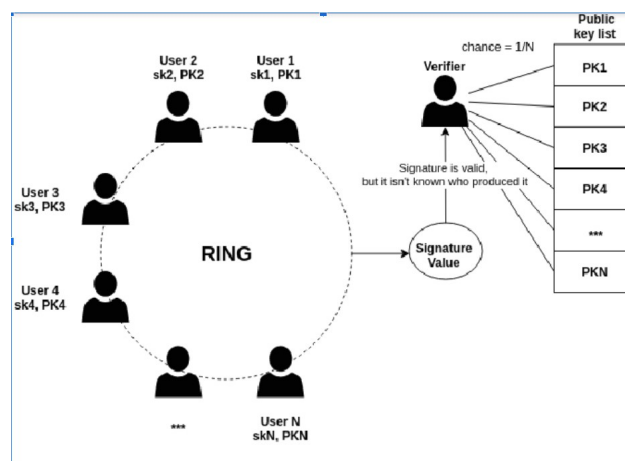


Figure 2.1: Ring Signature

It describes the concept of smart contracts which is blockchain based where they discuss applicability in Internet of Medical Things(IoMT) in the healthcare domain [4].For developing e-healthcare using blockchain they used Etheriuma popular for

creating distributed blockchain that supports smart contracts. Ether(ETH) is the native cryptocurrency of the platform. Smart contracts are simply programs that run when previous conditions are met and this is an agreement between peers. Smart contracts remove the need of a third party intermediary. With no intermediary's involvement or time loss are executed of associate agreement in order that all participants will be in real time sure of the result.

This study analyzes the financial sector through the eyes of using blockchain, its usefulness, merits, demerits, causes of recommendation which may lead to the effectiveness while using the blockchain in the medical line of Bangladesh [5]. Describing blockchain in a word that blockchain is a digital ledger of transactions which is distributed in computer systems. In blockchain the transaction is contained by block and each block contains information about the transaction. Furthermore, the client's ledger recorded the arrival of a new transaction. Blockchain uses distributed ledger technology(DLT). To hack the blockchain system the hacker needs to hack every single block in the system. The blockchain distributed system has three parts in total. And they are - Data, Hash and hash of its consecutive block. In this technology, the record for every transaction is kept in an immutable cryptographic signature which is the hash.

But the main drawback of using blockchain technology is that it is not that user friendly as most of the currently used technology. Interfaces for blockchain ledges are difficult to adopt. There must be a solution for handling a large number of users if we use blockchain technology. The transaction rate of Blockchain is less than the other exciting technique. For example the transaction rate of Blockchain is much lower than the VISA. Blockchain-based businesses or Medical system is very convenient for a developing country like Bangladesh, as it decreases the rate of corruption in many sectors.

The Paper discusses EHR (Electronic Health Record) and according to the International Organization of Standardization, electronic health records store the patient information in a very digital format, and also the information area unit changed firmly and solely accessible by approved authority [6]. It contains personal information about a patient. Its main purpose is to provide effective service towards a patient. Multiple types of EHR system situated in blockchain. Like: a) Gem Health Network: Data sharing through Gem health network is implemented for ensuring atmosphere while transferring user's data to deduct massive drawbacks. To construct centralization of information by decentralizing the information is its main purpose. Its framework totally supports decentralization. The feature of Gem network is each record under this network would be clear and any alterations with the record are mirrored to any or all the users of this network. b) Medrec: For using authentication, sharing, information confidentiality by using decentralization method below this network. By using smart contracts and decentralized methods this system is developed. c) Health Bank This platform firmly manages health data and also stores those data. This can be a replacement start-up that additionally provides some in-

centives to patients for his or her contribution. d) OmniPHR: PHR (public health record) provides the service, where patients can access their data. This module is developed for updating the data/record and to differentiate between EHR and PHR.

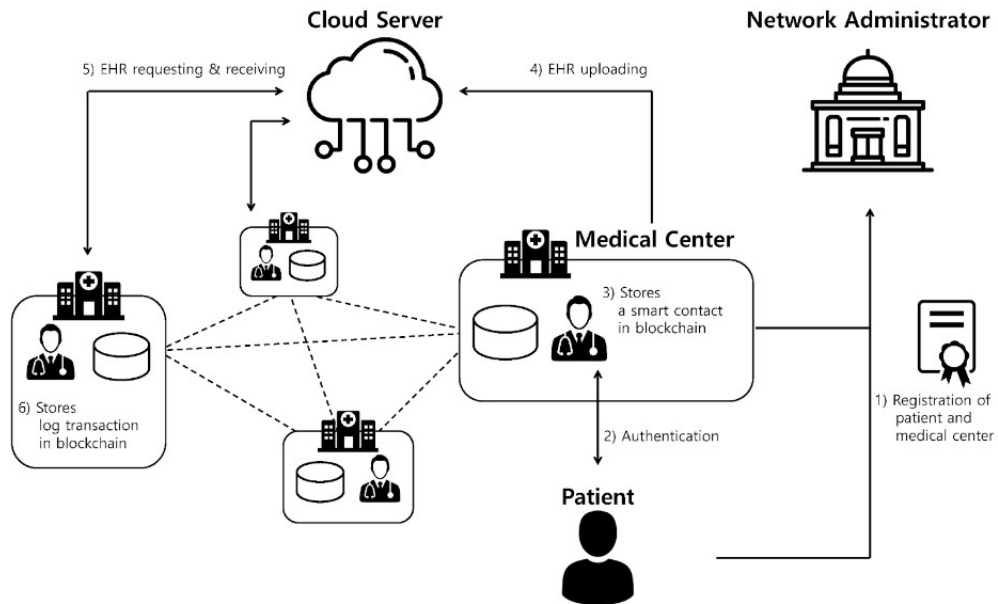


Figure 2.2: Electronic HealthCare Monitoring System

In this paper, they describe a peculiar feature of blockchain which makes a unique and powerful system for ensuring security, reliability in an IoT-inspired network for healthcare [7]. Some special features of blockchain are decentralization, transparency, immutability, and anonymity. Some of the key features of Blockchain are: Public Distributed Ledger, Hashing Encryption, Mining, Decentralization, Immutable, Consensus Protocol, Anonymity, Currency Properties etc.

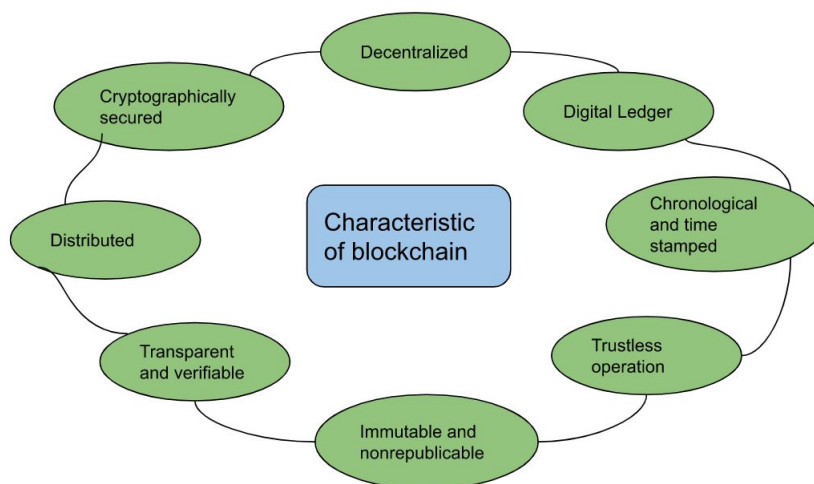


Figure 2.3: characteristics of Blockchain

In the medical health care system there can be a reputation system where patients can provide reviews of the doctors they know anonymously using blockchain technology [8]. But also the reputation of the patients who will give review on doctors will be provided by each other for calculating the truthfulness of their review. In reputation systems there are many category privacy preserving reputation systems are one of the most important category for cases where patient privacy needs to be preserved. This system mostly depends on cryptographic building blocks including secret sharing, zero-knowledge proofs, Secure Multi-Party Computation (SMPC), homomorphic encryption, zero-knowledge proofs, cryptographic signatures etc.

Blockchain can be used to secure land registry, medical securing data, bank based data, voting systems etc by using ethereum and smart contracts [9]. Ethereum is the most usable process to implement any idea for blockchain. In the blockchain, to make each block unique, hash value is calculated and the hash value also linked up with the previous block. Moreover, the SHA256 algorithm and proof of work (PoW) algorithm is used to calculate hash. These algorithms also help to make secure information with transactions. In the various cases, as usual we faced many fraud issues like criminal disturbance, data missing, false land, registry information missing, theft in digital domain etc. If this whole process will continue by a blockchain this process is easier and also will be a more secure process. It is easier to implement data transactions such as property information, property location, transaction information details etc by blockchain implementation. Moreover each block contains land transactions which cannot be matched with another transaction. Smart contract is also used for anonymous transactions. For anonymous transactions, ring algorithm, hybrid algorithm and DNA algorithm can be used in various ways. Authentication issues of blockchain continue by the public key cryptographic methods. A pair of public private keys, an Elliptic cryptographic curve algorithm is used to make the signature of each block. By using private keys the combination of cryptography and blockchain methods make a more secure process. Computing the Merkle root hash is done by aggregating transactions from a single entity onto the root entity, so the root contains the hash of the entire blockchain.

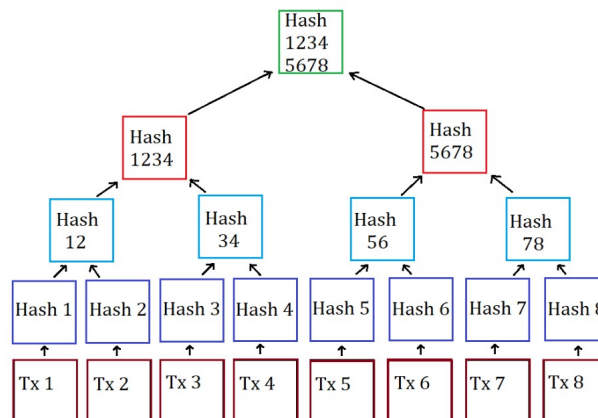


Figure 2.4: Markle Tree



a total 5 algorithms are implemented for land registry by blockchain. First of all, Transmission and division of land is done by the sender signing the land and using the Edwards curve digital signature algorithm transmitting it in whole blocks Public keys are distributed throughout the network to ensure that transactions are self-signed by their owners, ensuring their authenticity. To split the country, the availability of the affected user's property is checked. If available, a new block of transactions is created based on PoW by subtracting the required country from the old country variable. PoW implemented in the land registration process which is shown in the second algorithm. It shows until a certain condition is met take a block and calculate its hash. The proposed condition here is that the hash will start when it has three zeros. based on difficulty PoW tries to solve conditions. A random value called a nonce value that changes each time. The algorithm checks if the hash value of the block matches with the difficulty. Otherwise, the nonce value changes or increments everytime by which the hash value keeps changing and tries to match with the difficulty. .The third algorithm shown involves addition of peers and publishing communication. The network is trying to connect to an instance on a specific port. If the connection is true, it will be added to the peer list. Otherwise, incorrect connections will be reported. To process messages, her two other algorithms are designed, each block receiving a copy of the latest chain. Since the messages are sent across the network, attackers cannot penetrate your system. All transactions are hash protected and encrypted using the SHA256 algorithm. Using this algorithm, a hash value is calculated for each block and these values are used to concatenate the blocks to create a list of blocks as a chain.

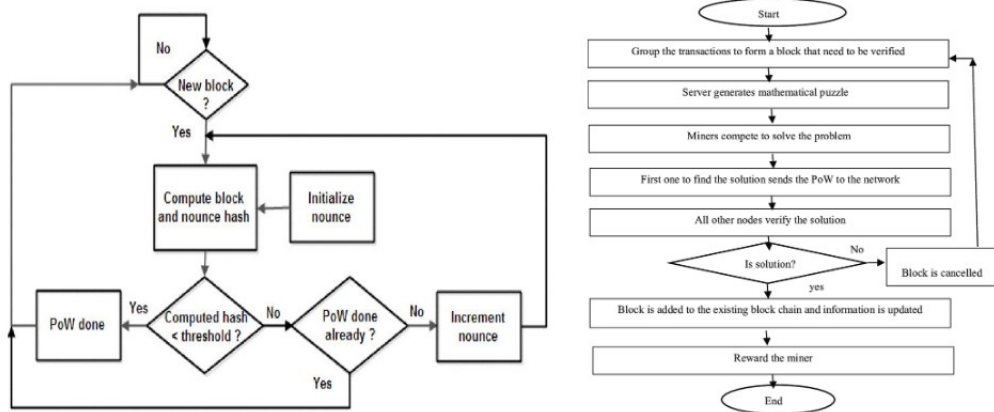


Fig: PoW Algorithm

Figure 2.5: PoW Algorithm

Now in the modern world e commerce has been playing a very important role in the modern economy [10]. Because of that, the supply chain is planning to apply blockchain for the secure connection among suppliers, manufacturers, dealers etc. Because by implementing blockchain the transaction can remain transparent. By using blockchain peers can trust each other. Among many consensus mechanisms PBFT(Practical Byzantine Fault Tolerance) is one of the most effective. Among PBFT, C-PBFT is more useful.

