

Privacy-preserving Healthcare Data Management System using Blockchain Technology

by

Abir Arshad

18101634

Devamitra Das

18101413

Md.Mostafizur Rahman

18101415

Md.Tarik-Ul-Mostafi

18101399

Swapnil Biswas

18101159

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

Department of Computer Science and Engineering
Brac University
May 2022

© 2022. 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.

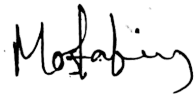
Student's Full Name & Signature:



Abir Arshad
18101634



Devamitra Das
18101413



Md. Mostafizur Rahman
18101415



Md. Tarik-Ul-Mostafi
18101399



Swapnil Biswas
18101159

Approval

"PRIVACY-PROTECTING HEALTHCARE DATA MANAGEMENT SYSTEM USING BLOCKCHAIN TECHNOLOGY" is the title of the thesis/project Blockchain Based Healthcare Management System, submitted by

1. Abir Arshad (18101634)
2. Devamitra Das (18101413)
3. Md. Mostafizur Rahman (18101415)
4. Md. Tarik-Ul-Mostafi (18101399)
5. Swapnil Biswas (18101159)

Of Summer, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on June 15, 2022.

Examining Committee:

Supervisor:
(Member)

Md. Sadek Ferdous

Md Sadek Ferdous, PhD
Associate professor
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chairperson)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

In recent years, blockchain technology has gotten plenty of attention, with rising interest in an exceedingly type of way resembling as-Banking, Telecommunication, IoT, aid etc. Each different sector, Blockchain has additionally completed a massive task in medical aid specialties. Antecedently the standard EHR- based mostly systems were aggravated by several knowledge loss hazards, security and unchangeableness accord for the aid records, there was a niche between communications among varied brought about hospitals and what is more the reclamation of the data was thus uncomfortable. Blockchain has lessened these issues. Varied beginning points for Blockchain technology within the aid trade area unit the main target of this report. A redistributed info that is ever delayed thus far presents several benefits to the aid industry. These benefits get particularly overwhelming, once many alternative parties want access to identical data. Through a shared network infrastructure, totally different aid specialists will enter identical data. This can additionally allow the event of a brand-new category of Blockchain- grounded exercises in aid that may loosen wasted coffers and break vital useful issues with extra secured infrastructure. Either with the assistance of good contracts it's going to be potential to alter a time- overwhelming method properly. This text describes a patient- doctor-centric construct for a redistributed aid management system that has a blockchain- based mostly on EHR and good contracts written in JavaScript. An acting epitome supported Hyperledger cloth and melodist technology has additionally been developed, guaranteeing the planned model's security. Cyber criminals have been increasingly interested in healthcare data. Decentralization could help to lessen the annihilating effects of healthcare data. A peer-to-peer (P2P) network allows for decentralization, allowing multiple parties to store and conduct computation while keeping sensitive health data private. Blockchain technology is based on a decentralized or distributed method, which assures that its use is transparent and trustworthy. This study describes a patient-centric healthcare data management system that employs Blockchain as a storage medium to ensure anonymity. The use of cryptographic methods to safeguard patient data ensures pseudonymity. Healthcare providers are increasingly using Internet of Things (IoT)-based wearable technologies to speed up diagnosis and treatment. Hundreds of billions of sensors, devices, and vehicles have been connected to the Internet in recent years. Remote patient monitoring is one such technology that is now widely used in the treatment and care of patients. These technologies, on the other hand, pose serious privacy and security problems when it comes to data transfer and logging. These medical data security and privacy issues could cause a delay in treatment, possibly putting the patient's life in jeopardy. We propose using a blockchain to manage and analyze healthcare large data in a secure manner. Blockchains, on the other hand, are computationally expensive, necessitate high bandwidth, and require additional computational capacity, making them unsuitable for most resource-constrained IoT devices aimed for smart cities. In this paper, we attempt to address the aforementioned concerns with blockchain and IoT devices. We offer a new framework of modified blockchain models that are ideal for IoT devices and rely on the network's distributed nature as well as other privacy and security features. Our model's added privacy and security features are based on advanced cryptographic primitives.

Keywords: Blockchain, PPHDM, DApp, Smart Contact, Privacy, Healthcare, Medical Records, Data Securing

Acknowledgement

First and foremost, we give thanks to Allah for allowing us to finish our thesis without any serious setbacks.

Second, we would like to thank our supervisor, Dr. Md. Sadek Ferdous sir, for his invaluable assistance and advice. He was always willing to assist us.

Finally, without our parents' support, it may not be achievable. We are currently on the verge of graduating thanks to their generous assistance and prayers.

Table of Contents

Declaration	i
Approval	ii
Abstract	iii
Acknowledgment	v
Table of Contents	vi
List of Figures	viii
List of Tables	ix
Nomenclature	ix
1 Introduction	1
1.1 Background	1
1.2 Problem Statement	2
1.3 Research Objective	2
1.4 Report Structure	3
2 Literature Review	4
3 Threat Modeling and analysis	11
3.1 Threat Modeling	11
3.2 Requirement Analysis	12
4 Architecture	14
4.1 Smart-Contract Supported Blockchain Platform	14
4.2 DApp	15
4.3 Stakeholders	16
4.4 Cloud and Local Data	17
5 Platforms, Languages and Implementation	18
5.1 Chaincode or Smart Contract	18
5.2 DApp	19

6	Protocol Flow	20
6.1	Communication Protocol between Patient and Doctor:	21
6.2	Communication Protocol between Patient and Hospital or Laboratory:	22
6.3	Communication Protocol among Patient and Insurance Company:	24
6.4	Communication between Pharmacy and Patient:	25
7	Discussion	27
7.1	Motivation of the Proposed Architecture	27
7.2	Advantages of this System	27
7.3	Limitations	27
8	Conclusion	29
8.1	Future Work	29
	Reference	30

List of Figures

4.1	Smart-Contract Supported Blockchain Platform	15
6.1	Data flow diagram of registration and login.	20
6.2	Login Page	21
6.3	Register Page	21
6.4	Communication Protocol between Patient and Doctor	22
6.5	Data Flow between hospital/laboratory and patient	23
6.6	Hospital Page	24
6.7	Insurance Page	25

List of Tables

2.1	Comparison of Referred Papers	9
2.2	Privacy and Security Table of Referred Papers	10
3.1	Threat Model and Analysis	13

Chapter 1

Introduction

1.1 Background

Blockchain Technology has begun a new chapter in the current period of science and technology with the emergence of security. As a decentralized system, blockchain is an immutable, cryptographically secured ledger that allows users to write once and retrieve many different types of data structures from different sources [1]. It saved all of the information or database records into the digital ledger via peerto-peer interactions. To everybody, it has proven to be a trustworthy, stable, and secure platform [2]. The blockchain technology enables for the prevention of database assaults of any form. Due to its openness, blockchain technology is a transparent system in which every public key holder can see what is going on on the blockchain network. Everyone on the blockchain network can see anything, but they can't tamper with them [3][4]. There is no single point of failure in the Blockchain network because all data is distributed, resulting in an intrinsic backup mechanism. Every single Blockchain node has a copy of the copied data. As a result, the volume of transactions between database systems is reduced, and the strain is reduced as well. Furthermore, data recorded in the blockchain is immutable, meaning it cannot be changed or erased once it has been saved. [4] [5]. Handling cash, employees, patients, legal diculties, logistics, inventories, and other procedures are all part of healthcare management. Medical workflows are usually made up of a number of conditional statements that can be organized as a series of recurring tasks related to patient care. These are aimed at providing greater internal controls, increased eciency, compliance, and productivity inside hospitals and other healthcare service providers, as well as minimizing risk, work cycles, and expense. In this article, several medical workflows are built for distinct healthcare management application areas. It's critical to determine whether the current study meets the expectations for blockchain technology in healthcare. The purpose of this study is to thoroughly investigate, evaluate, and summarize current peer-reviewed articles that demonstrate how blockchain has been utilized to improve health-care processes and services. In addition to reviewing the data, we intend to oer an overview of what has been done, what is known, and potential future directions on this topic. To summarize, using blockchain technology into the medical health-care system will advance the industry and ensure that all data is properly protected. Additionally, it will save users money and time.

1.2 Problem Statement

The advancement of technology has elevated the globe to a whole new level. It has also had an impact on healthcare facilities. In order to treat their patients, hospitals are now implementing innovative technology. Many diseases are detected and treated using a variety of equipment. Every patient's data is now stored in a database that is simple to use and retrieve. To keep track of patients' information, several healthcare facilities have implemented Electronic Healthcare Records (EHR). The number of users is steadily increasing. There is a lot more data now than there was previously. The authority found managing the EHRs difficult, and there were also data loss and security concerns. Many issues have been raised as a result of the EHR's security issue, and blockchain has emerged with its ledger system to answer all of these questions. So far, a number of systems and infrastructures that are patient-centric have been presented. The primary goal of their efforts has been to protect patients' electronic health records (EHRs). In this work, a system will be described to secure the entire records of the Healthcare management system, with each end user annexing a security ledger [1][2][6][7]. Potential Personally Identifiable Information (PII) will be utilized to identify each type of user in the system, and the data will be built using a selective disclosure mechanism so that no other users can access the entire data except those who have been granted access. The preferred end users will be given explicit tolerance for data use, while the rest of the stakeholders will be given zero-knowledge proof. The EHR's security will be improved by adding multisign to the blocks.

