Privacy Preservation in E-Healthcare Systems using Blockchain

By

Nigam Naveed

A thesis submitted to the faculty of Information Security Department, Military College of Signals, National University of Sciences and Technology, Rawalpindi in partial fulfilment of the requirements for the degree of MS in Information Security.

September 2021

Declaration

I hereby declare that except where specific reference is made to the work of others,the contents of this dissertation are original and have not been submitted in whole or in part for consideration for any other degree or qualification in this, or any other university. This dissertation is my own work and contains nothing which is the outcome of work done in collaboration with others, except as specified in the text and Acknowledgements.

Nigam Naveed

September 2021

Dedication

This thesis is dedicated to my Family, Teachers, and Friends for their unconditional love, endless support, and continuous encouragement.

Acknowledgement

Anything is possible when you have the right people there to support you.

-Misty Copeland

First and foremost, I would like to praise and thank Allah, The Almighty, who has granted countless blessings, knowledge, and opportunity, so that I have been finally able to accomplish the thesis.

I am indebted to my supervisor Assistant Professor Dr Fawad Khan and my committee members Assistant Professor Dr Muhammad Waseem and Assistant Professor Dr Waleed Bin Shahid for their guidance and patience. Without the timely help of the committee members and the motivation from my supervisor in the times of despair, I would not have been able to bring this herculean task to a fine conclusion.

This huge endeavour came with its highs and lows and when I was about to give up my teachers; Sir Fawad and Sir Waseem, parents, my siblings; Midhat and Talha and my friend Rida Rashid became my beacon of hope; for that I will always be grateful.

Abstract

An individual's all health-related data is stored in an electronic health record system (EHR system). The EHR system facilitates the data owner to control and share his or her information with specific people. Because of the fatal consequences of inaccurate data, the tamper resistance feature is critical for the EHR system. The immutability and irreversibility qualities of blockchain technology make it a potential solution. This research proposes an EHR model based on Hyperledger fabric blockchain. For providing tamper-resistant feature, the suggested framework is proposed using blockchain technology. To protect privacy, proxy re-encryption is used. Hyperledger fabric has been selected for this research. To run Hyperledger fabric, AstraKode blockchain is used as previous composer (Hyperledger composer), used to run the fabric, has been deprecated. A detailed security analysis is done to show that the proposed model is secure for privacy, and it also provides tamper resistance feature. Performance analysis of proxy re-encryption has also been observed.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

EHR	Electronic Health Record
MAC	Mandatory Access Control
DAC	Discriteionary Access Control
ABAC	Attribute Based Access Control
IBAC	Identity Based Access Control
SKE	Symmetric Key Encryption
PKE	Public Key Encryption
ABE	Attribute Based Encryption
DES	Data Encryption Standard
AES	Advanced Encryption Standard
EMR	Electronic Medical Record
PKI	Public Key Infrastructure
CS	Cloud Storage
BC	Blockchain

Chapter 1

Introduction

1.1. Introduction

Big data is increasingly being used in a variety of fields, such as science, engineering, and commercial areas, has sparked academic interest, due to growing concern about individual privacy and big data security across all sectors [1]. Data can be found in different forms, including social media sites, videos or images, cell phones, e-commerce, medical records, and a variety of numerous other fields. The total data generated every day is many quintillion bytes [2]. This data is referred to as "big data."

Because of the advancements in Big Data, the healthcare industry can now translate health data into EHR (electronic health record) or EHD (electronic health data) or. EHR contains medical histories, allergy information, laboratory test results, billing information, etc. The benefits of EHR include quick and easy access to clinical data, maintenance of effective clinical processes, improved patient safety, reduced medical errors and lower medical expenses. Recognizing these advantages, more than 90% of healthcare facilities in Australia and around the world have installed EHR systems to optimize the distribution of medical resources and the efficiency of healthcare [3]. EHR systems, nowadays, store records in cloud so that they can be accessed at anywhere by anyone such as doctor, patient, nurses etc at any time.

Cloud computing is a rapidly expanding digital technology paradigm that is widely used in the healthcare business [4]. The large-scale expansion of health data, in the age of big data, forces to use cloud service to manage this huge data and making it easier to interchange or transfer medical data among a variety of users[5]. Any improper update or alteration of EHR data could have irreversible negative consequences. As a result, every EHR system's privacy becomes a key component. Security and privacy are, without a question, the most difficult and serious issues.

Many studies suggest that if big data is not handled appropriately, it will compromise consumers' privacy [6]. The most essential characteristic of the EHR system is the tamper resistant property. Some of the privacy and security considerations that should be considered in the context of big data are listed below:

1. Persons' medical data is extremely sensitive as it can be misused by anyone. So, the person may not want everyone to know about it.
2. Another effect is social stratification, in which a literate person benefits from big data analysis while the illiterate suffers, as is the situation in developing countries where the digital gap between the two is prominent. [7].

Considering these points, it is critical to develop a secure process for exchanging data among different users. [8]. As a result, privacy becomes a critical component of any PHR system. The most essential characteristic of the EHR system is the tamper resistant property.

If an individual's health-related data can be reliably acquired and stored on tamper-resistant storage, an EHR system can considerably deliver high-quality preventive personal healthcare. Blockchain's immutability, cryptographic verifiability, and backup properties make it a viable tamper-resistant storage method for EHR systems. The goal of this study is to develop a framework for securely sharing patient data between enterprises while maintaining patient confidentiality.

1.2. Motivation

Patient data, as well as a patient's privacy, are critical in the current situation. Doctors want data to assess patients efficiently, and many pharmaceutical companies require this data for research. This information, combined with medical guidance, is necessary or a patient to make an informed decision about his health and life. He should also keep track of his or her medical advice and treatments. He also requires this information so that he can consult with a number of professionals before making a decision about his ongoing therapy. This scenario necessitates the efficient online sharing of patient data so that it is readily available to the appropriate party.