In the supply chain fast transactions are required. To reduce the delay and latency in transaction C-PBFT is very effective to bring the consensus. In this article, C-PBFT has been used instead of PBFT. There are so many benefits in using C-PBFT. In C-PBFT peers have been divided into 4 channels. Assume, there are 16 selector, so these 16 selectors have been divided into 4 channels and groups and due to this reason the consensus becomes fast to reach a valid block. The use of C-PBFT can reduce the delay and latency in block finalization and also this can bring comfortness in transactions in the supply chain.

If we start with a close to real world example where in a hospital a doctor has a couple of patients who need immediate treatment [11], [12]. Those patients arrive with various symptoms for example headache, stomach pain, chest pain, gallbladder problem and they need to be examined and need a couple of tests from the medical staff before being assessed by the doctor. One of the patient have mentions that the person received treatment from another clinic couple of days ago where that patient also undergo some tests and the doctor suggested him/her to another doctor for another reason. Now the clinician has to obtain EHRs(Electronic Healthcare Record) of those previous record from previous clinic and that recommended doctor which will be then provided to that clinic doctor. Therefore the clinician has to access all those EHRs via a middle party health care record to get the patient's record . By obtaining the previous information the doctor get a better picture of the patient's problem. So we can see that the doctor would never get those medical records and make proper assessment on patient problems unless that patient didn't inform about the previous healthcare visits. Besides the data being non authentic there is another problem which is if this procedure is taken, then to obtain all the information several days will be needed which may be something's incomplete and complex. Elsewhere the patients may also have unknown clinical healthcare data. That's why if there is a blockchain system where patients data are stored then any doctor and healthcare institute can access the patient's previous medical healthcare files. In blockchain system all of the information are available and they thus the new doctors can understand the health problem better and his overall health condition, previous illness, test results and given treatments which will reduce duplication, unnecessary new tests; this would result in cost and time reduction, increase efficiency. From the above abilities we can understand that blockchain is the key to reduce cost in healthcare and increase efficiency . If blockchain is launched then for patient's data entry, data management a certain procedure would have to be maintained thus all healthcare institute would maintain same format and understanding of retrieving data would be easier for healthcare providers(doctors). Blockchain will also ensure the security of data in it's own automated database. Furthermore, all the transactions(prescriptions

/patient data) would be transparent to the patients and patients can communicate easily. Blockchain stores and shares data in a distributed, immutable and trusted manner, not requiring a centralized dependency for checking transactions by removing intermediaries.

Blockchain can be included in the healthcare system which can be divided into four stages [13]. In first stage, healthcare providers will be directly connected to the network to the blockchain and in the existing health IT systems where all the data is stored. Via API and using Patient IDs patients various data is integrated to the blockchain network. All the inward transactions are executed by a smart contract also known as chain code where various rules are written in code format which executed after a condition is satisfied. All transactions excluding personal information of the patients are added to the blockchain via transactions using patient public IDs and all this data are immutable and connected with each other. These transactions are unique so that it can be identified easily. The health providers begin reverse mining or query processing via the APIs. Patient's personal information is not included in the database of blockchain so identity is secure. Finally if the patient wants to share their data they just have to share their private key to the healthcare provider. This is how the provider can then access the patient's data and take care of the health issue. Obviously, the data remains confidential to those who do not have the private key of the patient.

The current healthcare system is facing various kinds of difficulties in expenses, heavy regulation of quality treatment etc [14]. Electronic Medical Record (EMR) and Medical Health Record (MHR) are highly secret data in terms of a patient. No one wants to disclose to an unauthorized person what is happening to a patient. This study focuses on four key stakeholders and those are patient, cured patient, doctor and insurance company in a healthcare sector and applying a consensus algorithm Proof of Familiarity (POF). They have claimed that stakeholders will create a transparent medical decision which will create interoperability.

This paper indicates overall sharing information of Doctor's record, feedback of a cured patient, policy of insurance company and the decision making of the blockchain. The scheme stores medical decisions in blockchain and increases confidentiality.

To talk about their block architecture, they will give the hash of the previous block including the timestamp. They will store the patients' clinical history, doctor's decision, insurance company policy history and hash to cross check the originality in blocks. Also, the decision will be generated.

In their implementation and discussion part, they claimed that they are using multichain which is an open source blockchain implementation platform which will act as a prototype for accessing the POF consensus algorithm. The hardware is Windows 8 computers with intel i7-6700, 3.40 Ghz with 8 GB RAM which represents the particular entity.

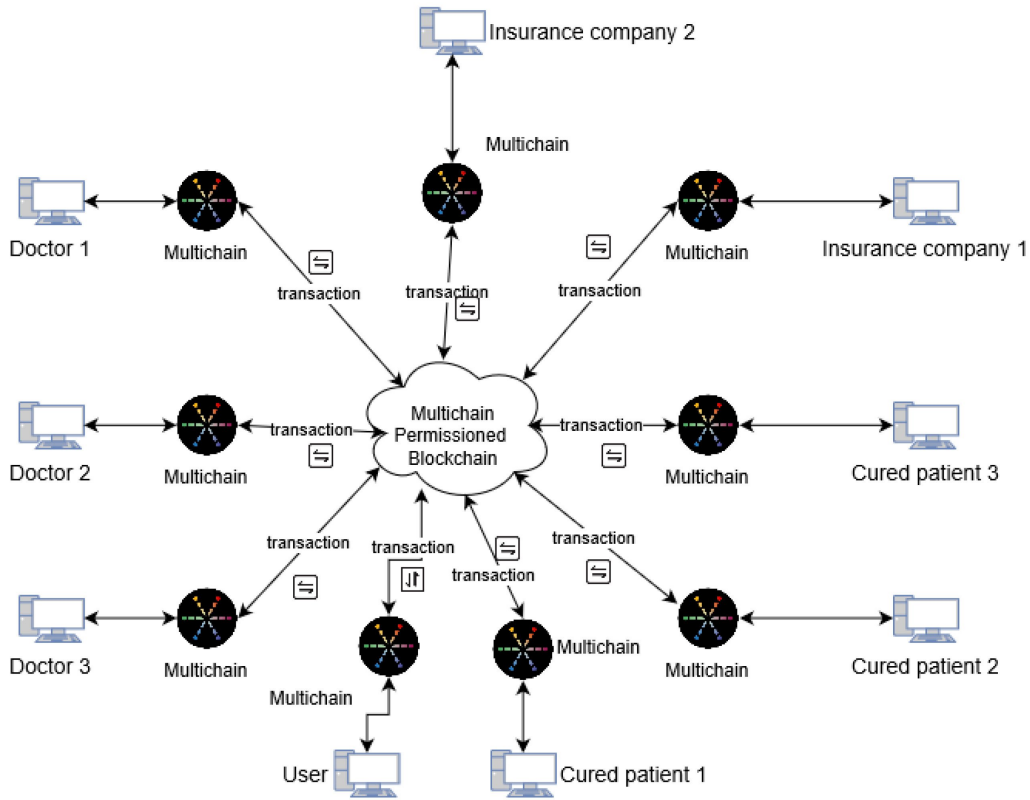


Figure 2.6: System design of POF communication environment in the Multichain

After designing all of the structures and applying POF the Journal is claiming that it has no single point of failure, it has smaller block size, proper security, effective cost, lesser time, scalability etc.

A time-dependent searchable encryption system known as Re-dtPECK combines a concurrent keyword search with a chosen tester and a timed enabled proxy re-encryption function [15]. Patients might have the option to provide limited access rights to third parties, enabling them to go over their files for a set amount of time. It is possible to set a time restriction for how long the delegate must search for and unlock the delegator's encrypted documents. The delegate's access and search privileges may also be automatically terminated after a predetermined amount of time. Additionally, it allows conjunctive keyword searches and offers defense against keyword guessing (KG) assaults. The solution allows the chosen tester to verify specific keywords' existence. They give a system model and a security model for the suggested Re-dtPECK methodology to demonstrate that it is a practical approach that has been proven secure in the reference model. The comparison and in-depth simulations show how little overhead there is in terms of computing and storage. They offer a cutting-edge encryption method that permits secure conjunctive keyword search and authorized delegation functionality. This approach is superior to existing systems in that it can accomplish time-enabled proxy re-encryption with

efficient delegation revocation. Delegation timing has been established, and owner enforcement is in effect. Each delegate may have a distinct access time period configured for them. formally demonstrated defense against the suggested-keyword suggested-time assault of the suggested method. It is also possible to halt attacks made using offline keyword guessing tools. The test algorithm requires the private key of the data server. The test algorithm prevented listeners from making keyword speculations. Instead of using the random oracle notion, the method's security is based on the conventional model. This first primitive also performs the aforementioned functions and incorporates the usual model

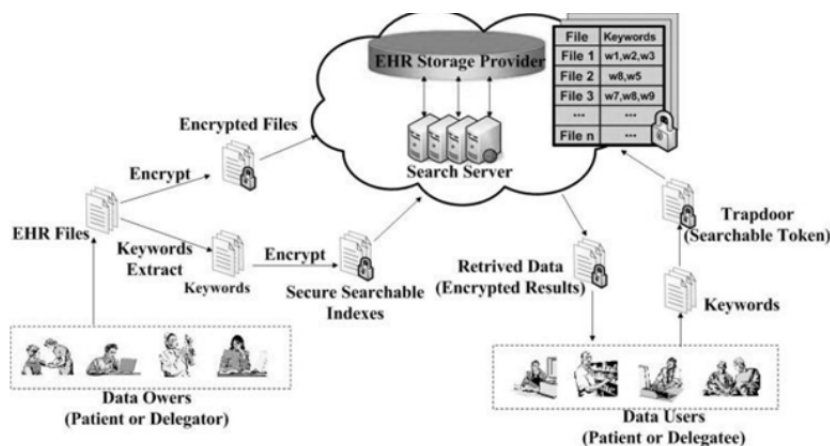


Figure 2.7: Timing Enabled Proxy Re-encryption Searchable Encryption Model

The transmission of medical data beyond the safe network of institutions poses a major danger to patient privacy since security issues may cause individuals to omit specific details about their ailment [16]. This situation is detrimental to the patient, scientific research, and all parties involved. To solve this problem, they suggest a blockchain-based data sharing architecture that takes advantage of the immutability and intrinsic autonomy of the blockchain. This effectively solves the access control problems associated with sensitive data stored on the cloud. Their platform is based on a permissioned blockchain, to which only verified users are invited and who can thereafter access it. Because all users are already identified and the blockchain keeps track of their activity, this strategy ensures even more accountability. Once the system has verified the users' identities and cryptographic keys, they are able to request data from the shared pool. The findings of the system evaluation back up the claim that our strategy is straightforward, flexible, and efficient.

In the article, they provide a scalable, secure access control solution. They successfully regulate access to private shared data pools using encryption and digital signatures, and they use a permissioned blockchain for added protection. They create a blockchain-based data sharing system that enables users and data owners to

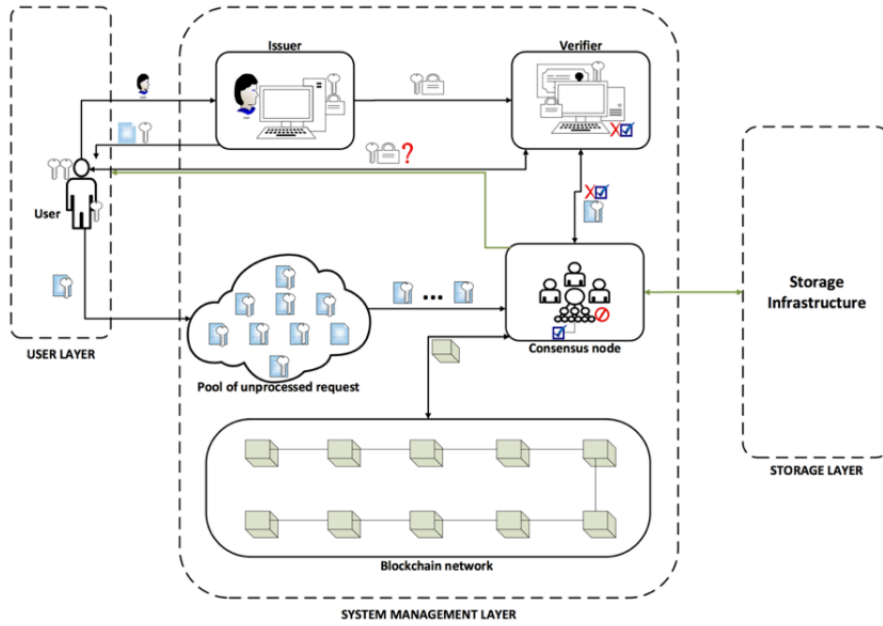


Figure 2.8: BBDS(blockchain based data sharing) system architecture

access electronic medical records from a central repository after their identities and cryptographic keys have been confirmed. The requests are added to a closed, permissioned blockchain after they have been verified and further processed. Where traditional access control techniques like firewalls, passwords, and intrusion detection systems fall short, our approach succeeds.