1.3 Research Objective

The major purpose of this project is to use blockchain technology to create a security mechanism for a decentralized database that will aid in the development of a smart healthcare management system. In general, blockchain is a digital ledger that uses cryptographic blocks to record and store data about transactions that have occurred on its platform. We will learn about blockchain technology and the usefulness of this technology in science as a result of this study. The key research goals are listed below,

- To gain a better understanding of how blockchain technology can be used to create a smart healthcare management system.
- To identify and formulate requirements to address the security and privacy hazards of a privacy-preserving healthcare management system.
- Develop a smart healthcare management system based on the identified requirements.
- Evaluate the resulting smart healthcare management system's performance and security.

In our Pre-Thesis I, we completed the first bulleted research objective point from the above-mentioned objectives. We successfully covered the second bulleted item in Pre-Thesis II. In the next section, we'll go over the rest of our goals in order to create a full system that follows our concept.

1.4 Report Structure

The study is divided into eight sections. Firstly the paper introduces blockchain technology and the history of PPHDM, as well as the problem statement and research objectives, were introduced in Chapter 1. In addition, similar studies from other research publications were evaluated in Chapter 2. Threat modeling, requirement, and comparison analysis were also presented in Chapter 3. In Chapter 4, the architecture was also suggested, which included a blockchain platform with smart contracts, a DApp, stakeholders, cloud and local data. Chapter 5 covered coding platforms, code languages, and the implementation of our suggested system. The protocol flow of the proposed system is then discussed in Chapter 6, which includes communication protocols between patients and doctors, patients and hospitals, patients and insurance companies, and patients and pharmacies. The motives, advantages, and limits of the suggested design were examined in Chapter 7. Finally, the research was completed with future work scopes.

Chapter 2

Literature Review

World nowadays has become so small with the help of technology and life has become easier than before because of the fast development or growth of technology. Everything can be done with the tap of our finger. With the advancement of technology life has become virtual and in this virtual life security is the most important issue. Then again blockchain has aroused with its decentralized, immutable, distributed ledger, encryption, and peer-to-peer network features. Satoshi Nakamoto invented this technology for the purpose to serve as a public transaction ledger using the bitcoin cryptocurrency. Bitcoin was the first invented cryptocurrencies. To handle this cryptocurrency no central authority was needed and also to solve the double-spending problem was the reason to invent this. In this technology there are some blocks connected with each other that create a chain and every block has a connection with the previous block by sharing a hash.

Contribution of Blockchain technology has developed a lot in the past few years. Now it's a strong security system. Blockchain technology has gotten a lot of attention, with rising interest in a variety of industries, including healthcare. The interest and momentum of Blockchain Technology has now extended to healthcare information technology. Blockchain is a distributed, secure database that does not require a central authority or administrator to operate. Blockchain has also garnered interest as a platform to improve the authenticity and transparency of healthcare data through many use cases, from maintaining permissions in electronic health records (EHR) to streamlining claims processing. Blockchain technology provides a platform that might be used in a variety of health-care applications. Many organizations have offered solutions that have the potential to improve healthcare data transparency and operational efficiency while still in the early stages of design and development. The future of this technology in healthcare and other industries is still being written, and the applications in research and clinical care are not yet established [1].

In [2], they have been introduced with a patient-centric healthcare system framework. The framework empowers a patient with such access control for seamless queries. A structure of blockchain is used as a tracker to track the history by using a distributed ledger. Without the interruption of the third-party by the consensus rule of the network ensures the honest transaction between the end users. The data that is on the blockchain cannot be changed which makes the blockchain so secure and trustworthy to everyone. The combination of the cryptographically secure encryption function and the common investment of the network peer via the difficulty and cost of the consensus mechanism employed by the network. The main advan-

tage of the blockchain is the transparency, security and instant transaction speed of this technology which makes it unique. A complex and highly connected EHR can operate by the help of blockchain.

Again due to globalization many have adopted the blockchain technology in order to secure their system from unwanted tampering. Supply chain is one of the systems. For the security of the supply chain it is a great deal of which cannot be compromised. Blockchain technology is potentially used in hospitals which have been started for testing as pilot projects globally. There are 4 hospitals where the pilot project is now being implemented in the USA and using virtual private networks Ethereum is managing data access [4].

There might be some fault errors or delays happening while recording data and using blockchain to reduce fraud and errors, the delays from paperwork's, improve the management inventory, rapidly identify issues, increase the consumer trust. The capacity to utilize smart contracts to automate processes and reduce costs is also a crucial mechanism by which blockchain technology could help achieve supply chain performance enhancement [7].

In [9], since the introduction of blockchain through Bitcoin, there has been continuing study into broadening its applications to non-financial use cases. Healthcare is one area where blockchain is expected to have a significant impact. Health informatics researchers and practitioners are always fighting to keep up with research in this subject, which is still relatively new but growing rapidly. This study presents the results of a systematic review of current research into the use of blockchain technology in healthcare. The research methodology is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines and a systematic mapping study process, in which a well-designed search protocol is used to identify, extract, and analyze all relevant publications using four scientific databases. The study's objectives were to identify blockchain technology's applications in healthcare, as well as example applications developed for these applications, challenges and limitations of blockchain-based healthcare applications, current approaches to developing these applications, and future research areas.

As per [10], in any healthcare system relationship between patients, doctors need to be secured and it can be done by using blockchain technology. The adoption of IoT has the potential to improve patient care quality. To maintain secure communication, interactions between devices must be verified. Using blockchain technology, the suggested architecture offers efficient decentralized authentication. It is clear that authentication is critical for secure communication in hospital networks.

Hackers and crackers, both amateur and professional, are frequently attacking electronic data in today's information security world. The security of a patient's electronic medical record (EMR) in a hospital management system is critical and must be addressed immediately. To accomplish this task efficiently, a blockchain framework called "Medichain" was built from the ground up, containing all of the essential blockchain features for securing patient data. Each blockchain block maintains a set of patient information records [11].

Again in [12], Remote Patient Monitoring (RPM) becomes a more powerful and versatile patient observation tool. The majority of RPM has a specific application area that helps doctors to get more information. Blockchain technologies are employed in electronic medical record systems, insurance claims, billing administration and other areas of hospitals.

Three types of Blockchain were introduced by Satoshi Nakamoto. Genesis block, valid block, Orphan block are those three blocks. While introducing Bitcoin Nakamoto first mined the Genesis block and that after that every block that is being mined are called valid blocks. A block is only added to the blockchain and distributed to other nodes on the network after the network reaches consensus. These blocks allow any cryptocurrencies to be operated and transacted. Some blocks that were valid but somehow lost or got orphaned from the part of the main blockchain network are known as Orphan blocks. Two miners trample out the same block at the same time, or with ample power of hashing an attacker might reverse the transaction which is the reason for blocks to get lost or orphaned.

With some challenges some solutions have been given regarding the healthcare blockchain [13]. The main idea is how to handle big data in the healthcare blockchain sector. Many basic ideas about blockchain are given here to understand easily about the blockchain. Another three types of block are shown here [14], which are Public, Private and Consortium. Also a comparison between the Consensus algorithms has been presented in [13].

A Global Fintech Report according to PwC, mentioned that from a company more than 500 employees or 55 percent employees are agreeing to take blockchain as part of their production system by 2018 and in 2020 the rate increased to 77 percent [15]. An infrastructure of a complete platform for patient data authentication and sharing among stakeholders has been provided by Azaria et al. [16]. For gathering consensus of the stakeholders, they have used Proof-of-Work (PoW) also there is incentive based data sharing and authentication for the system.

There is another system proposed which is a community-based network architecture for a healthcare exchanging mechanism by Peterson et al. [17]. Here the data can be accessed only for a particular node if the community members accept the data structure and semantics.

Because of the rapid development or advancement of technology, the world has become much smaller and living has become much easier than before. With a single tap of our finger, we can accomplish anything. With the advancement of technology, life has become virtual, and security is the most critical concern in this virtual world. The decentralized, unchangeable, distributed ledger, encryption, and peer-to-peer network aspects of blockchain, on the other hand, have piqued interest. This technology was created by Satoshi Nakamoto to serve as a public transaction ledger for the bitcoin cryptocurrency. Bitcoin was the first cryptocurrency to be created. There was no need for a central authority to administer this coin, and it was created to overcome the problem of double-spending. In this technology, several blocks are linked together to form a chain, and each block shares a hash with the previous block.

In the last several years, Blockchain technology has made a significant contribution. It's now a powerful security system. Blockchain technology has gained a lot of press, and it's gaining traction in a variety of fields, including healthcare. Blockchain Technology's popularity and momentum has now spread to healthcare information technology. Blockchain is a decentralized, secure database that runs without the need for a central authority or administrator. Many use cases, ranging from retaining permissions in electronic health records (EHR) to simplifying claims processing, have sparked interest in blockchain as a platform for improving the validity and openness of healthcare data. Blockchain technology provides a platform for a mul-

titude of healthcare applications. While still in the design and development stages, many firms have presented solutions that have the potential to increase healthcare data openness and operational efficiency. This technology's future in healthcare and other industries is still being written, and its applications in research and clinical treatment have yet to be determined [1].