Inadequate behavior on these records significantly harms the reputation, wealth, and other assets of all parties associated directly or indirectly with the data, which raises a number of privacy problems for patients whose medical information are released [17]. The inadequacy of current approaches for maintaining and preserving medical records is well established. The technology MeDShare is explained in this article as a solution to the problem of medical big data custodians communicating medical data in a risky setting. The blockchain-based solution in cloud repositories offers data provenance, auditing, and control for massive data entities that interchange medical data. MeDShare monitors organizations who use a data custodian system to access data for illegal purposes. All operations performed on the MeDShare system, including data exchange and entity migrations, are recorded in a tamper-proof log by MeDShare. Smart contracts and an access control system are used in the design to efficiently track data activities and deny access to entities who violate data permissions. MeDShare can exchange data between cloud service providers as efficiently as the most recent cutting-edge technology. MeDShare allows cloud service providers and other data guardians to securely share medical data with organizations like hospitals and research centers while establishing data provenance and audits

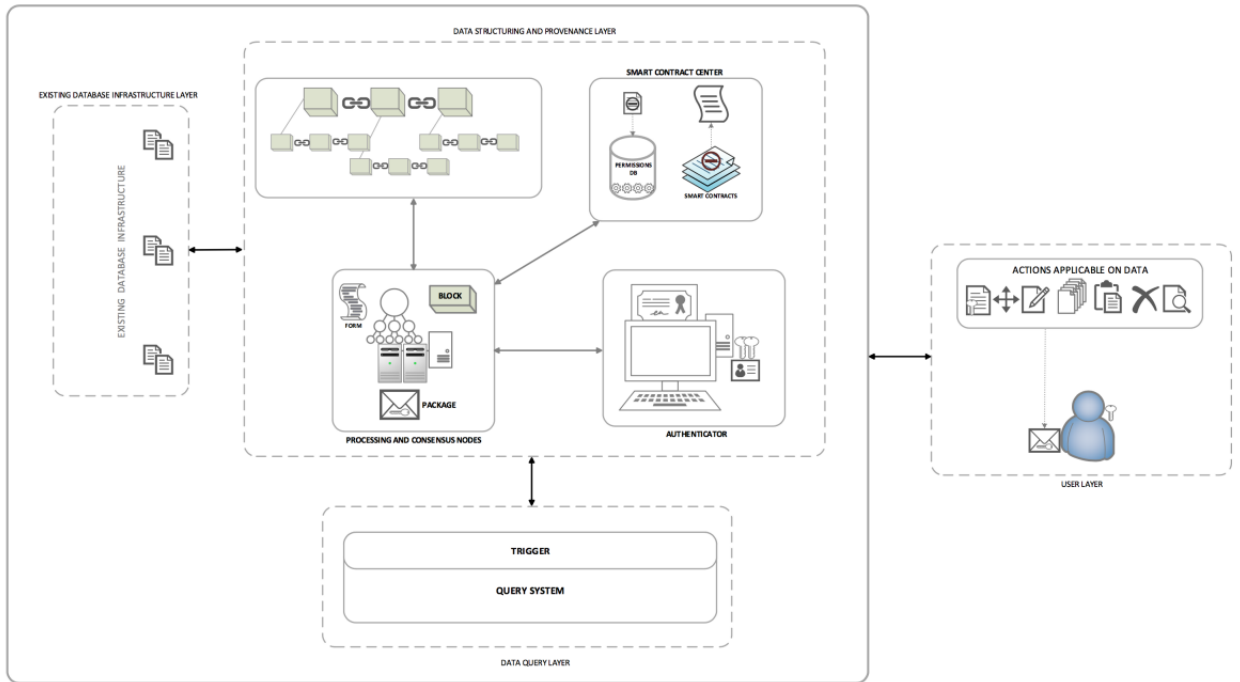


Figure 2.9: MeDShare: Trust-Less Medical Data Sharing System

Patient medical data are very crucial in terms of health [18]. The world needs a kind of security in the medical sector where the report will remain secure and immutable. If any changes happen that can be caught by applying some security methods. Blockchain here brings these changes to the world in the case of the medical sector. Blockchain brings a hash chain with decentralization, verifiability and immutability.

Those who visited hospitals know that medical data online is so vulnerable that it can be leaked at any time. In October, 2017, approximately 47 GB of medical data was opened in public from the Amazon database.

This article works with three types of transaction actors and those are Medical institutions, patients and insurance companies. Medical institutions are going to diagnose and generate medical reports of patients from different hospitals. Third parties such as insurance companies can provide some services. Due to storage and transaction speed problems only index information of medical data will be stored in blockchain and large medical data should be stored in the cloud storage which will remain under the chain. The patient can also withdraw the permission any time.

To talk about the read/ write access of medical data the patient, medical institution and third party agencies all of them have the permission. The other medical data will not be read by the patients and the third party agencies but the medical institutions can do that in an emergency. To write in others medical data, none of them have that permission but in case if someone needs to give permission, they can do that.

When a patient visits a medical institution the doctor will generate a medical report,

hash the report and post them in the blockchain. After that the patient will check the signature and after encrypting using the private key the report will also be stored in the cloud storage. The sharing of the data will be fully controlled by the patient.

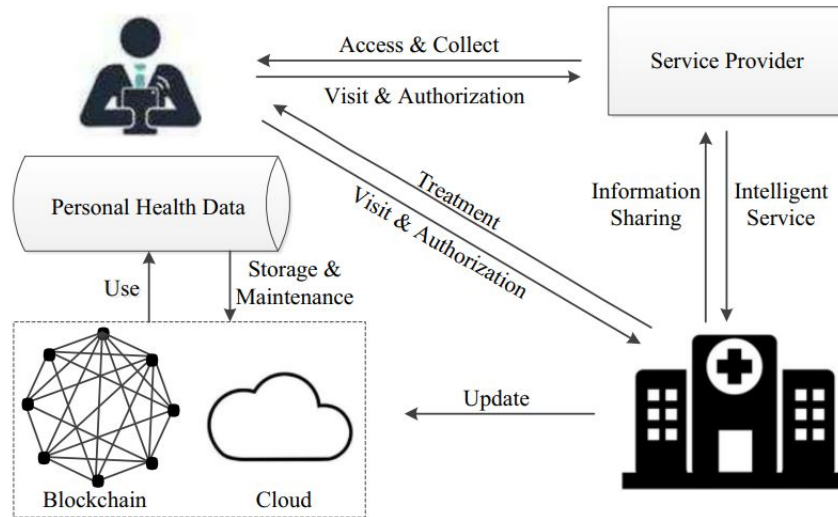


Figure 2.10: Framework of Blockchain technology in medical service

At last, this journal has claimed that it has no reliance on trusted third parties. It is Tamper resistance, privacy protected, has secured storage and has control over the medical records.

Electronic medical healthcare records are very sensitive information for the patients and that is why more secure, reliable and transparent technology which can be Blockchain. In this article [19] the authors have proposed a framework along with a consensus algorithm named mixed Byzantine Fault Tolerance Algorithm(MBFT) which is for medical information sharing also it will reduce blockchain forks along with increasing consensus speed and high fault tolerance.

The participants don't trust each other in the Consortium Blockchain so it is important to verify the block by most of the participants. In the structure of this system the patient will register from the user management. The medical record will be only seen by a doctor without requiring any kind of permission just for their own hospitals. The authorized management can get permissions from the patients to see the medical data. To check whether the information in a medical report has changed or not, the hash of the report in the hospital blockchain and the hash of the report in the hospital database can be compared to see if the data has been changed or not.



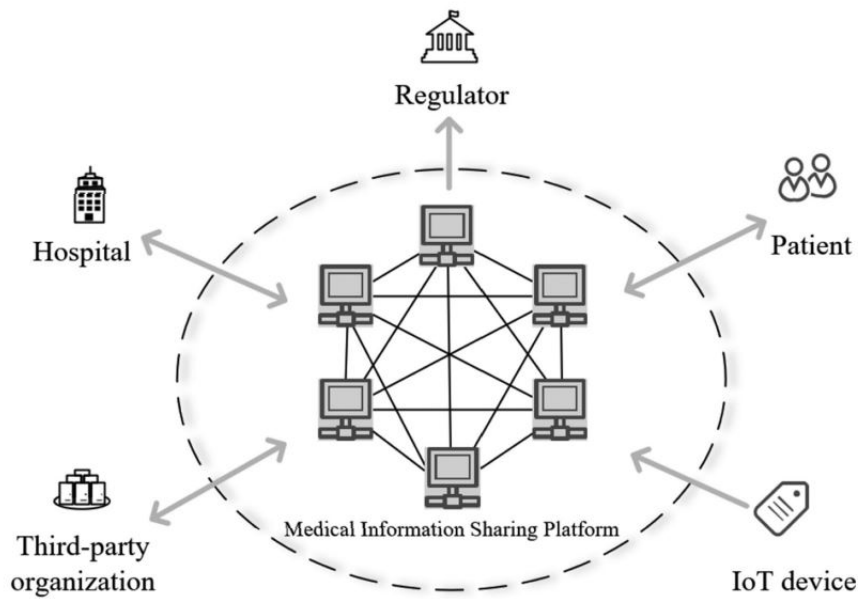


Figure 2.11: Structure of Consortium Blockchain

In this article, the healthcare industry is rebuilt by ensuring security and privacy by proposing blockchain technology. Blockchain technology has many types of uses [20]. Here the authors use a framework called Smart Healthcare System (SHS). By this framework all the medical entities can build a connection and also communicate with their own. SHS has several pillars which are Artificial Intelligence (AI), Internet of Things (IoT), cloud computing, Machine Learning (ML), Robotics, WAN and Big Data Analytics (BDA) etc.

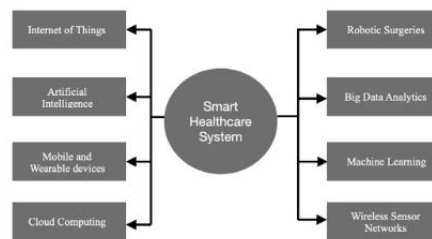


Figure 2.12: Pillars of Smart Healthcare System

To allow all entities (such as device monitoring, equipment of medicals, wearable devices etc) Internet of Things and wireless sensors used. It can connect to a network easily and also communicate with each other in a healthcare system. To monitor the patients conditions in real time the wearable devices work. All the volumes of data are stored in the cloud and it can be accessed or analyzed by using big data analytic techniques. By reviewing this data a doctor can easily diagnose the patients and the patient can easily show his previous diagnosis. The archived data can also be used in the ML and AI to train the dataset and further predict the diseases and

recommend possible treatments and prescriptions.

There are several barriers and challenges faced in this current Smart Healthcare system. The large volume of medical data can be hacked easily and makes it vulnerable. The hackers can easily take full control of the wearable devices and he or she can also misuse it which can be insecure of the system. The most common failure is system failure which makes the whole stored data and information inaccessible. Since the data is centralized it can easily lose data integrity and data flow. Also many types of virus attacks can happen in this system.

So the proposed framework is S2HS (Secured and Smart Healthcare System) which can achieve the success and overcome the challenges of the classical SHS. This is a secured healthcare system which is decentralized. By deploying blockchain technology this system works. The sensitive data and private data are captured in an encrypted manner where in SHS there is a centralized cloud storage. So that's why in this proposed model data will be immutable. The proposed system used WSN for connecting all the entities together. There are a total five prime entities in S2HS. Such as electronic Health Records/Clinical Data, wearable devices, Encryption or Decryption and Standardization, Blockchain Mechanism, end Users etc.

Doctors utilize IoT-based wearable devices for real-time monitoring of patient conditions. These devices, resembling wristbands and watches, are convenient to wear and incorporate miniature sensors. These sensors detect both environmental factors and vital signs in patients, including diabetes, pressure, heart bit rate, pulse rate, temperature rate, ECG, humidity etc. Prompt notifications are sent in real time to doctors and clinicians, reaching them via smart devices and SMS messages to the relevant healthcare professionals. By monitoring the patients continuously there is a huge amount of data created. These data are not always effective for the real time but it can provide some useful information after analyzing. All of these data are captured by the wearable devices and some of the monitoring units are saved in the cloud. But in S2HS the data is encrypted before being stored in the cloud. That's why data has always greater privacy and less chances to be hacked. Encryption/Decryption and Standardization are the most important and critical parts of the S2HS. All types of data and information are not measured in the same formats. Different data has different formats. So firstly all of the data is necessary to convert in the standard format. It can be helpful to apply the blockchain mechanism and put the data for encryption. Also Smart contracts will be developed and can easily be signed by the stakeholders easily. Transactional data stored in a storage block which remains unchangeable. It also ensures that only authorized users can access it. These systems make it easy for participating parties to access all types of data by using smart contracts. A standard blockchain can operate as a decentralized system of control and access, where every participant holds a stake, and there is no singular administrator. All individuals have equal rights and authority within this structure. End users means all types of employees and clients of the hospital such as doctors, nurses, patients, chemists, clinicians, pathologists etc. They will use this system along with smart devices or web browsing. In this proposed model there are two types of blockchain platform used. One is private blockchain and another is public blockchain. The private blockchain is used for the eternal entities of the healthcare ecosystem. Also to interact with external entities the public blockchain is used. This is how the two types of blockchain are used in this proposed model.