They were introduced to a patient-centered healthcare system paradigm in [2]. The framework provides such access control to a patient for seamless inquiries. The blockchain structure is utilized as a tracker to track the history of a distributed ledger. The honest transaction between the end users is ensured without the interruption of a third-party by the network's consensus rule. The data on the blockchain cannot be modified, making it extremely secure and trustworthy to all parties involved. The combination of a cryptographically safe encryption function and the network peer's shared investment via the network's consensus mechanism's complexity and expense. The blockchain's key advantage is its transparency, security, and rapid transaction speed, which distinguishes it from other technologies. Blockchain can be used to run a sophisticated and interconnected EHR.

Because of globalization, several companies have implemented blockchain technology to protect their systems against tampering. One of the systems is the supply chain. There is a lot that cannot be compromised in terms of supply chain security. Blockchain technology could be employed in hospitals that are currently being tested as pilot projects around the world. In the United States, the pilot project is currently being implemented in four hospitals using virtual private networks. Data access is managed via Ethereum [4].

While capturing data and using blockchain to eliminate fraud and errors, the delays from paperwork, better inventory management, quickly identify issues, and build consumer trust, there may be some fault errors or delays. The ability to use smart contracts to automate procedures and save money is another important way that blockchain technology can help improve supply chain performance [7].

Since Bitcoin's inception, there has been ongoing research into expanding blockchain's uses to non-financial use cases [9]. One sector where blockchain is predicted to have a large influence is healthcare. Researchers and practitioners in health informatics are always battling to keep up with research in this field, which is still relatively new but fast expanding. The findings of a comprehensive review of existing research into the usage of blockchain technology in healthcare are presented in this article. The research methodology is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines and a systematic mapping study process, in which all relevant publications are identified, extracted, and analyzed using four scientific databases using a well-designed search protocol. The study's goals were to identify blockchain's uses in healthcare, as well as examples of apps produced for these applications, obstacles and limitations of blockchain-based healthcare applications, existing ways to develop these applications, and future research areas.

According to [10], in every healthcare system, the relationship between patients and doctors must be protected, which can be accomplished with blockchain technology. The use of IoT has the potential to improve the quality of patient care. Interactions between devices must be checked in order to preserve secure connection. The proposed architecture uses blockchain technology to provide efficient decentralized authentication. Authentication is clearly necessary for secure communication in hos-

pital networks.

In today's information security world, amateur and professional hackers and crackers often target electronic data. In a hospital management system, the security of a patient's electronic medical record (EMR) is crucial and must be addressed immediately. To make this effort go as smoothly as possible, a blockchain framework dubbed "Medichain" was created from the ground up, with all of the necessary blockchain capabilities for securing patient data. A collection of patient information records is kept in each blockchain block [11].

Remote Patient Monitoring (RPM) becomes a more powerful and versatile patient observation tool once again in [12]. The majority of RPMs have a dedicated application area that assists doctors in gathering additional data. Electronic medical record systems, insurance claims, billing administration, and other departments of hospitals use blockchain technology.

Satoshi Nakamoto introduced three forms of Blockchain. Those three blocks are the Genesis block, the Valid block, and the Orphan block. When introducing Bitcoin, Nakamoto first mined the Genesis block, following which all subsequent blocks are referred to as Valid blocks. After the network obtains consensus, a block is added to the blockchain and distributed to other nodes on the network. These blocks enable the operation and transaction of any cryptocurrency. Orphan blocks are blocks that were valid but were lost or orphaned from the main blockchain network for whatever reason. Two miners stomp the same block at the same time, or an attacker with enough hashing power reverses the transaction, resulting in blocks being lost or orphaned.

Regarding the healthcare blockchain, various solutions have been provided in response to particular issues [13]. The central concept is how to deal with massive data in the healthcare blockchain industry. Many fundamental concepts of blockchain are presented here for easy comprehension. There are three other sorts of blocks shown here [14]: public, private, and consortium. In [13], a comparison of the Consensus algorithms is also offered.

According to PwC's Global Fintech Report, companies with more than 500 employees are agreeing to adopt blockchain as part of their production system by 2018, with the rate increasing to 77 percent by 2020. [15].

Azaria et al. [16] built the foundation for a full platform for patient data authentication and exchange across stakeholders. They used Proof-of-Work (PoW) to obtain stakeholder consensus, and there is also incentive-based data exchange and authentication for the system.

Another approach, proposed by Peterson et al. [17], is a community-based network design for a healthcare exchange mechanism.

Reviewing twenty nine papers related to the health care management system we made a table and in Table 2.1 it describes the type, consensus, software module, structure, insensitive mechanism, scalability, language and cost.

In Table 2.2 describes about the impression attack, session key disclosure attack, perfect forward secrecy, replay attack, privileged attack, single point of failure, mutual authentication and bottleneck.

Table 2.1: Comparison of Referred Papers

Ref	Type	Consensus	Software Module	Structure	51 percent Attack	Incentive mechanism	Scalability	Language	Cost
24. EMR related	Public	PoW	Backend Library, Ethereum Client, EHR Management, Database Gatekeeper	Permissionless	N/A	N/A		Solidity	Yes
25. related	Consortium	DPoS	EMR Management, Ethereum Client	Permissioned	Yes	N/A		Solidity	Yes
26. Both EMR and EHR related	Private	PoA	Ethereum Client, DB Manager, EMRs Interface, Cipher/Decipher Management, Records Evaluation Manager	Permissioned	N/A	Yes		Go	Yes
27. PHR related	Private	PoW	IPFS, Trusted oracles, reputation system, proxy re-encryption	Permissioned	N/A	Yes	High	Solidity	Yes(High)
28. EMR related	Public	N/A	CHG, GA, Database	Permissioned	N/A	Yes	High	Solidity	Yes(High)
29. EMR related	Private	PoW	N/A	N/A	N/A	N/A	Low	Python	No
30. PHR related	Private	N/A	Ethereum Swarm, Ethereum Client,	Permissioned	Yes	N/A	Low	Solidity	Yes(Low)
31. EMR related	Private	N/A	MIRACL, cpabe toolkit	Permissioned	No	N/A	Low	N/A	Yes
32. Cloud-Based Medical Record	Public	N/A	EMR Client	Permissioned	No	N/A	Low	N/A	High
33. EMR related	Public	N/A	Ethereum, IPSC	Permissioned	Yes	N/A	High	Solidity	Yes(Ether)
34. EHR related	Private	N/A	MIRACL	Permissioned	N/A	N/A	High	Python	Yes
35. EMR related	Private	PoW	Ethereum Client, SQL query, Database Gatekeeper, EMR Manager, Backend Library	Permissioned	N/A	Yes	High	Solidity	Yes
36. EMR, EHR related	Public	N/A	N/A	Permissionless	N/A	Yes	Low	N/A	Yes
37. EHR related	Public	N/A	Ethereum Client	Permissionless	N/A	N/A	High	Solidity	Yes
38. EMR related	Hybrid	PoA	Real Private Blockchain, Bitcoin Client	Permissioned, Permissionless	N/A	N/A	High	Python	No
39. Python based query application	Private	PoA	N/A	Permissioned	Yes	N/A	High	Go, Python, Django	Yes
40. EMR related	Private	DPoS, PoW	IPFS, Multiminer	Permissioned	N/A	N/A	Low	C++	No
41. EMR related	Private	N/A	Ethereum Client, MedRec API, Database Gatekeeper, SQL query	Permissioned	N/A	N/A	High	Solidity	Yes(Low)
42. EMR related	Private	N/A	Spyder IDE, FLASK(0.12.2), Postman API Framework(7.29.1)	Permissioned	N/A	N/A	High	Python	No
43. EMR related	Consortium	N/A	Hyperledger Caliper, Ethereum API, Hyperledger Fabric API	Permissioned, Permissionless	N/A	N/A	High	Solidity	Yes
44. EMR related	Public	N/A	Real Private Blockchain, Bitcoin Client	Permissioned	N/A	N/A	Low	Low	No
45. EHR related	Private	PoW	Backend Library, Ethereum Client, EHR Management, Database Gatekeeper	Permissionless	N/A	N/A	High	Solidity	Yes
46. EMR, EHR related	Public	N/A	N/A	Permissioned	N/A	N/A	High	Python	Yes
47. EHR related	Public	N/A	Ethereum, Hyperledger Fabric API	Permissioned	Yes	N/A	Low	Python, HTML	Yes
48. EHR related	Public	N/A	Ethereum, Hyperledger Fabric API	Permissioned	Yes	N/A	Low	Python, HTML	Yes
49. EMR, EHR related	Private	N/A	EMR Management, Hyperledger Fabric API, Ethereum Client	Permissioned	N/A	N/A	High	Python	Yes
50. EMR related	Public	N/A	Bitcoin Client, Ethereum Client, EMR Management	Permissioned	N/A	N/A	High	Python	Yes
51. Both EMR and EHR related	Public	N/A	EMR Management, Ethereum Client, Bitcoin Client, Hyperledger Caliper	Permissioned	N/A	N/A	High	Solidity	Yes
52. EHR related	Private	N/A	Ethereum Client, Hyperledger Fabric API,	Permissionless	N/A	Yes	Low	Solidity	No
53. Cloud-based Medical Record	Private	N/A	N/A	Permissioned	Yes	N/A	High	Python	Yes