There was a scalability issue because here lots of data is unorganized in different formats So In the future, it should focus on enhancing the scalability of S2SH. Additionally, it's critical to build a universal standard for the blockchain technology in the healthcare system. The blockchain in healthcare also links to the creation of infrastructure and seamless connectivity to facilitate widespread adoption in future. Overcoming the significant obstacle of limited awareness among stakeholders is another key area that requires attention in the future.

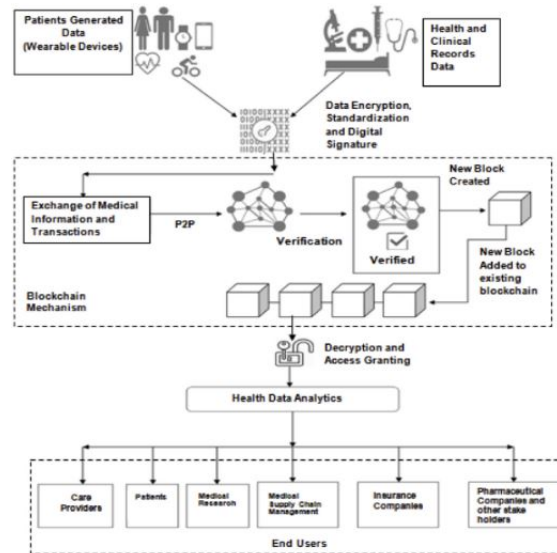


Figure 2.13: S2HS Blockchain Based Model

In this paper, the healthcare applications are widely used to track patients' health issues and patients medical details by using IOT devices with blockchain technology [21]. The complex biomedical sensors are used as IOT wearable devices to complete different tasks in healthcare technologies. Still there are some security and privacy issues that occur for securing patient monitoring data. There are several types of errors for example the cost of processing tasks, security issues, content scheduling etc. In this thesis paper the authors propose a new model to solve those above issues. Here is using a new algorithm framework which is called DRLBTS. It means deep reinforcement learning-aware blockchain-based task scheduling . It can ensure security issues and also can solve the current issues in the medical healthcare system. In the proposed systems, there are three types of nodes used for processing. These are mobile , fog and cloud nodes. Different types of tasks handled by different nodes. In the public blockchain, this system is also used to maintain all the dataflow for healthcare purposes. There is a partitioning and resource allocation which are structured for maintaining the resource balancing during workflow. Here also used the consensus mechanism proof of work for focusing the validation of data, security and distributed processing among all the nodes. There are also different types of algorithms to make this systems more efficient.

---

**Algorithm 1: DRLBTS Algorithm Framework**

---

```
Input :G,...,A
1 begin
2   foreach (G = 1 to A) do
3     Divided the workloads based on annotated;
4     mobile[v = 1 ← G];
5     fog[v = 1 ← G];
6     cloud[v = 1 ← G];
7     G = mobile + fog + cloud;
8     Optimize  $X \in X \in A$ ;
9     Call Scheduling;
10    Call Adaptive Scheme;
11    Call Blockchain PoW Scheme;
```

---

Figure 2.14: DRLBTS Algorithm Framework

---

**Algorithm 2: Initial Assignment of Workflows on Different Agents**

---

```
Input :G,...,A
1 begin
2   foreach (G = 1 to A) do
3     Schedule mobile[v = 1 ← G];
4     Call Algorithm 3;
5     Apply blockchain mechanism as shown in Figure 2;
6      $\pi \leftarrow X = \textit{mobile}[v = 1 \leftarrow G]$ ;
7     Schedule fog[v = 1 ← G];
8     Call Algorithm 3;
9     Apply blockchain mechanism as shown in Figure 2;
10     $\pi \leftarrow X = \textit{fog}[v = 1 \leftarrow G]$ ;
11    Schedule cloud[v = 1 ← G];
12    Call Algorithm 3;
13     $\pi \leftarrow X = \textit{cloud}[v = 1 \leftarrow G]$ ;
14    Apply blockchain mechanism as shown in Figure 2;
```

---

Figure 2.15: Workflows on Different Agents

These algorithms are used for different purposes like the first algorithm that means the the DRLBTS algorithm framework used to solve the task scheduling problem. It is computing on the different nodes for their work purpose. The second one demonstrates all types of nodes like mobile, fog, cloud etc. It must execute their tasks in their respective states with the efficient policy and objective in work. There are also some executions completed in this paper like mobile execution, fog execution and cloud execution which is discussed in another algorithm on Adaptive task scheduling and blockchain mechanism.

This model is a very potential model in the healthcare system but there are some limitations .The proposed DRLBTS model consumes too much energy while executing their computational works on different nodes. So as a future work it will be developed on the cost efficiency and low energy consumption. This model can handle all the situations like task failure, leakage and deadline but it does not support real time healthcare applications and sometimes it gives wrong information. That's why as a future work it is also included that its implementation should be more accurate about long running queries which can execute the requirements of the application with the medical runtime execution.

## 2.2 Characteristics of Blockchain

### 2.2.1 Block Structure

The blockchain technology stored informations by adding blocks which is so secure that it is almost impossible to hack or penetrate. In this system it is also impossible to cheat due to Cryptographic hash. Each block carries sevrsal transaction and another block also carries several transaction which remain connected through chain.

**Timestamp:** In blockchain, a timestamp is very crucial component which is used to record the exact time and date then a block or tracsaction is added to the blockchain. There are various types of timestamp. Among those two are:

1. Transaction Timestamp
2. Block Timestamp

**Merkle Root Tree:** A Merkle Root Tree is used to summarize all the transaction within a block also it is used to verify all the transaction.

**Hash:**Blockchain is a distribnuted technology where records are connected through blocks using immutable cryptographic signature known as hash. If one block om a chain was changed, it would be immediately apparent.

**Prev-Hash:** Reference of the hash of the Previous block.

**Nonce:** Nonce is a random whole number which is usually used by the miners for use as the hashing value of the block which must be a valid number.

**Data:** It can be referred as transaction which is stored in every block

## 2.2.2 Consensus Mechanism

The consensus mechanism of blockchain means a set of particular rules by which it is ensured that if a transaction is validated or not by the nodes. This is very important for the integrity of the blockchain. It eventually ensures agreement among all the nodes in a decentralized network where no node is bound to trust each other which can be solved by consensus mechanism. These nodes are responsible to find out the validity of a transaction. Now this validity is checked depending on how many nodes agree and disagree. If most of the nodes vote for in favor of the transaction then the transaction is valid otherwise the transaction is not valid. Now there are many procedures or consensus mechanisms for checking the validation of the transaction for example how many votes from the nodes need in favor of the transaction and how the voting will happen.

**Proof-of-Work:** Proof-of-work is a consensus mechanism where the validation of the transaction is done by the vote of the majority of the nodes which is similar to others. But the difference is who will propose the transaction. Here the nodes who participate on adding the blocks on the blockchain are called “miners” and the process is called “mining”. In mining the miner who can solve a complex puzzle gets to propose the block and then if it gets the most votes then gets added into the blockchain.

**Proof-of-Stake:** Same as proof-of-work the block is added in the blockchain if the block gets most of the votes in favor of it. But the node who can propose the block is different. Here the validator or creator of the block is chosen randomly based on the stake they have. If any validator node does unethical work then that node's stake is seized. For that reason this procedure is safe and more efficient because it demotivates the miners who will propose the block from any evil act.

**Proof-of-Authority:** It is a modified version of proof of stake where the validators or nodes are selected by the authority based on their reputation. This mechanism is mostly used in exclusive use where all the nodes are known and easy to select the right validators.

**PBFT:** PBFT is Practical Byzantine Fault Tolerance. PBFT is a consensus algorithm where clients send messages to everyone. Then the primary node sends pre-prepare messages to all replica nodes. Then replica nodes send  $2n+1$  prepare messages and after receiving  $2n+1$  prepare messages by everyone they send  $2n+1$  commit messages. After confirming  $2n+1$  commit messages the consensus works and information updates to the client.

**DPOS:** Delegate Proof of stake is another consensus algorithm. Here no fork can occur. Here 21 delegates have been selected to create blocks and after that 1 proposer is being selected among them to propose a block.. After proposing a block other 21 delegates have to vote to add that block into a blockchain.

### 2.2.3 Hashing Algorithm

Blockchain technology uses a hashing algorithm to process transactions and provide a fixed-length output. When a message is meant for a single receiver, hashing is one approach to ensure a safe transaction. A formula is used to construct the hash, enhancing the transmission's security against manipulation.

### 2.2.4 Distribution

**Centralized:** In centralized systems, parties are known to each other and that's why this system is trustworthy where participants are allowed to add to the ledger. Also transactions can be examined carefully because it knows the identity of the participant.

**Decentralization:** Blockchain systems adopt decentralized systems for transmission, verification, storing and updating of information for distributing system structure. Resistance to censorship and immutability are two of decentralization's most crucial characteristics. Its most distinguishing trait is its lack of reliance on a third party for security, which also ensures the protection of a person's assets or property.

### 2.2.5 Accessibility

There are 3 types of accessibility in the blockchain system. 1) Public 2) Private 3) Permissioned

**Public:** On a public blockchain, every user has the same set of rights. These include distributing authority equally among all participants rather than delegating control to a single party. Each party also has the flexibility to enter or exit the entire network at any time. Transactions can be validated by any source, including Bitcoin, and participation is completely free.

**Private:** A private blockchain ensures the centralized configurations. Furthermore, it was stated that only one entity has the power to decide, control operations, and manage the transaction validation process. The centralized authorized member will ensure that the recommended consensus is the only one followed, according to study. Any centralized entity, even state-level governments, would suffer from this.

**Permissioned:** Unlike a permissioned blockchain, which is a distributed ledger that is private. Only those with authorization are able to access this scattered network. This enables the users to carry out particular actions like reading, accessing, and creating data on the blockchain.



# Chapter 3

## Threat Modeling & Requirement Analysis

### 3.1 Threat Modeling

To understand threats in blockchain based medical healthcare systems we will use threat modeling which will help us design a secure system and it is used to identify,communicate and understand threats.We choose a model designed by Microsoft called STRIDE which encapsulate various threats for example :

1. **Spoofing Identity:** This term means an unauthorized person using the identity of an authorized person( a doctor/patient/system manager) to access the medical healthcare system to modify data.
2. **Tampering with Data:** An adversary will try to change data stored in the server of a hospital.
3. **Repudiation:** This model refers to denying having performed a particular action of a user.
4. **Information disclosure:** When stored data flows through the system or processed(doctors generate data and retrieve data) those data can be leaked.
5. **Denial of Service(DoS) :** In this threat an attacker can disrupt the availability of the system by identifying vulnerabilities.The attacker can overwhelm the system by finding the application level vulnerabilities, for example patient,doctor interaction with the system.
6. **Elevation of Privilege :** An adversary can get unauthorized access to higher privileges within the system using malicious software without the knowledge of a doctor who is responsible for block generation and retrieval.

### 3.2 Requirement analysis

Here we are going to identify and define security requirements for proposed blockchain based medical healthcare system by considering each part of the STRIDE model. First our proposed system has some core functionality and here we will discuss how proposed system keeps the functionality by identifying threats and ensuring security.

1. Both patient and doctor can register themselves from system manager.
2. The patient can give access to the doctors of his medical record
3. The doctor can propose a block into the private blockchain and retrieve data from other hospital's private blockchain

Now we are going to break down the requirement analysis process for each element of the STRIDE:

1. Our proposed blockchain based medical system must ensure authentication mechanism where only authorized patient and doctor can get access which mitigates Spoofing
2. A block will only be changed if more than  $2/3$  of nodes(block generators) from a private blockchain vote to change it. So even if any adversary try to change a data he/she must get  $2/3$  votes to change it which mitigates data tampering, repudiation.
3. Even if an adversary take over a node of a private blockchain he/she needs (specific patient id and keyword to obtain a data from the server) without these information he/she can't access patient data which mitigates information disclosure
4. The system will guard against any Dos attack by utilizing DDos protection service algorithm, traffic filtering, rate limiting etc which mitigates denial of service
5. The doctor can only add a block and retrieve data from a block only after the consent of the patient and if validated by others nodes. Which means doctor needs these minimum requirements to obtain data which mitigates elevation of privilege.

# Chapter 4

## System Design

### 4.1 Methodology

Usually, a patient may see a variety of healthcare experts, such as primary care doctors, specialists, and therapists. In light of the importance of data security and privacy preservation in this sector, industry and academics are paying greater attention to the sharing and exchange of health records [22]. One disease in a patient may be brought on by or linked to another pathology. The quantity and correctness of the patient's other health information that the doctor obtains in this circumstance has an impact on how accurately the diagnosis is made. By asking the patient, the doctor may learn a little bit about the sickness that is connected. Due to two factors, this method is insufficient to aid in diagnosis.

1. If events occurred in the past, the patient may forget certain details, such as the medications or medical tests they underwent, which could affect the accuracy of the diagnosis or treatments they received.
2. The patient's insufficient medical knowledge prevents him or her from describing the diagnosis or therapies in a professional manner, which impairs the present doctor's judgment. As a result, the current physician might not be able to make the proper diagnosis.