Table 2.2: Privacy and Security Table of Referred Papers

Ref	Impersonation attack	Session key disclosure attack	Anonymity	Perfect forward secrecy	Replay attack	Privileged attack	Single point of failure	Mutual authentication	Bottleneck
24	NO	NO	YES	NO	YES	NO	NO	NO	NO
25	NO	YES	YES	YES	NO	NO	NO	YES	NO
26	YES	YES	YES	YES	NO	YES	YES	YES	YES
27	NO	YES	YES	NO	NO	NO	YES	NO	NO
28	NO	NO	YES	YES	NO	NO	YES	NO	NO
29	NO	NO	YES	NO	NO	NO	NO	YES	NO
30	NO	YES	YES	YES	NO	NO	NO	YES	NO
31	YES	YES	NO	NO	NO	YES	NO	YES	YES
32	NO	YES	YES	YES	NO	NO	NO	YES	NO
33	NO	YES	YES	YES	NO	NO	NO	YES	NO
34	YES	NO	NO	NO	NO	YES	NO	YES	YES
35	NO	YES	YES	YES	NO	NO	NO	YES	NO
36	NO	NO	YES	NO	NO	NO	NO	YES	NO
37	NO	NO	YES	YES	NO	NO	NO	YES	NO
38	NO	YES	YES	NO	NO	NO	YES	NO	NO
39	YES	YES	YES	YES	NO	YES	YES	YES	YES
40	NO	YES	YES	YES	NO	NO	NO	YES	NO
41	NO	NO	YES	NO	YES	NO	NO	NO	NO
42	NO	YES	YES	NO	NO	NO	YES	NO	NO
43	NO	NO	YES	NO	NO	NO	NO	YES	NO
44	NO	NO	YES	NO	YES	NO	NO	NO	NO
45	NO	YES	YES	YES	NO	NO	NO	YES	NO
46	YES	YES	YES	YES	NO	YES	YES	YES	YES
47	NO	YES	YES	NO	NO	NO	YES	NO	NO
48	NO	NO	YES	YES	NO	NO	NO	YES	NO
49	NO	NO	YES	NO	NO	NO	NO	YES	NO
50	NO	YES	YES	YES	NO	NO	NO	YES	NO
51	YES	NO	NO	NO	NO	YES	NO	YES	YES
52	NO	YES	YES	YES	NO	NO	NO	YES	NO
53	NO	YES	YES	YES	NO	NO	NO	YES	NO

Chapter 3

Threat Modeling and analysis

Decision tree algorithm is a very popular way to design a predictive modeling. Decision tree builds classification or regression models in the form of a tree structure. It breaks down a data set into smaller and smaller subsets. We offer a threat model (Section 3.1) and examine a variety of functional, security, and privacy requirements (Section 3.2) for a blockchain-enabled EHR management system in this section.

3.1 Threat Modeling

For every system model there might be some threats and for mitigating or canceling them models are needed. These models are one of the essential parts for any type of system to identify the threats. Identifying the threats mitigation or cancellation steps are taken to secure the system. In our work for developing a secure patient Data Management system we have chosen ‘STRIDE’, a well-established threat model developed by Microsoft. This model encodes different security threats. Our modeled threats using the above-mentioned threat model discussed below.

- **T1-Spoofing Identity:**
Someone can act as an authorized user (Attacker) of the system with illegal or harmful intentions (e.g., Consulting Doctors through online chat with fake ailment).
- **2-Tampering with Data:**
Attacker can change the data of any entity or entities that are stored in the database of the system (e.g., For Doctor- Attacker can change the prescription of patients, For Patients- Attacker can change the ailment history of any patients which makes the doctors wrong meds for patients.)
- **T3-Repudiation:**
An attacker can repudiate invalid or false transactions for the medicines or for the insurance companies. Also, they can repudiate after bringing certain changes in the system’s database.
- **T4-Information disclosure:**
Any kind of sensitive data can be published or leaked to the attackers.
- **T5-Denial of Service (DoS):**
The data of the system (e.g., Patient history, medicine store document for tracking medicines, Insurance Company’s patient data) could be flooded by an attacker.

- T6-Elevation of privilege:
Attacker can elevate his privilege by using malicious software without the authorized user noticing the issue.

3.2 Requirement Analysis

In this part, we are going to uphold some functional requirements indicating the core functions of the system that users can use. Also, we will discuss some security and privacy requirements that can mitigate or cancel the threats we detected.

- Functional Requirement (FR):
Requirements that state the functionalities of the system or the functions stakeholders can perform are functional requirements. Below we stated these functional requirements of our system,
F1. Patients can directly take appointments for doctors at any time without any third party through this system.
F2. Patients can purchase medicines from stores from home and can pay the bill through online payment or cash on delivery.
F3. Patients can permit access to the stakeholders as per request.
F4. Stakeholders (excluding patients) can access data within the timeframe that the owner has set.
- Security Requirements (SR):
Here we are going to present a set of Security requirements that will mitigate or cancel the threat we mentioned above,
S1. Our system will ensure that each stakeholder from each sector will have a different identity to differentiate them from others (e.g. Patient, Doctor, Medicine Store Keeper, Insurance Company agents). This will mitigate T2.
S2. Each user will have an authentic ID to avail the system securely. Threat T1 is mitigated by this.
S3. Patients' health records will be visible to only doctors and insurance companies but only the doctors and patients will have the edit access of the records by using authentic ID. This will mitigate T2, T3 and T5.
S4. For updating the record doctor needs patient permission and again any patient wanting to update his/her own records need doctor approval. Thus T4 can be mitigated or can be canceled.
S5. Every request will be logged and immutable in the system. This will mitigate T6.
- Privacy Requirement (PR):
Privacy requirements are one of the most important requirements to mitigate the threats and build a secure system. The Requirements are stated below,
P1. Selective Disclosure Property must be implemented into the system so that the user can have full control over the data.
P2. Explicit consent of the owner will be shared with the data.
P3. Zero-Knowledge Proof or Protocol will be implemented in the system to verify data of any user without additional information.

Table 3.1: Threat Model and Analysis

Threat	Requirement(s)	Solution
T1	S2	Mitigation
T2	S1,S3	Mitigation
T3	S3	Mitigation
T4	S3,S4	Cancelation
T5	S3	Mitigation
T6	S5	Mitigation

Chapter 4

Architecture

In order to handle the distinguished security, all the privacy issues related with the system and to attain all the requirements (presented in Section-II), we have proposed an architecture rooted on Smart-Contract supported Blockchain which is illustrated in Figure 1. A decentralized blockchain system secures not only money transactions, but also many other components such as data and a time-stamping recording mechanism, as well as strong integrity and immutability support. Furthermore, a smart-contract enabled blockchain system enables the deployment of complex and immutable logic within a blockchain that may be activated autonomously via transactions. Keeping all the essential requirements we have proposed this smart-contract supported private blockchain network fully decentralized.

Our proposed architecture includes the smart-contract supported blockchain platform in Section 3.1, DApp (Decentralized Application) and Cloud Storage in Section 3.2 respectively. Also, we scrutinize the properties of the abovementioned components in their respective sections along with their inter-component interactions.

4.1 Smart-Contract Supported Blockchain Platform

According to the architecture mentioned in Figure 1 the blockchain platform is the central component. Blockchain platforms can be public or can be private. Although public blockchain systems are more secure, they are still highly slow, require a lot of energy, are available to everyone, and have a high cost to process and store data in a SC enabled public blockchain (e.g., Bitcoin, Ethereum) [17][18]. Private blockchain systems, on the other hand, are private and quick, with no energy consumption issues, and give a respectable level of security. As we do not want to publish the patients records to everyone so we have implemented this private blockchain.

Talking of private blockchain there are lots of private blockchain platforms. Hyperledger Fabric [21], Hyperledger Sawtooth [22], Quorum, and others are examples of private blockchain platforms. Hyperledger Fabric, on the other hand, is now the most stable and widely used private blockchain platform [23]. It also offers a unique channel concept, which allows several blockchains to coexist in the same network, providing a privacy layer for different companies. As a result, during the implementation process, Hyperledger Fabric was chosen as our preferred blockchain solution. Peers, endorsers, and orderers are some of the network entities used by Fabric. In