The sharing of the patient's medical history is a promising solution to the issue because it enables the targeted doctor to collect the necessary data for a more precise diagnosis. The doctor may view the relevant health record immediately through the local area network with the patient's consent if the patient had previously seen another doctor at the same hospital or medical facility and the record was prepared by that facility. In fact, the patient may visit a variety of hospitals and doctors for a range of symptoms. In this situation, if there isn't a separate agreement for the sharing of medical health records (MHR), other institutions will refuse the doctor's request to share the data.

Because blockchain is a distributed ledger and may be used to store health records for sharing, exchanging, and other purposes across stakeholders, it is suggested as a helpful approach to handle security concerns. [23]. A blockchain-based MHR sharing platform is expected to make medical record transfers secure. Despite its advantages

for dissemination and immunity, the blockchain-based system for exchanging medical records still confronts the following difficulties. How, for example, can a consensus method be created to allow blocks to be validated while patient privacy is preserved? How can we guarantee that the doctor has access to only the MHR that is intended for them? How can we stop unauthorized parties from connecting the health records of patients?

To solve the aforementioned issues, we propose creating a consortium blockchain instead of each hospital maintaining its MHR on a separate private blockchain. This would allow for secure and privacy-preserving MHR sharing among the hospitals. This has the advantages of speedy transactions, increased privacy protection, lower costs, and enhanced security. We employed two different forms of blockchain in our suggested framework: a private blockchain and a consortium blockchain. These two serve two different functions. For example, a private blockchain is used to organise MHR data, while a consortium blockchain records safe MHR indexes. Public keys are encrypted with keyword search to secure data security, control of access, security, and privacy, as well as to facilitate quick search. Additionally, in order to ensure system availability when adding new blocks to blockchains, proof of conformance is required.

As there will be numerous servers that hold the MHR in encrypted form and that reference will be maintained in a private blockchain, each hospital retains the patient's information. With these, we can get transactions completed quickly, at a low cost, and with enhanced privacy and security protection. Additionally, by accessing the private blockchain of particular institutions, clinicians can search for patient information indexes and access to the original record in the consortium blockchain.

1. In our framework we propose a blockchain for storing MHR, we used two blockchain. Private blockchain for storing reference of MHR of patients and consortium blockchain for keeping secure indexes of the MHR.
2. We design data structures and consensus mechanisms and block structure for both private and consortium blockchain.
3. We propose a protocol for MHR sharing where patients' MHR are encrypted for data security. Moreover, the identity of a patient is also encrypted for privacy called pseudo identity for further access of MHR. In this protocol, only the authorized doctor can be able to search the pseudo identities where patients' indexes are serialized. And only authorized doctors can get access to the patient's previous history of record.

## 4.2 Scenarios

To execute this plan there are basically 3 actors. The main one is the patient because the medical information of patients needs to be secured. Another actor is a doctor

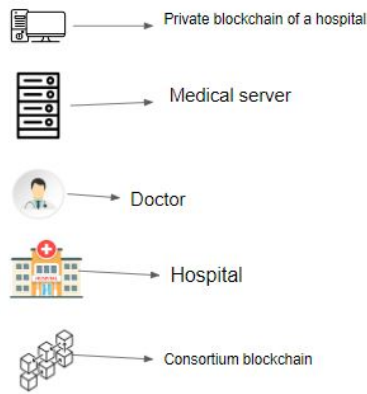


Figure 4.1: Assests in Proposed Scenerio

who will generate the medical prescription and the last one is the system manager who will be in charge of the whole system. Let's see the roles of each actor below.

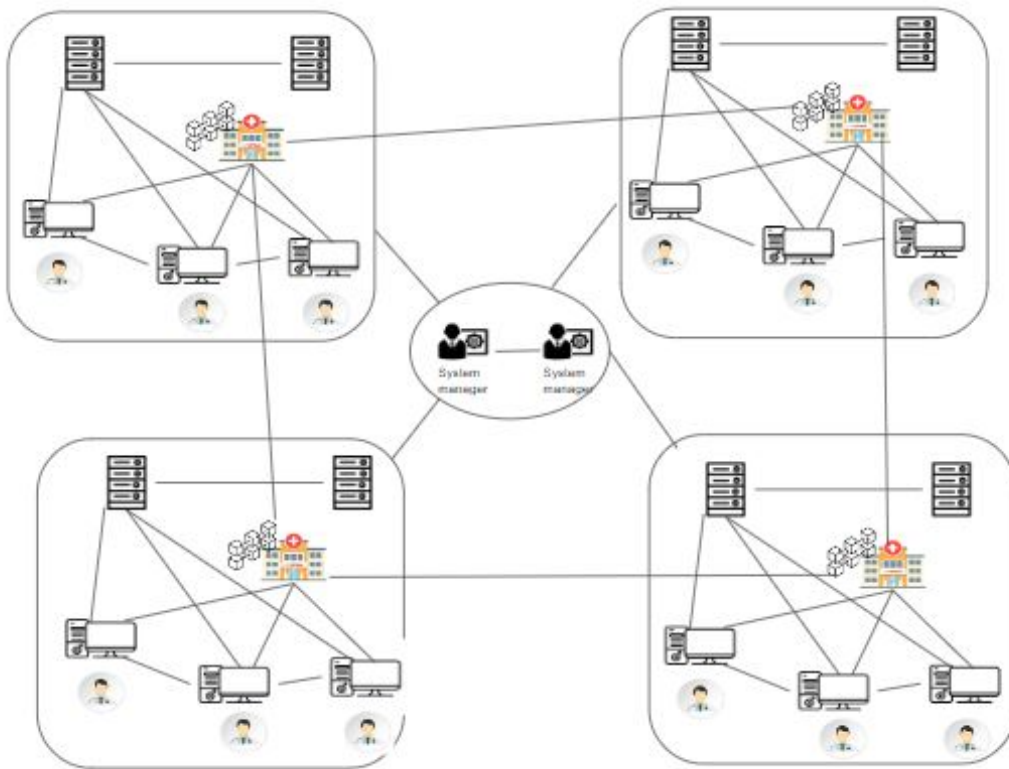


Figure 4.2: Scenarios

Let's imagine that multiple hospitals in Bangladesh come up with an agreement to connect a group to share their patients' health information. For these agreements two types of blockchain need to be constructed. Where the private blockchain of each hospital stores the original record and consortium blockchain stores keywords of Medical Health Record (MHR) generated by all the hospitals through private

blockchain. Some scenarios are:

**Scenario 1:** Both doctor and patient went to a system manager to get an account for themselves to register in the system. The system manager will be in charge of the whole system. Patients and doctors need to be registered by the system manager. It generates consensus vectors for consortium blockchain. System manager regulates system parameters and keeps a public key for both users and doctors. They will hand over the accounts to the doctors and patients. Firstly, doctors and patients need to register from the system manager only once in a lifetime. After registration, each patient and doctor will get a token to keep it secret. The patient can only show his/her to the doctor during checkup. This is evidence of interaction between doctor and patients and authorization to the doctor to generate a Medical Health Record (MHR) for the patients.

**Scenario 2:** A patient went to a medical institution or hospital where patients get their health services. Each hospital includes a private blockchain. Each computer client is operated by a doctor to store his/her corresponding patients record. Then those clients, which is basically a doctor, propose a block where the patient report is stored. When that particular doctor proposes a block the system will check the validation of the doctor and also the validation of the patient. The validation of the patient will be done by checking the secret id. When there will be two-third confirmation the block will be added in the private blockchain otherwise the block will be dropped.

**Scenario 3:** Medical Health Record (MHR) of a patient is stored in the private blockchain of the hospital where that person has visited. A patient can check up multiple doctors for different diseases, where that person can use that previous Medical Health Record (MHR) which is stored in a private blockchain. After then the hospital sends searchable keywords of blocks in their hospital's private blockchains and private blockchain to the common consortium blockchain. Then, the patient will confirm the authorized doctor when a doctor wants to get data from the private blockchain of another hospital through consortium blockchain. At this stage, since the consortium blockchain is stored in all of the hospitals, the doctor can retrieve the data from another hospital. Like this the Medical Health Record (MHR) is stored as distributed, immutability.

## 4.3 System Architecture

Here we design the blockchain for the MHR sharing system. We used data structure, and consensus mechanism in aspect to share MHR.

### 4.3.1 Data Structure

The blockchain based medical health care system there are a couple of things required which are data integrity , patient identity security and to ensure patients get the proper care and have control over their data. In order to generate Patient Medical

Health record(MHR) we proposed each hospitals will have a private blockchain with same consensus mechanism.These hospital with their own private blockchain will be connected through a consortium blockchain.The private blockchain will be responsible for generating patient data more secure way.To begin with, when a patient will visit the doctor for treatment the doctor will treat the patient and all information beside MHR for example who generated the block(doctor id) ,the owner of the block(patient secret id), MHR reference - the location of the server where the MHR is stored , MHR identifier - this field indicates the category of the disease so that when another doctor will search for the patient history he can find specific MHR , MHR hash value is a hashed value generated using SHA-256 from the MHR which will ensure if the data is modified or not.Moreover each block will have unique Block ID , Block size , previous block hash, contributor signature (sign by the doctor) and timestamp-when the block is generated.The doctor will then propose the block to be added to the private blockchain of the hospital.As the doctors are the participants for generating blocks all other participants will try to verify the block based on the consensus mechanism of the private blockchain in this case Permissioned Proof Of Stake .The doctors will be provided cryptocurrency by the system manager and based on their ranks the senior doctors will have more cryptocurrencies than others so that their block will get more priority.The participants validate a block by checking the identity of the doctor and whether the doctor have enough cryptocurrency to propose a block, weather the digital signature of the doctor is valid or not.

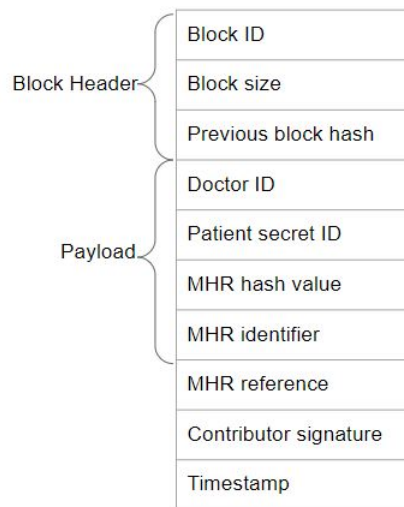


Figure 4.3: Structure of a block in private blockchain of hospital

Secondly, consortium blockchain store the indexes of that block and not the whole data so that using the indexes from consortium blockchain a specific block can be found(Figure 4.3).The header section is same as all the block of blockchain unique block id, block size , previous block hash.In payload section there is block generator id-in this system hospital id(hospital will generate the block of the consortium blockchain), there will be secure indexes part where couple of transactions from a hospital.The blocks of the consortium block is proposed by the hospitals. In a certain hospital when doctors add blocks to the private blockchain of that hospital the server

of consortium blockchain actually extract some information from the blocks. The informations are Block Id of a particular block, patient secret ID , MHR hash value and MHR identifier and treated as transactions for the block that the hospital will going to propose. After a certain amount of time the transactions that the hospital server collected will be added to the block and the hospital server will propose the block to be added to the blockchain. Then other hospitals that are participating in this block generation process will check the validity of the block based on the consensus mechanism of the consortium blockchain which is Proof of Authority. Proof of Authority is chosen here because all the participants are known and trusted authorities (Hospitals). It has low latency and high throughput as no computation power is needed to generate a block and unlike Proof of Stake no cryptocurrencies are needed to keep as stake to be able to participate in the block generation process. All other participants here will check the validity of the block by checking the validity of the block generator id and digital signature.

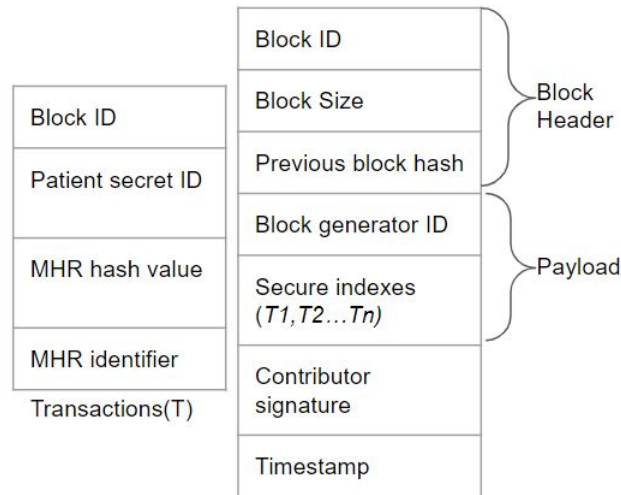


Figure 4.4: Structure of a block in the consortium blockchain

### 4.3.2 Mechanism

To start, we will focus on the term system manager and how he manages. The system manager will be responsible for overall system. Though system manager is a single term but it is a distributed system like blockchain which will generate both patient and doctor's account for the consortium network. Initially, both patient and doctor will submit necessary papers for opening an account. If majority of the system manager approve, then an account is provided and secretly kept for recovery. If a person wants to retrieve his/her user account then necessary documents have to be submitted and if majority system manager approves then the account can be retrieved. There is an exception for patient account, besides providing the private id the patient will also be provided an secret id for secure identity. Using the account the doctors can log in at their respective hospital's private blockchain. Before joining the hospital the network will check the validity of the user by sending the id to system manager and if authorized then the doctor can login to the private blockchain. In a hospital



a doctor will have the whole private blockchain in his computer.