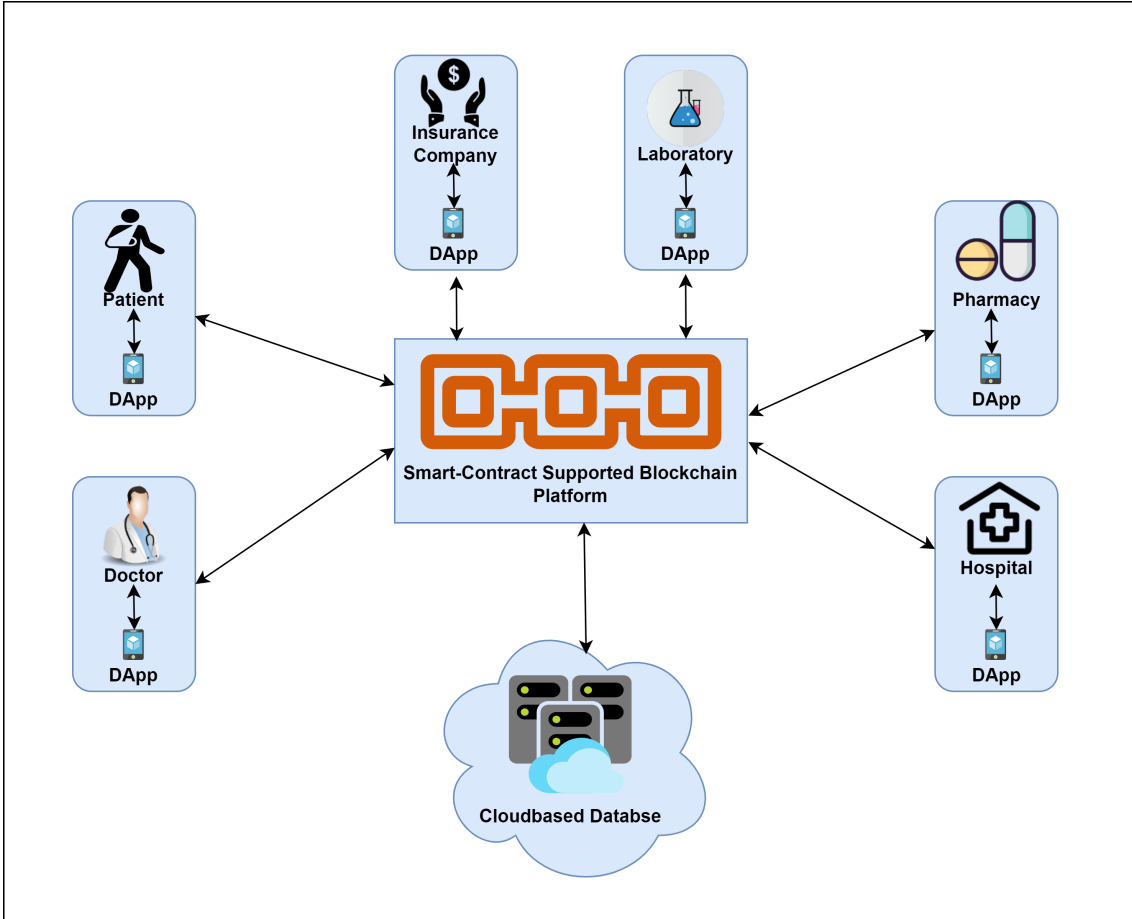


Figure 4.1: Smart-Contract Supported Blockchain Platform

Fabric jargon, a smart-contract is referred to as a chaincode, and it can be triggered using transactions. Peers are used for submitting transaction requests and then it forwarded to endorsers, lastly after getting verified it goes to order(s). The Orderer uses the transaction to generate a block, which is subsequently returned to the endorsers and peers and added to the blockchain, modifying the state of the ledger or updating after pushing or popping data. All of the entities (peers, orderers, and endorsers) are registered and validated through the Membership Service Provider, a Fabric-specific special entity (MSP). This ensures that the blockchain network is only accessible to authorized entities [23]. The smart-contract or chaincode of our proposed blockchain system has been developed with an open-source programming language GO. A smart contract is a self-executing contract in which the conditions of the buyer-seller agreement are put directly into lines of code. The code, as well as the agreements it contains, are disseminated throughout a decentralized blockchain network. This meets most of our requirements and helps to build a highly secure system.

4.2 DApp

Decentralized applications (DApp) are digital programs or applications that run on a blockchain or peer-to-peer (P2P) network of devices rather than on a single device. DApps exist outside of a single authority's jurisdiction and control. In our

architecture we have introduced DApp as the bridge between stakeholders and the blockchain platform, because no stakeholders can connect directly to the blockchain platform for the data transaction. Moreover, DApp manifests APIs (Application Programming Interfaces) to the respective stakeholders. Every stakeholder who utilizes these APIs to submit any request (e.g., storing data or asking for data) to the DApp uses the Security Assertion Markup Language, or SAML interface. After this the DApp converts these requests into blockchain transactions, which are then sent to the blockchain via a node. Each of these transactions effectively calls a SC logic, which is subsequently followed by the regular flows.

In an effort to develop the DApp for our proposed model we have used Node.js along with Express [20][21]. Node.js is a JavaScript runtime environment that is open-source and cross-platform. On the other hand, Express is a Node.js web application framework that offers a comprehensive range of functionality for both web and mobile apps. Fabric includes all of the necessary APIs for interacting with Node.js applications. Every stakeholder has been integrated with the DApp in such a way that they 4.3 Stakeholders Each peer node that is connected to the blockchain platform through DApp are the stakeholders of our system. These stakeholders are Patients, Doctors, Hospital, Insurance company, Government, Pharmacy. Self-sovereign IDM will provide each stakeholder a unique ID for participating into the blockchain network. Every stakeholder will be assigned to a distinct group in order to identify them based on their IDs (Such as- the id of patients can be started with 101, on the other hand 202 will be used at first for identifying doctors). Then, with the support of Explicit Consent, patients can grant permissions and grant data access to stakeholders. Furthermore, patients have the option of selecting data for stakeholders. They will be able to access patient data as a result of this. For instance, the Pharmacy merely needs access to the patient's prescription. Patients can now use Selective Disclosure to allow the pharmacy to access simply the prescription, which will be shown in view mode. Furthermore, if a stakeholder requests access to the PHR, they must first be recognized before seeking authorization. The system for proving one's identity to others on the blockchain network is known as Zero-Knowledge Proof. Thus, the data will be transacted between the stakeholders into the above-mentioned architecture. 20 can interact with the blockchain platform under a certain protocol.

4.3 Stakeholders

Each peer node that is connected to the blockchain platform through DApp are the stakeholders of our system. These stakeholders are Patients, Doctors, Hospital, Insurance company, Government, Pharmacy. Self-sovereign IDM will provide each stakeholder a unique ID for participating into the blockchain network. Every stakeholder will be assigned to a distinct group in order to identify them based on their IDs (Such as- the id of patients can be started with 101, on the other hand 202 will be used at first for identifying doctors). Then, with the support of Explicit Consent, patients can grant permissions and grant data access to stakeholders. Furthermore, patients have the option of selecting data for stakeholders. They will be able to access patient data as a result of this. For instance, the Pharmacy merely needs access to the patient's prescription. Patients can now use Selective Disclosure to allow the pharmacy to access simply the prescription, which will be shown in view

mode. Furthermore, if a stakeholder requests access to the PHR, they must first be recognized before seeking authorization. The system for proving one's identity to others on the blockchain network is known as Zero-Knowledge Proof. Thus, the data will be transacted between the stakeholders into the above-mentioned architecture.

4.4 Cloud and Local Data

A cloud database is a database service that is produced and accessible via the internet. It performs many of the same tasks as a traditional database, but with the extra benefit of cloud computing flexibility. To implement the database, users install software on a cloud infrastructure.

Features to look for:

- A cloud-based database service that may be accessed from anywhere.
- Allows business customers to host databases without having to purchase dedicated hardware.
- It can be controlled by the user or it can be provided as a service and managed by the supplier.
- Supports both relational and non-relational databases (including MySQL and PostgreSQL) (including MongoDB and Apache CouchDB).
- Accessed via a web interface or an API given by the vendor.

Keeping all these in mind we have used this cloud-based database to store all the PHR and data related to our infrastructure. All the data will be stored as their designated storage and managed by the cloud itself.

Chapter 5

Platforms, Languages and Implementation

In this section, we will highlight our development part that we have worked on so far. We have used Hyperledger fabric, an open source Blockchain platform. In this platform all the users are permissioned or known and authenticated to say specifically. For the development purpose we have chosen Javascript and React. Also we have used a variety of libraries used in js to build our system.

5.1 Chaincode or Smart Contract

For every blockchain network a protocol is needed to run every kind of transaction in order and with enough security. To make the system perform according to the contractor this chaincode is needed to build which will let everyone to become a node of the blockchain network and help to transact securely without any kind of hindrance. Every peer of the network has to go through this automation process and verify them.

We have built such Chaincode or SmartContract that can automates our conditions for our system. As we have implemented a system which can not only secure the electronic health record of a patient but also a secure interaction with doctors and other entities included into our system.

```
async CreateFile(ctx, key, name, downloadLink, fileHash, uploaderEmail)
const file = Key: key,
Name: name,
DownloadLink: downloadLink,
FileHash: fileHash,
UploaderEmail: uploaderEmail,
DocType: 'file';

await ctx.stub.putState(key, Buffer.from(JSON.stringify(file)));
return JSON.stringify(file);
```

Here in this code snippet we have implemented a function which is for uploading the health record of a particular stakeholder. Whenever a stakeholder uploads

his/her details it will be encrypted with an encryption algorithm. There are so many varieties of encryption algorithms and we have used SHA256 algorithm for our encryption. Thus we are securing our stakeholders records.

```
async MakeAppointment(ctx, key, userEmail, doctorEmail, appointmentDoc)
const file = Key: key,
UserEmail: userEmail,
doctorEmail: doctorEmail,
AppointmentDoc: appointmentDoc,
DocType: 'file' ;
await ctx.stub.putState(key, Buffer.from(JSON.stringify(file)));
return JSON.stringify(file);
```

```
async OrderMedicine(ctx, key, userEmail, medicineList)
const file = Key: key,
UserEmail: userEmail,
MedicineList: medicineList,
DocType: 'file' ;
await ctx.stub.putState(key, Buffer.from(JSON.stringify(file)));
return JSON.stringify(file);
```

The above two code snippets are showing two different functions of interaction with doctor and pharmaceutical securely. MakeAppointment function is used to take an appointment from doctor and the OrderMedicine function is used for ordering medicines by using the prescription. Similarly we have built our Chaincode with such functions that will automate our required conditions and let the system perform according to our requirements.

5.2 DApp

Decentralized Application is a middleware that connects the blockchain network to the backend and frontend. A DApp can use blockchain to process data and perform transactions over distributed networks. We use DApp to connect our chaincode to the front end. Users cannot directly send data to their blockchain database. It passes it on to DApp. The entire data was then saved in the database using DApp. Our DApp function was created using JavaScript.

Chapter 6

Protocol Flow

In this section, we present the protocol flow between different components in Privacy-preserving Healthcare Data Management (PPHDM). Because of its security, we used Smart-Contract backed Blockchain to connect all of the components in our architecture. First and firstly, users must register an account. He must complete the relevant information, which will be stored in a blockchain database via a DApp. The entire procedure is depicted in figures 6.1, 6.2, and 6.3.

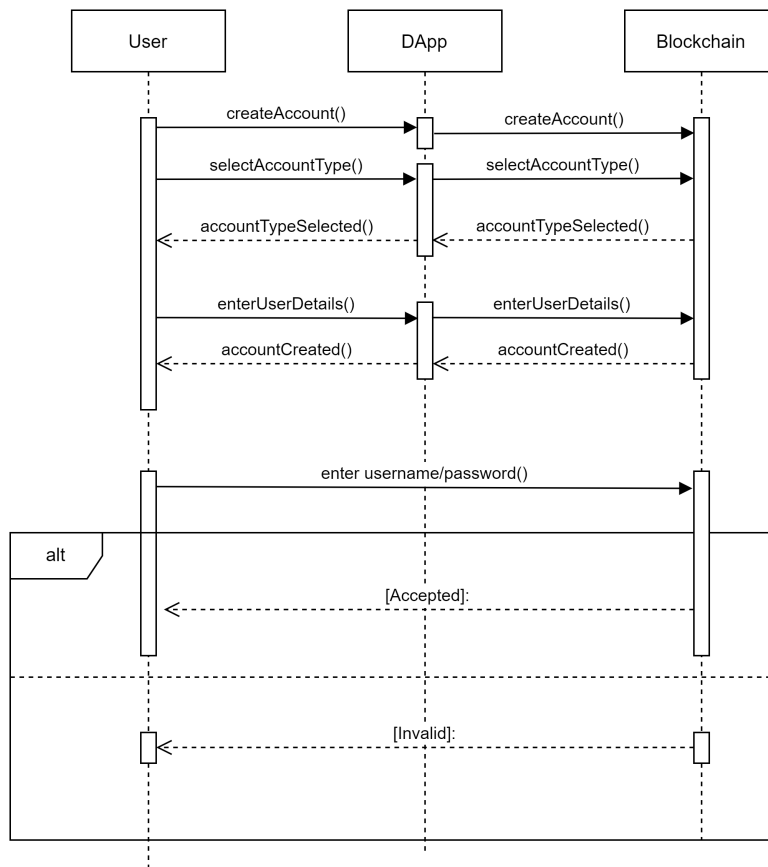


Figure 6.1: Data flow diagram of registration and login.

Figure 6.2: Login Page

Figure 6.3: Register Page

6.1 Communication Protocol between Patient and Doctor:

When a patient visits a doctor with a medical problem, he must provide the doctor with his medical history. When a patient creates an account in PPHDM, he must save his medical history to a smart contact via DApp, which cannot be altered by anyone. The doctor will send the patient a request for access to his medical records. The patient, once again, has the option of giving approval. He can limit the view to solely looking at his medical records. The doctor is unable to make changes to the medical records in this situation. Rather, he can provide the doctor edit access to his medical data, allowing the doctor to update his current state for future treatment. He can also use this section to upload the prescription. Only verified doctors in our database have access to a patient's medical records.

Furthermore, the doctor may recommend a physical examination or refer patients to a hospital for additional treatment. He will give his designation and transmit the data to the patient to check after updating the patient’s medical records utilizing smart contract. The data will be saved in the data management system via DApp after the patient has verified it[Figure.6.4].

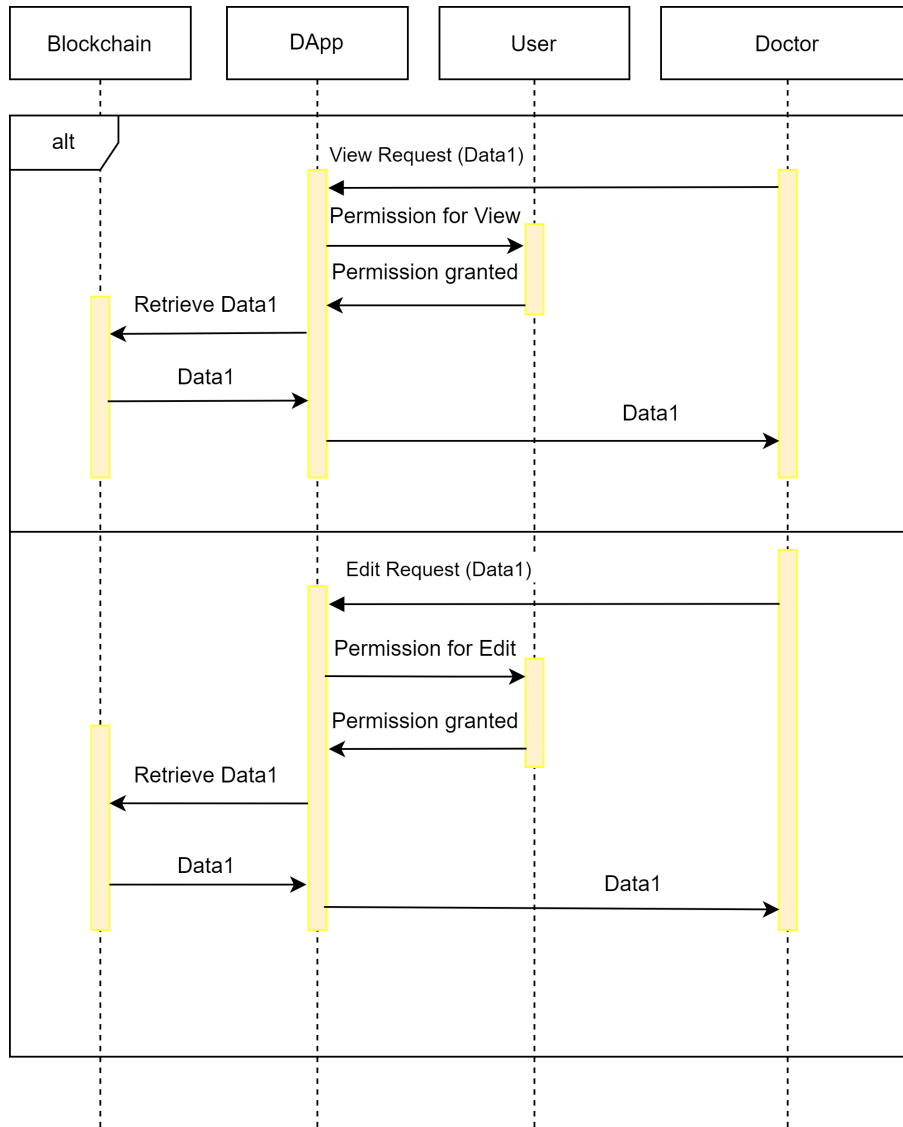


Figure 6.4: Communication Protocol between Patient and Doctor

6.2 Communication Protocol between Patient and Hospital or Laboratory:

Following response from a doctor, the patient can select a hospital and schedule an admission date. He can also view all of the costs on our website. All needed information and costs will be updated via certified hospital and laboratory sources. First and foremost, the patient must provide the hospital access to his medical records. The patient selects a service and submits a request for a pricing estimate. The hospital authority calculates and locks in the patient’s estimated cost. The patient then

schedules an appointment to be admitted to the hospital or a laboratory for testing. After that, the patient pays for his treatment. The patient receives a confirmation communication from the hospital. After completing the test, the laboratory will use DApp to upload his report to smart contacts. The hospital creates the patient’s testimonials, reports, prescriptions, and other documents (medical files). The patient can obtain a copy of his report from the portal. If necessary, the patient can cancel access permission from the hospital at any time[Figure.6.5].

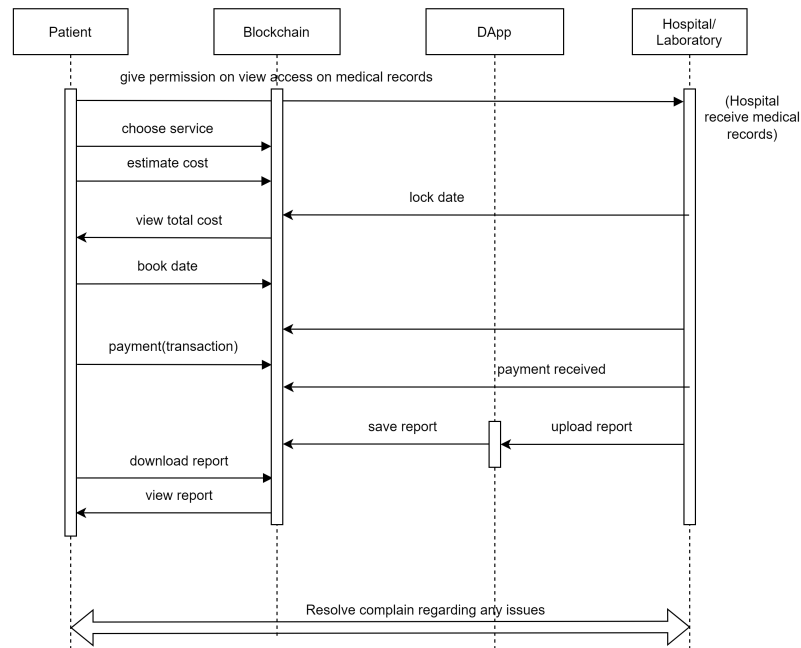


Figure 6.5: Data Flow between hospital/laboratory and patient

If the patient does not file a complaint or consent to the medical report within the timeout period, the hospital will remove the locked funds (both the patient’s and the hospitals) and terminate the protocol. A timeline check is performed in each function to ensure that each process in the protocol is completed within the allotted time frame. Additionally, both parties are given functions to cancel the protocol at each level of the protocol to avoid indefinite waiting if one of the parties stops responding.