Secondly, generation of patient healthcare procedure is involved just doctors and patient .When a patient wants to visit a doctor that patient will first give access that doctor means patient secret id will be send to that doctor.Then the patient will physically visit the doctor and using the secret id doctor will generate a medical record.Medical record will be generated and stored encrypted(SHA-256) at the hospital’s multiple replicated server and it will managed using data mirroring .But all the information regarding that record will be saved in a block of that private blockchain which will include a reference pointer point towards the location of the record in medical server.Doctors are nodes here so if more than 2/3 of the nodes approves for the block the block gets added to the blockchain.The hospital’s server for consortium blockchain will store the reference points for the blocks that already generated in the private blockchain.It means using consortium blockchain a block of a private blockchain can be find easily. Thirdly, when a patient visits a doctor of a hospital the doctor needs previous medical information.The doctor will use a specific keyword(MHR identifier) for specific disease record and secret id of the patient to look into the consortium blockchain.

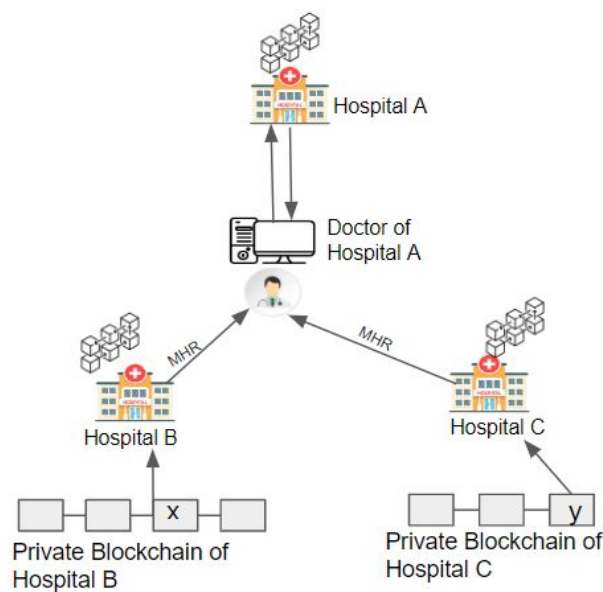


Figure 4.5: Mechanism of proposed system

From (figure 4.5) the doctor first searches the patient information from his/hers hospital’s consortium blockchain server.The information mainly contains private blockchain name, that private blockchain’s block id , MHR hash value,patient secret id.For example, the doctor is searching for a patient whose secret id is “1bad34. . . 23” and he needs information on previous diabetes records and treatments the patient received.Then from consortium blockchain doctor knows that there are two medical records on diabetes of the patient “1bad34. . . 23”.One of the two records is in “block x” of Hospital B’s private blockchain and another is “block y” of Hospital

C's private blockchain. After receiving these information the doctor will then try to log into respective medical private blockchain. The hospital will only allow the doctor if he/she is verified from system manager. The doctor initially checks if the private block's MHR hash value is same as MHR hash value from consortium. The MHR hash value is a hash value of the medical record which means if a hospital want to change someone's medical record the MHR hash value of that record will also change and will not match with the initial MHR hash value that is stored in the consortium blockchain. Then the doctor retrieve the MHR of that patient from the specific block. The block doesn't contain actual MHR just the reference location of the server where the data is stored.

# Chapter 5

## Implementation

### 5.1 Window Navigation Diagram

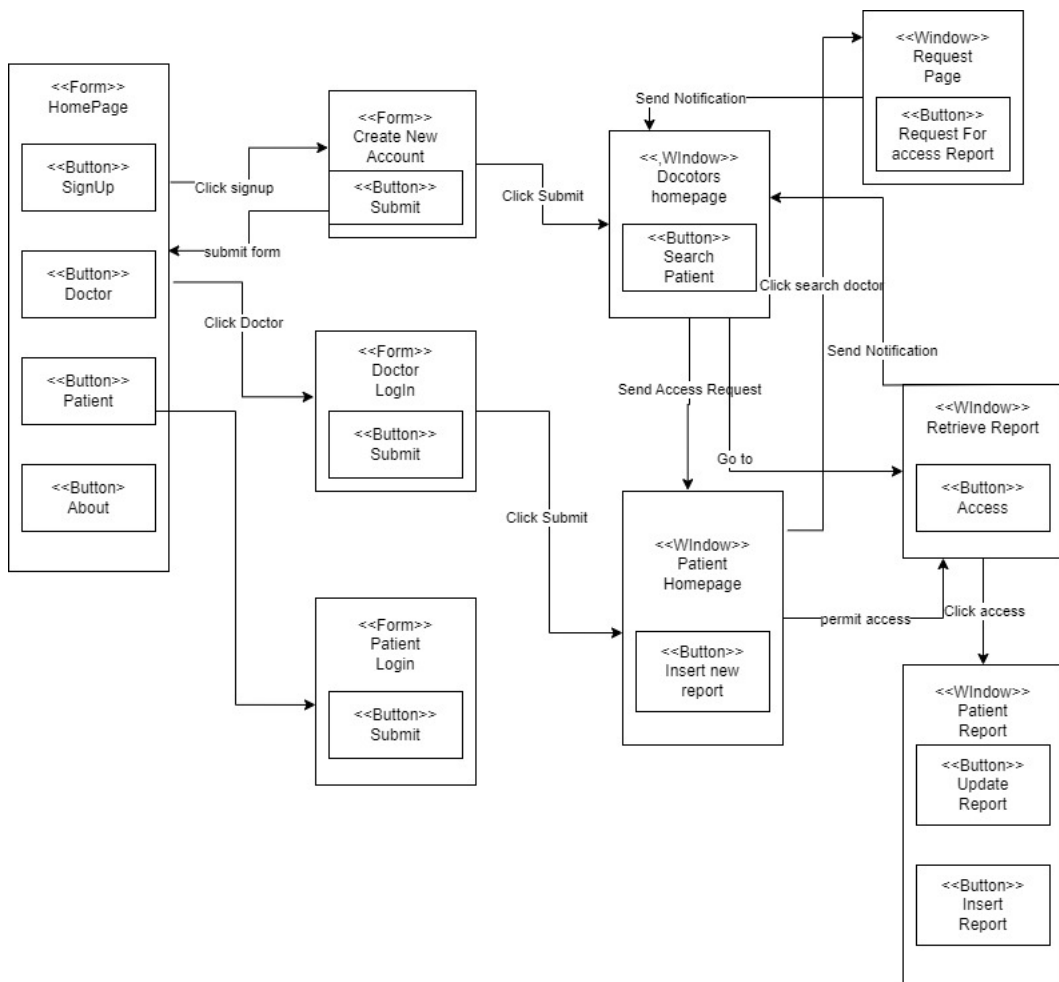


Figure 5.1: Window Navigation Diagram of Proposed Plan

#### 5.1.1 Full Procedure of Window Navigation Diagram

First patient will log in using a provided private key from the administrator which is the same for a doctor. patient will have several options for example they can see their

all medical records history, search for registered doctors, give permission to a specific doctor and also can remove permission that was given. Now all these procedures are complex. To begin with searching the doctors using their name is done where a search bar option is shown in patient end of the web. For this procedure all the private key of all the doctors that are registered under all the private blockchains are stored in patient end. Using the private key website will retrieve the basic information of that doctor (Name, field of speciality (Medicine, Surgeon etc), degree of qualification (MBBS, MD etc)). Patient will search by the name of the doctors and select a doctor which he/she want to give access. When he/she will press access the unique id of that patient (which will be used for storing MHR) will be sent to the doctor. Then in the doctor end doctor can see the patient lists who allowed him their MHR access. Our website will automatically collect the MHR (Medical Health Information), based on all the unique id of the patients. When doctor will accept the patient request all the information will be shown and he will have some extra feature which is add new MHR. The doctor will then prescribe the patient based on previous medical history if necessary.

## 5.2 Blockchain Account

Every patient and doctor have a unique blockchain Id. By this id the doctor and patient will interact with each other. This Id helps the patients to find the specific doctor among all the doctors and take appointments from the doctor. Also the doctor will use this unique id for treatment and prescribe the patients.

```
function App() {
  const dispatch = useDispatch();
  const loadBlockchainData = async () => {
    const provider = loadProvider(dispatch);
    const chainId = await loadNetwork(provider, dispatch);
    window.ethereum.on("accountChanged", () => {
      loadAccount(provider, dispatch);
    });
    console.log({ provider, loadAccount });
    window.ethereum.on("chainChanged", () => {
      window.location.reload();
    });
    const medicalStorage = loadMedicalStorage(
      provider,
      config[chainId].MedicalStorage.address,
      dispatch
    );
    subscribeToEvents(medicalStorage, dispatch);
  };
  useEffect(() => {
    loadBlockchainData();
  });
}
```

Figure 5.2: Initializing Data

## 5.3 Smart Contract Description

The smart contract contains several elements and there are some variables and functionality. There are struct type variables for example Patient (name, age, problem, doctors[])

,Doctor(name,details,PatientList(list)) and Diagnosis(name of the diagnosis,medical info etc).There are some functions for example:

- registerDoctor:
  - Functionality: Allows a doctor to register in the system.
  - Parameters: name and details(academic degree).
  - Moreover this function emits an event while creating using the doctor's name and details.
- addPatient:
  - Functionality:add a patient into the blockchain
  - There are several parameters like `_name`,`_age`,`_problem` which was memory type variables where all these information are send to struct Patient patient list if a new patient got registered.
- addDoctor:
  - The functionality of addDoctor is that the patient will have a list of all the doctors in their dashboard from which he/she will choose a doctor who will have access to the patient history.
  - This function wiil have the algorithm:

if doctor already given permission and number of permission given to

$(doctors < 5) :$

Show error message(doctor already exist)

else:

The private blockchain address of the doctor will be added under that patient

- revokeDoctorAccess:
  - This function will allow the patients to revoke access of their medical information from a doctor by the private address of the doctor.
  - The algorithm is :
    - If the private blockchain address of doctor exist in patient's doctor list and patient in doctor's patient list:
      - Revoke access of the doctor from the patient list of doctors and revoke access of the patient from the doctor list of patients
    - Else:
      - Doctor/patient not found
- ProvideDiagnosis:
  - This function will allow the doctors to provide a diagnosis and medicine info for a patient which blockchain address will be given.

- The algorithm is :
  - If the patient address exists and the doctor has authorization:
    - The doctor can provide diagnosis
    - Store the diagnosis and the medical information in patient’s record
  - Else:
    - Doctor not authorized
- Event: Emits a `MedicalStorage _ProvideDiagnosis` event with the patient’s address, the doctor’s address, diagnosis, and medicine information.
- `findDoctorIndex(private)`:
  - This function finds the index of a doctor from the list of doctors of a patient.
  - The algorithm is :
    - If the patient address and doctor address are valid :
      - returns an index number of the doctor
    - Else:
      - return -1(not found)
- `findPatientIndex(private)`:
  - This function finds the index of a patient from the list of patients of a doctor
  - The algorithm is :
    - If the patient address and doctor address are valid:
      - returns an index number of the patient
    - Else:
      - return -1(not found)
- `checkDoctorAlreadyExists (public)`:
  - This function is the function which is called from other functions to check whether a doctor is already in a patient’s list of doctors or not
  - The algorithm is :
    - If the doctor address present at patient list:
      - return True
    - Else:
      - return False
- `checkPatientAlreadyExists (public)`:
  - This function is the function which is called from other functions to check whether a patient is already in a doctor’s list of patient or not

- The algorithm is :
  - If the patient address present at doctor list:
    - return True
  - Else:
    - return False

## 5.4 Medical Record

Medical records part collects all the data from both patients and doctors. Here, a total of nine functions are used to collect all the records. These all 10 functions are gathered by the struct method which is a creative data structure format in Solidity where variables of diverse data types can be bundled into one variable or a custom-made type. By calling every patient's and doctors recordID the recorded data has been found. The functions are like

- **getRecordId():**

Here the medical sector gives their patient a specific recordID. This recordId generates from the transaction between patient and doctors. This unique RecordId holds the specific data for each of the patients. Here this function is used for getting the RecordID for each transaction between a doctor and patients.

```
function getRecordId() public view returns (uint) {
    return recordId;
}
```

Figure 5.3: Get Record ID

- **getTimeStamp(uint \_recordId):**

The Timestamp

```
function getTimeStamp(uint _recordId) public view returns (uint) {
    return records[_recordId].timestamp;
}
```

Figure 5.4: Time Stamp ID

- **getAge(uint \_recordId):**

The getAge function helps to generate the age of the patients to the specific patient information. The specific patient has been identified by the recordId. Because each patient has a unique recordId.

```
function getAge(uint _recordId) public view returns (uint) {
    return records[_recordId].age;
}
```

Figure 5.5: Get Age

- **getName(uint \_recordId):**

The getName function helps to generate the name of the patients to the specific patient information. The specific patient has been identified by the recordId. Because each patient has a unique recordId.

```
function getName(uint _recordId) public view returns (string memory) {
    return records[_recordId].name;
}
```

Figure 5.6: Get Name

- **getGender(uint \_recordId):**

The getGender function helps to generate the gender of the patients to the specific patient information. The specific patient has been identified by the recordId. Because each patient has a unique recordId.

```
function getGender(uint _recordId) public view returns (string memory) {
    return records[_recordId].gender;
}
```

Figure 5.7: Get Gender

- **getBloodType(uint \_recordId):**

The BloodType function helps to generate the blood group of the patients to the specific patient information. The specific patient has been identified by the recordId. Because each patient has a unique recordId.



```
function getBloodType(uint _recordId) public view returns (string memory) {
    return records[_recordId].bloodType;
}
```

Figure 5.8: Get Blood type

- **getAllergies(uint \_recordId):**

The getAllergies function helps to generate the Allergies of the patients to the specific patient information. It helps to find the patient's past diseases. The specific patient has been identified by the recordId. Because each patient has a unique recordId.

```
function getAllergies(uint _recordId) public view returns (string memory) {
    return records[_recordId].allergies;
}
```

Figure 5.9: Get Allergies

- **getDiagnosis(uint \_recordId):**

The getDiagnosis function helps to generate the diagnosis result of the patients to the specific patient information. The specific patient has been identified by the recordId. Because each patient has a unique recordId.

```
function getDiagnosis(uint _recordId) public view returns (string memory) {
    return records[_recordId].diagnosis;
}
```

Figure 5.10: Get Diagnosis

- **getTreatment(uint \_recordId):**

The getTreatment function helps to generate the suggested treatments of the patients to the specific patient prescriptions. The specific patient has been identified by the recordId. Because each patient has a unique recordId.

```

function getTreatment(uint _recordId) public view returns (string memory) {
    return records[_recordId].treatment;
}

```

Figure 5.11: Get Treatment

## 5.5 Front End

First patient will log in using a provided private key and password from the administrator which is the same for a doctor. patient will have several options for example they can see their all medical records history, search for registered doctors, give permission to a specific doctor and also can remove permission that was given. Now all these procedures are complex. To begin with searching the doctors using their name is done where a search bar option is shown in patient end of the web. For this procedure all the private key of all the doctors that are registered under all the private blockchains are stored in patient end. Using the private key website will retrieve the basic information of that doctor (Name, field of speciality (Medicine, Surgeon etc), degree of qualification (MSC, MD etc)). Patient will search by the name of the doctors and select a doctor which he/she want to give access. When he/she will press access the unique id of that patient (which will be used for storing MHR) will be sent to the doctor. Then in the doctor end doctor can see the patient lists who allowed him their MHR access. Our website will automatically collect the MHR (Medical Health Record), based on all the unique id of the patients. When doctor will accept the patient request all the information will be shown and he will have some extra feature which is add new MHR. The doctor will then prescribe the patient based on previous medical history if necessary.

In this project, there are many features to get medical based information for both doctors and patients with higher privacy. Here both patients and doctors can register to their platforms. After that a patient can select his suggested doctor and give the medical information access to the doctor and on the other hand the doctor can see the patient's medical details and give the diagnosis of a particular disease. If the patient wants to remove the access to his medical information, he or she can remove the access from the doctor. The functionalities are divided into two parts. One is for doctors registration and login and one is for patients registration and login.

### 5.5.1 Patient

For patients, here is particular patient login and registration. For registration we have a form to fill up with the **registration** information. After registration we can **login** as a patient. Then we can see the **patient's personal information** with the patient name, age and problem. Here there is a button for **Show diagnosis** which can show the doctors prescribing medical tests or diagnosis and the doctor's name also. Below the patient's personal information there is an option to **share the medical record** with the particular doctor. Here we can share the medical record with the particular doctor selection. Also in the bottom there is an option like **Current EMR Access Holder** which can remove the access of a particular

doctor by showing doctors name, details and public key. If the access will remove the shared medical data with the doctors will be removed also.

Figure 5.12: Patient Registration

Name	Details	Public Key	Revoke Access
rifat	AH	0xa06...b02e	Revoke

Figure 5.13: Patient Dashbord

## 5.5.2 Doctor

For doctors, here is particular registration and login. For registration we have a form to fill up with the **registration** information as usual. After registration we can **login** as a doctor. Then we see a window which contains doctors **personal information** and **Access EMRs**. In doctors personal information the doctor can see his name and details. Below this segment there is another feature called Access EMRs which contains the shared medical records of the patients with the patient name, public key and view records. By clicking the **view record** button the doctor can see the patient’s name, age, problems and the previous diagnosis results. Here doctors can prescribe **new medicine** and new diagnosis.

**Personal Information**

**Name:** shaheen  
**Details:** MBBS

**Access EMRs**

Name	Public Key	View Records
Aditya	0xFeAe4EB8C66B08F38AC9CE62C9F6F4BbBdAc568A	<a href="#">View Records</a>
Tahmid Chowdhury	0x68A4Cde2Bf99E82d07a8fc71232114b593CCafe2	<a href="#">View Records</a>

Figure 5.14: Doctor Dashbord

**Personal Information**

**Name:** shaheen  
**Details:** MBBS

**Access EMRs**

Name	Public Key	View Records
Aditya	0xFeAe4EB8C66B08F38AC9CE62C9F6F4BbBdAc568A	<a href="#">View Records</a>
<div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <p><b>0x68A4Cde2Bf99E82d07a8fc71232114b593CCafe2</b></p> <p><b>Previous Diagnosis :</b> eye chekup</p> <p><b>Previous Medicines :</b> napa</p> <p><b>Give New Diagnosis :</b></p> <p><b>Name :</b> Tahmid Chowdhury</p> <p><b>Age :</b> 23</p> <p><b>Problem :</b> Hyperopia</p> </div> <div style="width: 35%;"> <p><input type="text" value="Eye sergery"/></p> <p><input type="text" value="Paracetamol"/></p> <p><input type="button" value="Submit"/></p> </div> </div> <div style="text-align: right; margin-top: 10px;"> <input type="button" value="Hide Records"/> </div>		

Figure 5.15: Prescription Writing

# Chapter 6

## Discussion

This chapter will perform the analysis and interpretation of the conclusions and presumptions made in the methodology chapter.

### 6.1 Validation of Model

This model proposed a system where the patient's information, including their prior medical history, will be securely preserved in a decentralized server system in each hospital with the help of blockchain technology, reducing recurring costs and establishing provider responsibility by suggesting a blockchain-based healthcare system with appropriate access controls for patient data. This model differs from [24] where the private blockchain is responsible for storing the MHR while the consortium blockchain keeps records of the secure indexes of the MHR. In this paper, we discussed, Medical health information (MHR) is stored using a private blockchain, and secure MHR indexes are recorded on a consortium blockchain. Patient private key are hidden instead they use pseudo id to secure data security, control of access, security, and privacy. Additionally, in order to ensure immutability, decentralization, data integrity in this model, permission proof of stake is required for private blockchain and proof of authority is required for consortium blockchain. Data immutability is also ensured by some key features stored in both private and consortium blockchain. Besides all data in the medical server are encrypted using SHA-256 encryption and can only be retrieved using their exact location which is stored in the MHR reference section of the blocks. Moreover to access that block patient authorization is needed (patient secret id).

### 6.2 Hardware Cost

It would be better if we use to hold all medical data in blockchain but due to practical issues like storage capacity, cost, transaction of medical data onto the blockchain, large medical data should be stored out of the blockchain [18]. Private blockchain hardware cost lesser than any public blockchain. Since, it targeted a specific amount of people, so the requirements of hardware system can be simple. Windows 8 (Intel i7-6700, 3.40 GHz with 8 GB RAM Samsung Inc. Seoul, South Korea) these hardware has been used to mine in POF by using Multichain 2.0 [14]. Since proposed model is also a permission based so these configuration should be enough to run proposed

system. Now a days if someone wants to build a PC that person, normally will buy this kinds of configuration. To run modern games and softwares 8 GB RAM is required. Infact also in [14] the researchers used this configuration to create a realtionship among patient, cured patient, doctor and insurance company through blockchain by using Multichain 2.0. In their blockchain record, there will be doctor’s record, feedback of a cured patient along with policy of insurance company and decision of the blockchain system. Proof of Familiarity(PoF) has been use here as a consensus mechanism.

Now, it is important to see the price range of this hardware components in Bangladesh so that it can be shown that how much feasible the system is. We are adding the others components also like storage, monitor, mouse, keyboard, CPU case etc to make a full Price of a PC which will be in the work of a doctor. Startech is a famous shop in Bangladesh for selling laptop, computer gadgets etc. The price of the components in Startech is given below. It can be verified through their website.

Table 6.1: Cost Table

<b>Hardware</b>	<b>Specification</b>	<b>Price (in BDT, can be changed time to time)</b>
Intel 10th Gen Core i7-10700 Processor	Frequency: 2.90 GHz up to 4.8GHz; 16M Cache; 8 Core 16 Threads; Intel UHD Graphics 630	25000
Crucial 8GB DDR4 3200MHz UDIMM Desktop RAM	Capacity: 8GB; Speed: DDR4-3200; CAS latency: 22-22-22-22; Voltage: 1.2V	2100
Samsung 980 1TB PCIe 3.0 M.2 NVMe SSD	Form Factor: M.2 (2280); NVMe SSD: PCIe 3.0 ; Read Speeds: 3,500MB/s; Write Speeds: 3,000MB/s	7899
Asustor DRIVESTOR 4 Pro AS3304T 4-Bay NAS	MPN: AS3304T; Model: DRIVESTOR 4 Pro; Realtek RTD1296 Quad-Core 1.4 GHz CPU; Uses 2 GB DDR4 40% more efficient; Max Internal Capacity: 72 TB	56980 * 2 = 113960
DeepCool CC560 Limited Mid-Tower Case	Motherboard Support: Mini-ITX / Micro-ATX / ATX; Full-sized Tempered Glass Window; Top Panel Magnetic Dust Filter; I/O Ports: USB3.0×1, USB2.0×1, Audio×1	3600
Continued on next page		

Table 6.1 – Cost Table (continued from previous page)

Hardware	Specification	Price (in BDT, can be changed time to time)
Acer Nitro V206HQL A 19.5” HD Monitor	Model: V206HQL A; Resolution: HD (1600 x 900); Display: TN, 60Hz, 5ms; Ports: VGA, HDMI; Features: Ergonomic design	8200
Logitech K120 Usb Keyboard With Bangla Black (920-008363)	Model: Logitech K120; Type :USB; Cable Length 150cm Approx; Weight: 1.21 pounds;	725
Micropack M101 Optical USB Mouse	Model: Micropack M101; Interface Type :USB 2.0; Button: 3D; Resolution: 1000dpi; Cable Length: OD 3.2mm;	325

If we use this configurations to build a PC for the doctor then it will cost total 161934 taka.

**Clarification of the Storage:** If we follow the storage of the table 6.1 which is 1 TB SSD then we can assume a scenerio of patient data storage and according to that a calculation of how many years it can be used is given below .

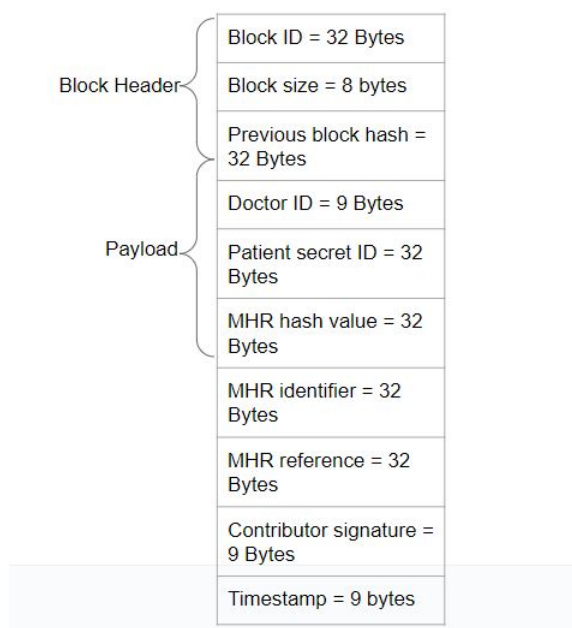


Figure 6.1: Size of Blocks in a Private Blockchain

From [24] we can get ideas that what can be the size of a block in a Blockchain network and with it we also assumed some of the sizes. According to Figure 6.1 the total sizes of the block is 227 Bytes. If in a hospital the number of patients becomes 10000 daily, then the size will be 2.27MB. If it continues till 1 year then the size of the files becomes 828.55 MB. If it continues for 70 years then the size will be 57995 MB which is equal to 57.995 GB. Since we are taking a plan to give the storage 1 TB so from this calculation we can find that the private blockchain can be worth storing many years of patients data like this.