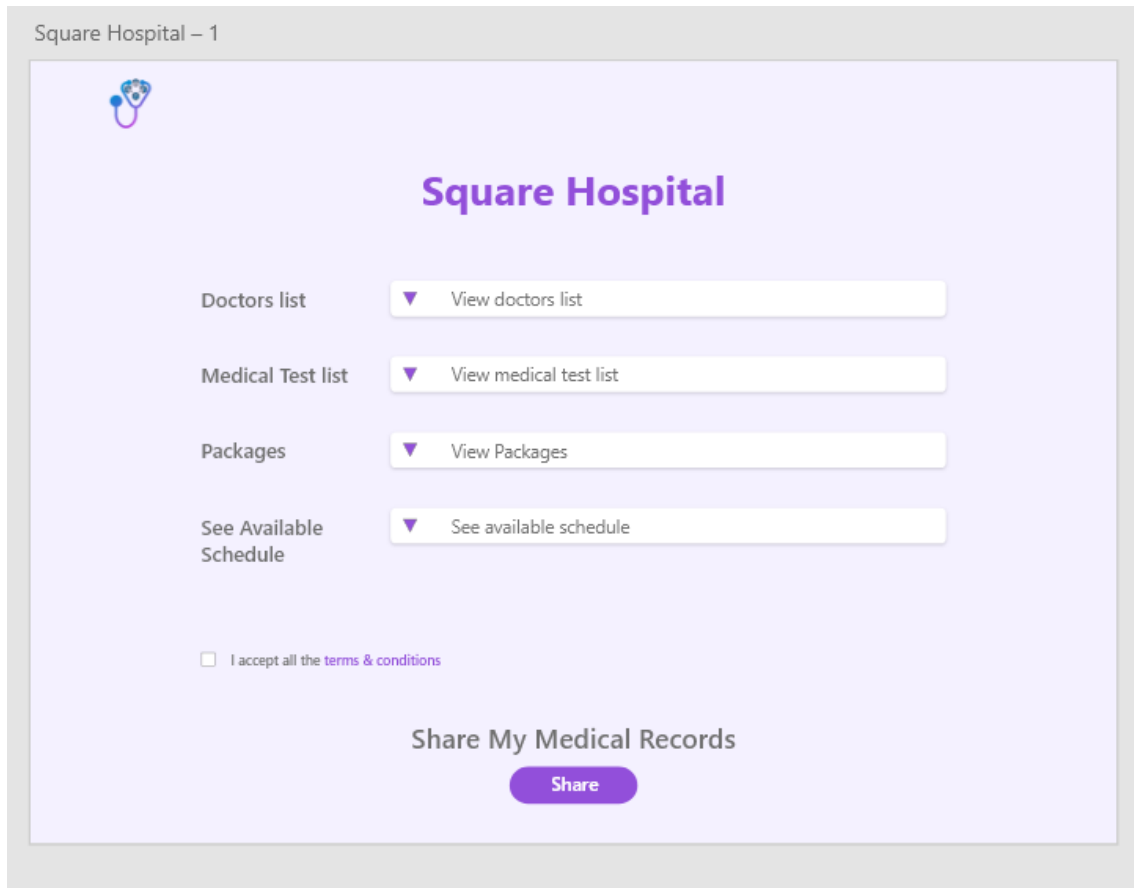


Figure 6.6: Hospital Page

6.3 Communication Protocol among Patient and Insurance Company:

We can say that every Medical Insurance Company maintains a database where all the information about policy has been stored. For policy buying or claiming purposes, buyers and the insurance company have to make some transactions that are kept in blockchain for future accountability purposes, to make clearance about the system. Our PPHDM system also includes an insurance company. A patient can also apply to an insurance company for a package. Initially, the insurance company must store their packages, eligibility for the packages, and company policy in our smart contract, which cannot be amended, via DApp. The validity of the company will next be verified by our data management owner. Following that, the patient must select an insurance company from our website. The user will then select a package that is appropriate for their medical records. The insurance company will send a view request to the patient as a user for verification before applying for the package. After the user accepts the request, it remains pending for a certain amount of time. The insurance company will now verify to see if the patient's medical records match their packages or not. If the patient's package meets the insurance company's requirements, the company will approve the patient's package for further processing. If the package does not meet the requirements, the corporation will deny permission and recommend a suitable package for the patient within a certain time frame. If the company approves the patient's request, an employee will be dispatched to

the patient's residence on a specific day to complete the process, paperwork, and transaction. The date and a list of required documents for the package will be sent to you via our website, which the insurance company will upload.

For buying or claiming an insurance policy it has to go through two phases. Firstly, the buyer has to choose a particular policy depending on his interest and lock it and put the hash of the terms and condition file in the blockchain. Secondly, within a fixed time duration the insurance company also needs to mention the hash of the terms and conditions file and the policy price to the contract. If they respond in time and if these two hash values are the same then the policy price is transferred to the insurance company's account and the system provides a unique policy ID to the user for future references. All the necessary information of the user has been stored in the blockchain. From that very moment, the user or buyer is a legitimate person to get the benefits of the policy upon satisfying the terms and conditions of the policy. In case the two hashes do not match or the insurance company does not reply in time then the user can withdraw his locked money from the system.

Policy 01

User ID/Email :

Amount :

Terms and Conditions :

- Terms and Conditions 01
- Terms and Conditions 02
- Terms and Conditions 03
- Terms and Conditions 04

I accept all the terms & conditions

Share My Medical Records

Share

Figure 6.7: Insurance Page

6.4 Communication between Pharmacy and Patient:

When a patient visits a pharmacy to buy prescribed drugs, he/she has to provide the pharmacist with his uploaded prescription history. When a patient creates a profile in our system (PPHDM) he must save his medical history, as well as an updated prescription to a smart contact via DApp. And it cannot be altered by anyone else. Then the pharmacist will request access to his/her prescription for view only. The

patient will have the option of giving approval to view the data only to pharmacists but not any edit access. He also can limit the view to solely looking at his latest or updated prescription. In this situation, the pharmacist is unable to make changes to his/her prescription. Only verified pharmacies will have access to a patient's prescription. Then after viewing the uploaded prescription, the pharmacist will be able to give the patient his/her necessary drugs. The data will be saved in our system via DApp after both the patient and pharmacist verifies it.

Chapter 7

Discussion

7.1 Motivation of the Proposed Architecture

The proposed architecture is essential for the following reasons:

- We found a small number of hospital administration systems based on blockchain in existing research where medical records are a critical issue. We aim to provide a solution in which no one can alter records without the consent or access of the owner. It provides a safe database for users' medical information.
- It also helps us to save time. Users do not need to collect their prescriptions because they will be uploaded into their database by a verified doctor, and they will be able to search it whenever they want.
- Patients are not required to physically visit the hospital. They can collect it from their house because it will be safely uploaded by the hospital's verified laboratory, and they will be able to download it.
- Users can choose any insurance policy from the website by sharing their medical records, and they can also share their medical records with a verified pharmacy to avoid carrying their prescription.

7.2 Advantages of this System

The benefit of this proposed architecture is that it will provide users with data automatically. When a user verifies their identity, they may simply browse through the system, schedule appointments with doctors, purchase medications prescribed by doctors from pharmacies, and schedule appointments for testing conducted by doctors. They will be able to readily access all of their medical records through this system, which will be secured using Blockchain.

7.3 Limitations

In this study we have developed a system where there is a backend service and frontend service with an api. To connect with the blockchain network we have

used a connector which is a decentralized application. Our system won't function properly if the decentralized application or DApp stops working in the middle of the data transaction. As this DApp is the connector of the system and blockchain network so the whole system falls down. This is the only limitation we have found so far for our system.

Chapter 8

Conclusion

To sum up, our privacy preserving healthcare data management system, which uses block chain technology, has demonstrated how a decentralized database is being utilized in the medical ecosystem for large-scale data management and to simplify complex medical operations. We use block chain to demonstrate a new method to medical record management that provides auditability, interoperability, and accessibility. This system, which is designed to record flexibility and granularity, allows for the sharing of patient data as well as incentives for medical researchers to support the system. Our proposed solution employs block chain technology to establish an iterative, scalable, safe, accessible, and decentralized healthcare ecosystem. This will let people freely and securely share their medical records with doctors, hospitals, research groups, and other stakeholders while preserving complete control over their medical data's privacy. Many of the present healthcare system's problems will be solved, including data management, legacy network inconsistency, unstructured data gathering challenges, prohibitively high administrative expenses, a lack of data security, and unresolved privacy concerns.