**Our Hardware Configuration:** To test proposed model, we have created a sample. While creating a sample for proposed model we have used a laptop which configuration was Intel core i7 8th generation with 12 GB DDR4 RAM and 512 GB SSD which price also be almost similar or lesser than the previous hardware cost. Here we, have just used our laptop to test the model, so the storage capacity is lower than the [14]

**Blockchain Size:** In Permission base proof of stake blockchains, block size is not typically a major concern like bitcoin or Proof of Work blockchains. Same goes for the Proof of Authority. We all know the Ethereum is a public blockchain network that means all of the transaction in Ethereum stored in a single blockchain network. According to a website named ardrive which gives various informations about blockchain network, the Ethreum was established in December 2013 and till December. 2022 the size of the Ethereum blockchain is only 1055 GB which is equal to 1.055 TB. As we are using a private blockchain network the size should not be much like this. So the block size and data storage will not be a problem for proposed design and requirements.

## 6.3 Security Impact to secure Confidential Medical Information

### 6.3.1 Data Integrity and Immutability

The proposed model allows a technology to make sure that medical data is immutable once it is stored on the blockchain and cannot be changed or interfered with. The proposed model keep it's data integrate where only authorized person can access them in this model it's the doctors.A block will only be changed if more than 2/3 of nodes(block generators) from a private blockchain vote to change it.So even if any adversary try to change a data he/she must get 2/3 votes to change it which ensures the data will be immutable.Moreover even if the hospital authority tries to change data they can change it because of 2/3 rule, it can be traced.There is a field called MHR hash value which is common in both block of private blockchain and transactions of consortium blockchain.So if data is change then those two field will not match.The risk of medical fraud or data manipulation is decreased thanks to this feature, which improves the integrity of patient information by preventing



unauthorized adjustments.

### **6.3.2 Enhanced Security**

To ensure patient privacy, confidential medical information needs to be protected by strong security measures. The proposed model allows guarantees that only authorized parties can access private keys and cryptographic methods that protect sensitive medical data. The system's decentralized structure also lowers the possibility of single points of failure and unwanted access.

### **6.3.3 Consensus Mechanism**

This model depends on consensus techniques to authenticate and include transactions in the chain. By ensuring that all network users concur on the data's state, this distributed consensus makes the network highly resistant to attacks and preserves the accuracy of medical information.

### **6.3.4 Resistance to DDoS Attacks**

Since decentralized blockchain networks lack a centralized server to attack, distributed denial-of-service (DDoS) attacks are less successful against them. Moreover the system will guard against any Dos attack by utilizing DDoS protection service algorithm, traffic filtering ,rate limiting etc which mitigates denial of service. By doing this, the system's availability is improved and any disruptions are avoided.

### **6.3.5 Interoperability and Data Sharing**

The proposed model allows private, secure data sharing across various healthcare organizations and providers. This model ensures collaboration between different private blockchain which are linked with consortium blockchain. If an authorized doctor wants he/she can access patient data by accessing in the consortium block chain. The consortium blockchain stores information regarding a block of a private blockchain. In order to facilitate smooth interoperability throughout the healthcare ecosystem, patients can authorize access to their medical records based on a need-to-know basis.

### **6.3.6 Data encryption**

The model we proposed ensures the encrypted medical data before storing it in the blockchain. That's why, if someone gain the access the data, they can't read the data without decryption key.

### **6.3.7 Data privacy**

Once data is in the chain it is extremely difficult to remove or delete or alter, as blockchain technology is immutable. This is one of the core advantages in our proposed model. When a doctor generates the medical report all the information regarding that report will be added to the blockchain, he or she can't edit or delete the report. This one helps to find out fraud reports or doctors. Also, only authorized doctors have the access to sensitive medical data and can control those data.

## 6.4 Comparison With Other Models

Table 6.2: Comparison

Properties	[15] Y.Yang, M.Ma	[16] Q.Xia, E.B. Sifah, K.O. Asamoah, J.Gao, X.Du, M. Guizani	[17] Q.Xia, E.B. Sifah, K.O. Asamoah, J.Gao, X.Du, M. Guizani	[14] J. Yang, M.Onik, N.Y. Lee, M. Ahmed, C.S. Kim	[18] Y. Chen, S. Ding, Z.Xu, H. Zheng, S.Yang	[19] M.Du, Q.Chen, J.Chen, X.Ma	Proposed Model
Blockchain-based	N	Y	Y	Y	Y	Y	Y
Access control	Y	Y	Y	Y	Y	Y	Y
Secure Search	Y	Y	Y	N/A	Y	Y	N
Data auditing	Y	Y	Y	Y	Y	Y	Y
Tamper Resistance	N	N	N	Y	Y	N/A	Y
PoW	N	N	N	N	N	N	N
Secure Storage	N	Y	Y	Y	Y	Y	Y
Consensus	N/A	PoS	PoS	PoF	DPOS	MBFT	PPoS + PoA
Can retrieve Lost Information	N	Y	Y	Y	N	N	Y

# Chapter 7

## Conclusion

Blockchain implementation is continued in various platforms. But except for a few implementations, all implementations are not perfect. There are some failings and complexity. As we know, Bitcoin is the first successful Blockchain implementation introduced by Satoshi Nakamoto. In our reports the implementation of those platforms is also processed day by day. Mostly we used blockchain for securing data and platforms. So, Blockchain implementation should be growing in an efficient way which can be easily used and also give us a secure world.

In a regular system patient's electronic data is stored in a central server by a health service provider and the data store format is different from other health provider's data store format which has probability of being hacked and a single point of failure. In our proposed model medical records are encrypted and stored outside a blockchain and location of the records and other transaction information are stored in the blockchain also only be accessed who have permission. In our model doctors prescribe patients sometimes based on previous medical records stored in decentralized database and store new medical records via transactions using patients secret key. If anyone want to access that data he/she need patient's secret key which patient will provide. Thus data will be accessed only by trusted parties.

In our protocol Hyperledger Fabric (private blockchain) will be used for decentralized secure architecture for the all hospitals. For the private blockchain Permissioned Proof Of Stake (PPoS) is used where there will be entity within the hospital who will be responsible for generating the blocks. On the other hand the consortium blockchain will be the bridge between the private blockchain and decentralized which will use Proof Of Authority (PoA). In this mechanism all the nodes will be the hospitals themselves who are a limited set of known and trusted nodes who will be authorized to validate the transactions on consortium blockchain. PoA is suitable for this type of architecture where all the nodes will be predefined by the main authority. In our project the implementation of the private blockchain which was used for all the transactions for each hospital. Here, using doctor and patient unique id patient and doctor both can login. The doctor can prescribe a medicine of a patient of a single particular hospital. Moreover the doctor can only access the previous medical record of that hospital but can't access other hospitals medical information. So the future work will be to incorporate the consortium blockchain where there will be medical history of all the hospitals the patient visited and doctors of one hospital

can access healthcare information prescribed by other doctors.

To conclude, the model will be able to achieve patient data access control and data integrity.

# Bibliography

- [1] Government of the People’s Republic of Bangladesh, *National blockchain strategy: Bangladesh. pathway to be a blockchain-enabled nation*, Information and Communication Technology Division, Mar. 2020.
- [2] Z. Sun, D. Han, D. Li, X. Wang, C. C. Chang, and Z. Wu, “A blockchain-based secure storage scheme for medical information,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2022, no. 1, 2022. DOI: 10.1186/s13638-022-02122-6.
- [3] X. Li, Y. Mei, J. Gong, F. Xiang, and Z. Sun, “A blockchain privacy protection scheme based on ring signature,” *IEEE Access*, vol. 8, pp. 76 765–76 772, 2020. DOI: 10.1109/access.2020.2987831.
- [4] A. Sharma, Sarishma, R. Tomar, N. Chilamkurti, and B.-G. Kim, “Blockchain based smart contracts for internet of medical things in e-healthcare,” *Electronics*, vol. 9, no. 10, p. 1609, 2020. DOI: 10.3390/electronics9101609.
- [5] S. Nusrat, *Use of blockchain technology in banking in bangladesh; usefulness, hurdles and recommendations*.
- [6] K. Häyrinen, K. Saranto, and P. Nykänen, “Definition, structure, content, use and impacts of electronic health records: A review of the research literature,” *International Journal of Medical Informatics*, vol. 77, no. 5, pp. 291–304, 2008.
- [7] Q. Wang, F. Zhu, S. Ji, and Y. Ren, “Secure provenance of electronic records based on blockchain,” *Computers, Materials and Continua*, vol. 65, no. 2, pp. 1753–1769, 2020.
- [8] O. Hasan, L. Brunie, and E. Bertino, “Privacy preserving reputation systems based on blockchain and other cryptographic building blocks: A survey,” *HAL Open Science*, 2020.
- [9] M. I. Khalid, J. Iqbal, A. Alturki, S. Hussain, A. Alabrah, and S. S. Ullah, “Blockchain-based land registration system: A conceptual framework,” *Applied Bionics and Biomechanics*, vol. 2022, pp. 1–21, 2022.
- [10] X. Xu, D. Zhu, X. Yang, S. Wang, L. Qi, and W. Dou, “Concurrent practical byzantine fault tolerance for integration of blockchain and supply chain,” *ACM Transactions on Internet Technology*, vol. 21, no. 1, pp. 1–17, 2021. DOI: 10.1145/3395331.
- [11] S. Tanwar, K. Parekh, and R. Evans, “Blockchain based electronic healthcare record system for healthcare 4.0 applications,” *Journal of Information Security and Applications*, vol. 50, p. 102 407, 2020. DOI: 10.1016/j.jisa.2019.102407.

- [12] P. Pandey and R. Litoriya, “Securing and authenticating healthcare records through blockchain technology,” *Cryptologia*, vol. 44, no. 4, pp. 341–356, 2020. DOI: 10.1080/01611194.2019.1706060.
- [13] P. Li, S. D. Nelson, B. A. Malin, and Y. Chen, “Dmms: A decentralized blockchain ledger for the management of medication histories,” *Blockchain in Healthcare Today*, vol. 2, pp. 1–15, 2018. DOI: 10.30953/bhty.v2.38.
- [14] J. Yang, M. Onik, N.-Y. Lee, M. Ahmed, and C.-S. Kim, “Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making,” *Applied Sciences*, vol. 9, no. 7, p. 1370, Apr. 2019. DOI: 10.3390/app9071370. [Online]. Available: <https://doi.org/10.3390/app9071370>.
- [15] Y. Yang and M. Ma, “Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds,” *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 4, pp. 746–759, Apr. 2016. DOI: 10.1109/tifs.2015.2509912. [Online]. Available: <https://doi.org/10.1109/tifs.2015.2509912>.
- [16] Q. Xia, E. Sifah, A. Smahi, S. Amofa, and X. Zhang, “BBDS: Blockchain-based data sharing for electronic medical records in cloud environments,” *Information*, vol. 8, no. 2, p. 44, Apr. 2017. DOI: 10.3390/info8020044. [Online]. Available: <https://doi.org/10.3390/info8020044>.
- [17] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, “MeD-Share: Trust-less medical data sharing among cloud service providers via blockchain,” *IEEE Access*, vol. 5, pp. 14 757–14 767, 2017. DOI: 10.1109/access.2017.2730843. [Online]. Available: <https://doi.org/10.1109/access.2017.2730843>.
- [18] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, “Blockchain-based medical records secure storage and medical service framework,” *Journal of Medical Systems*, vol. 43, no. 1, Nov. 2018. DOI: 10.1007/s10916-018-1121-4. [Online]. Available: <https://doi.org/10.1007/s10916-018-1121-4>.
- [19] M. Du, Q. Chen, J. Chen, and X. Ma, “An optimized consortium blockchain for medical information sharing,” *IEEE Transactions on Engineering Management*, vol. 68, no. 6, pp. 1677–1689, Dec. 2021. DOI: 10.1109/tem.2020.2966832. [Online]. Available: <https://doi.org/10.1109/tem.2020.2966832>.
- [20] G. Tripathi, M. A. Ahad, and S. Paiva, “S2hs- a blockchain based approach for smart healthcare system,” *Healthcare*, vol. 8, no. 1, p. 100 391, Mar. 2020. DOI: 10.1016/j.hjdsi.2019.100391. [Online]. Available: <https://doi.org/10.1016/j.hjdsi.2019.100391>.
- [21] A. Lakhan, M. A. Mohammed, J. Nedoma, R. Martinek, P. Tiwari, and N. Kumar, “DRLBTS: Deep reinforcement learning-aware blockchain-based healthcare system,” *Scientific Reports*, vol. 13, no. 1, Mar. 2023. DOI: 10.1038/s41598-023-29170-2. [Online]. Available: <https://doi.org/10.1038/s41598-023-29170-2>.
- [22] A. Abbas and S. U. Khan, “A review on the state-of-the-art privacy-preserving approaches in the e-health clouds,” *IEEE Journal of Biomedical and Health Informatics*, vol. 18, no. 4, pp. 1431–1441, Jul. 2014. DOI: 10.1109/jbhi.2014.2300846. [Online]. Available: <https://doi.org/10.1109/jbhi.2014.2300846>.

- [23] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, “Blockchain distributed ledger technologies for biomedical and health care applications,” *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Sep. 2017. DOI: 10.1093/jamia/ocx068. [Online]. Available: <https://doi.org/10.1093/jamia/ocx068>.
- [24] A. Zhang and X. Lin, “Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain,” *Journal of Medical Systems*, vol. 42, no. 8, Jun. 2018. DOI: 10.1007/s10916-018-0995-5. [Online]. Available: <https://doi.org/10.1007/s10916-018-0995-5>.