8.1 Future Work

The development done here according to the study is at the initial level. We have planned to develop this system further in future. As for now we have just shown the primary features of our system. We will make our DApp more advanced and we will build an application of this system using Dart language. Also we will implement another encryption protocol to make our system more secure and unbreachable. This is the upcoming plan for our system.

Reference

1. G. Magyar, "Blockchain: Solving the privacy and research availability tradeo for EHR data: A new disruptive technology in health data management," 2017 IEEE 30th Neumann Colloquium (NC), 2017, pp. 000135-000140, doi: 10.1109/NC.2017.8263269.
2. A. P. Singh et al., "A Novel Patient-Centric Architectural Framework for BlockchainEnabled Healthcare Applications," in IEEE Transactions on Industrial Informatics, vol. 17, no. 8, pp. 5779-5789, Aug. 2021, doi: 10.1109/TII.2020.3037889.
3. Deloitte. Blockchain: opportunities for health care [Internet]. New York (NY): Deloitte;c2019. cited at 2019 Jan 15. Available from: <https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html>.
4. Dimitrov, Dimiter V. "Blockchain Applications for Healthcare Data Management." Healthcare Informatics Research, vol. 25, no. 1, Jan. 2019, pp. 51–56. synapse.koreamed.org, <https://doi.org/10.4258/hir.2019.25.1.51>.
5. Gordon WJ, Catalini C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. *Comput Struct Biotechnol J*. 2018; 16:224–230. <https://www.sciencedirect.com/science/article/pii/S200103701830028X?via=ihub>
6. Liu, H.; Crespo, R.G.; Mart´mez, O.S. Enhancing Privacy and Data Security across Healthcare Applications Using Blockchain and Distributed Ledger Concepts. *Healthcare* 2020, 8, 243. <https://doi.org/10.3390/healthcare8030243>
7. Clauson, K. A., Breeden, E. A., Davidson, C., Mackey, T. K. (2018). Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare:: An exploration of challenges and opportunities in the health supply chain. *Blockchain in Healthcare Today*, 1. <https://doi.org/10.30953/bhty.v1.20>
8. L. Ismail, H. Materwala and S. Zeadally, "Lightweight Blockchain for Healthcare," in IEEE Access, vol. 7, pp. 149935-149951, 2019, doi: 10.1109/ACCESS.2019.2947613.
9. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. *Healthcare* 2019, 7, 56. <https://doi.org/10.3390/healthcare7020056>.
10. A. Yazdinejad, G. Srivastava, R. M. Parizi, A. Dehghantanha, K. -K. R. Choo and M. Aledhari, "Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 24, no. 8, pp. 2146-2156, Aug. 2020, doi: 10.1109/JBHI.2020.2969648.
11. Rahul Johari, Vivek Kumar, Kalpana Gupta, Deo Prakash Vidyarthi, BLO-SOM:Blockchain technology for Security Of Medical records,ICT Express,2021,ISSN 2405-9595,<https://doi.org/10.1016/j.icte.2021.06.002>.

12. J. Hathaliya, P. Sharma, S. Tanwar and R. Gupta, "Blockchain-Based Remote Patient Monitoring in Healthcare 4.0," 2019 IEEE 9th International Conference on Advanced Computing (IACC), 2019, pp. 87-91, doi: 10.1109/IACC48062.2019.8971593.
13. Onik, Md. Mehedi Hassan (2019). Big Data Analytics for Intelligent Healthcare Management — Blockchain in Healthcare: Challenges and Solutions. , (), 197–226. doi:10.1016/B978-0-12-818146-1.00008-8 url to share this paper: <https://sci-hub.mkksa.top/>
14. What types of blocks exist on the blockchain? Bit2Me Academy. (2021, May 11). Retrieved October 3, 2021, from <https://academy.bit2me.com/en/types-of-blocks-in-blockchain/>.
15. Dariush Yazdani. (2017). Global FinTech Report 2017 [Ebook]. Retrieved from <https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-global-fintechreport-2017.pdf>.
16. A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: using blockchain for medical data access and permission management, in: International Conference on Open and Big Data (OBD), IEEE, 2016, pp. 25–30.
17. M. J. M. Chowdhury, M. S. Ferdous, K. Biswas, N. Chowdhury, A. Kayes, M. Alazab, and P. Watters, "A comparative analysis of distributed ledger technology platforms," IEEE Access, vol. 7, no. 1, pp. 167 930–167 943, 2019.
18. <https://msferdous.info/DynaSAMLPersonal.pdf>.
19. "Node.js". Accessed: 2020-07-10. [Online]. Available: <https://nodejs.org/en/>
20. "Express JS". Accessed: 2020-07-10. [Online]. Available: <https://expressjs.com/>
21. <https://www.hyperledger.org/use/fabric>.
22. <https://www.hyperledger.org/use/sawtooth>.
23. <https://arxiv.org/pdf/2011.08846.pdf>.
24. <https://msferdous.info/DynaSAMLPersonal.pdf>.
25. BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records. (n.d.). Ieeexplore.Ieee. <https://ieeexplore.ieee.org/abstract/document/8647713>.
26. MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management. (n.d.). IEEE.<https://ieeexplore.ieee.org/abstract/document/8895951>.
27. Blockchain for Giving Patients Control Over Their Medical Records. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/9233462>.

28. A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform. (n.d.). ScienceDirect. <https://www.sciencedirect.com/science/article/abs/pii/S1389041718301177>.
29. BLOSOM: BLOckchain technology for Security Of Medical records. (n.d.). ScienceDirect. <https://www.sciencedirect.com/science/article/pii/S2405959521000783>.
30. Blockchain in Healthcare: A Patient-Centered Model. (n.d.). NCBI. <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6764776/>.
31. Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR). (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/8422883>.
32. Blockchain vehicles for efficient Medical Record management. (n.d.). NPJ. <https://www.nature.com/articles/s41746019-0211-0Sec3>.
33. A blockchain-based framework for electronic medical records sharing with fine-grained access control. (n.d.). PlosOne. <https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0239946>.
34. Block-Based Access Control for Blockchain-Based Electronic Medical Records (EMRs) Query in eHealth. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/8647433>.
35. MedRec: Using Blockchain for Medical Data Access and Permission Management. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/7573685>.
36. DASS-CARE: A Decentralized, Accessible, Scalable, and Secure Healthcare Framework using Blockchain. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/8766714>.
37. Vara, C. (n.d.). Distributed e-health wide-world accounting ledger via blockchain. Iospress. <https://content.iospress.com/articles/journal-of-intelligent-and-fuzzysystems/ifs169949>.
38. Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/8761307>.
39. Kumar, N., and Parangjothi, C. (n.d.). Peer Consonance in Blockchain based Healthcare Application using AI-based Consensus Mechanism. IEEE. <https://ieeexplore.ieee.org/abstract/document/9225550>.
40. Wu, S., and Du, J. (n.d.). Electronic medical record security sharing model based on blockchain. ACM. <https://dl.acm.org/doi/abs/>
41. Ekblaw, A., and Azaria, A. (n.d.). MedRec: Medical Data Management on the Blockchain. VC. <https://viral.media.mit.edu/pub/medrec/release/1>.
42. A Combined Framework of InterPlanetary File System and Blockchain to Securely Manage Electronic Medical Records. (n.d.). SpringerLink. <https://link.springer.com/chapter/10.1007/978981334673440>.

43. Hybrid blockchain–based privacy-preserving electronic medical records sharing scheme across medical information control system. (n.d.). SAGE Journals. <https://journals.sagepub.com/doi/full/10.1177/0020294020926636>.
44. Hang, L. (2019, April 25). A Novel EMR Integrity Management Based on a Medical Blockchain Platform in Hospital. MDPI. <https://www.mdpi.com/2079-9292/8/4/467>.
45. Blockchain: Solving the privacy and research availability tradeo for EHR data: A new disruptive technology in health data management. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/8263269>.
46. Blockchain-Enabled Secure and Smart HealthCare System. (n.d.). Cornell University. <https://arxiv.org/abs/2108.00807>.
47. Blockchain in healthcare and health sciences—A scoping review. (n.d.). ScienceDirect. <https://www.sciencedirect.com/science/article/pii/S138650561930526X>.
48. Mettler, M. (n.d.). Blockchain technology in healthcare: The revolution starts here. IEEE. <https://ieeexplore.ieee.org/abstract/document/7749510>.
49. Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare.(n.d.).BlockchainHealthCare Today. <https://www.blockchainhealthcaretoday.com/index.php/journal/article/view/20>
50. Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. (n.d.). IEEE. <https://ieeexplore.ieee.org/abstract/document/8970497>.
51. Cyran, M. A. (n.d.). Blockchain as a Foundation for Sharing Healthcare Data. BlockchainHealthCareToday. <https://www.blockchainhealthcaretoday.com/index.php/journal/article/view/13>.
52. IEEE 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) - Madurai, India (2020.5.13-2020.5.15) 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS) Enhancing Data Security In Cloud Using Blockchain. (n.d.). IEEE. <https://zh.booksc.eu/book/82545206/7f265e>.
53. Design of a Secure Medical Data Sharing Scheme Based on Blockchain. (n.d.). SpringerLink. <https://link.springer.com/article/10.1007/s10916-019-1468-1authFulong-Chen>.