When private data is sent to third-party cloud servers, chances for exposure of sensitive data increases. As a result, security is critical to ensure its legitimate and permitted use, ensuring that the legitimate user receives the data in its accurate form.

Another purpose for this study is to investigate various techniques that provides security to healthcare data. The current privacy-preserving techniques are insufficient to assure perfect security for cloud-based EHR management.

E-health data contains a wide range of confidential and sensitive information. Its' exposure can cause financial losses too. In addition, there has been a steady growth in the fraudulent distribution of medicinal medications to patients without prescriptions. This misuse of medical medications has the potential to result in death due to an overdose.

As a result, sensitive information relating to people's data must be protected in terms of privacy, integrity, confidentiality, and availability. Cybersecurity is required in this scenario to prevent, identify, and respond to unauthorized access to a health system's data. Data encryption, strong authentication, secure storage, key management, and access control are just a few of the issues that still need to be addressed. This has inspired us to create a new method that enhances the privacy of healthcare systems.

We proposed a permissioned blockchain framework using proxy re-encryption scheme to create a prototype that may be utilized for efficient data exchange, health record management.

1.3. Research Problems

As discussed earlier, privacy of health data is extremely important. We identified following concerns for this research:

1. To solve the inadequacies of present systems, how might blockchain technology be used to implement a system which is efficient enough to provide a smooth access control?
2. How can a new framework, for ensuring patient privacy and data security, be designed, developed, and analyzed?

1.4. Objectives

The main goal of this study is to create a patient centric framework. This will be accomplished by utilizing a specific encryption mechanism for privacy and access control to develop a secure system. Also, blockchain will be used to protect the integrity of the data.

The following are the research's individual goals:

a. Analyze privacy preservation techniques in e-healthcare.

b. Propose a blockchain based privacy preservation framework for e-healthcare data.

c. Comparative security analysis of proposed framework with existing framework.

1.5. Thesis Composition

The following is a summary of the thesis's structure:

Chapter 1: The study aims, objectives, motivation, research issues, and contributions are all presented in Chapter 1 of the book. The introduction describes the motives for performing this research, as well as why it is important.

Chapter 2: This chapter presents a survey of e-health security and privacy challenges, as well as several privacy-preserving techniques used for privacy and security of electronic health records stored in the cloud.

Chapter 3: A proxy re-encryption technique is shown. This chapter explains how it all works. Also, this chapter introduces blockchain technology. Different types of blockchain i-e public, private, and consortium blockchain, are explained. Hyperledger fabric and Hyperledger composer has also been discussed in this chapter. Furthermore, AstraKode blockchain has also been introduced.

Chapter 4: In this chapter, a framework is proposed using a proxy re-encryption scheme and blockchain.

Chapter 5: This chapter presents implementation of proxy re-encryption and blockchain network on AstraKode. Privacy and security analysis of our proposed framework has also been discussed in this chapter. Also, a comparative analysis between our proposed scheme and existing techniques has been shown.

Chapter 6: This chapter incorporates the thesis's main conclusions and analysis, as well as future research directions based on the findings.

Chapter 2

Literature Review

2.1. Introduction

The literature work done in this chapter provides background information for this research to be carried out further. This chapter demonstrates different methods and approaches used in this field of study. It presents a comprehensive overview of various privacy-preserving techniques used for electronic health records (EHR) systems in the cloud. In order to establish an EHR safety model, this research focuses on the challenges and opportunities in the field of cyber security research.

Following tasks are identified in this chapter, which explores and reviews various parts of multiple articles:

1. Requirements for privacy of EHR data in cloud.
2. EHR privacy and security.
3. Cryptographic and non-cryptographic approaches for privacy of electronic health records.

This chapter also examines non-cryptographic techniques such as MAC, DAC, RBAC, ABAC, and cryptographic techniques such as Public Key Encryption, Symmetric Key Encryption, Proxy Re-encryption, Attribute based access control. This review examines the benefits, drawbacks, and research issues of current privacy-preserving techniques.

2.2. Requirements For Privacy and Security of EHR Data in The Cloud

Outsourcing health data to cloud servers in this big data era increases the risk of a variety of cyber-attacks, including information disclosure, MITM attacks, DoS attacks, ransomware attacks resulting in loss of privacy, financial losses and much more [9]. As a result, there is a need to safeguard data in order to protect patient privacy.

Following are the privacy and security requirements for EHR data:

1. Confidentiality
2. Integrity
3. Non-repudiation
4. Audit

Data confidentiality: It ensures that sensitive health information does not get into the wrong hands. The most comprehensive way for ensuring data secrecy is data encryption.

Data integrity: It assures that no unauthorized entity has tampered with the patient's health information.

Non-repudiation: Non-repudiation refers to a sender's and receiver's refusal to deny their authenticity.

Audit: This criterion ensures that health data is monitored and secured, by keeping track of the records.

Cloud computing is a centralized structure making it more open to different attacks, putting health records at risk. Even though cloud technologies follow to strict security measurements, they may not provide a guaranteed solution for e-health adoption due to security concerns. In Table 2-1, several innovative cloud protection solutions are examined, including their benefits and drawbacks.

2.3. Cloud Based EHR Systems Overview

An e-health system's electronic health record (EHR) is a collection of patients' electronic health information. These records contain all information related to health, including medical histories, lab reports, billing information etc. [10]. EHR systems provides information about medical data of patient, but they also put privacy of patient at risk through inappropriate permission and the exploitation of EHR data. As a result, privacy of healthcare systems is critical, when the data is shared between different users.

The e-health architecture is depicted in Figure 2-1.

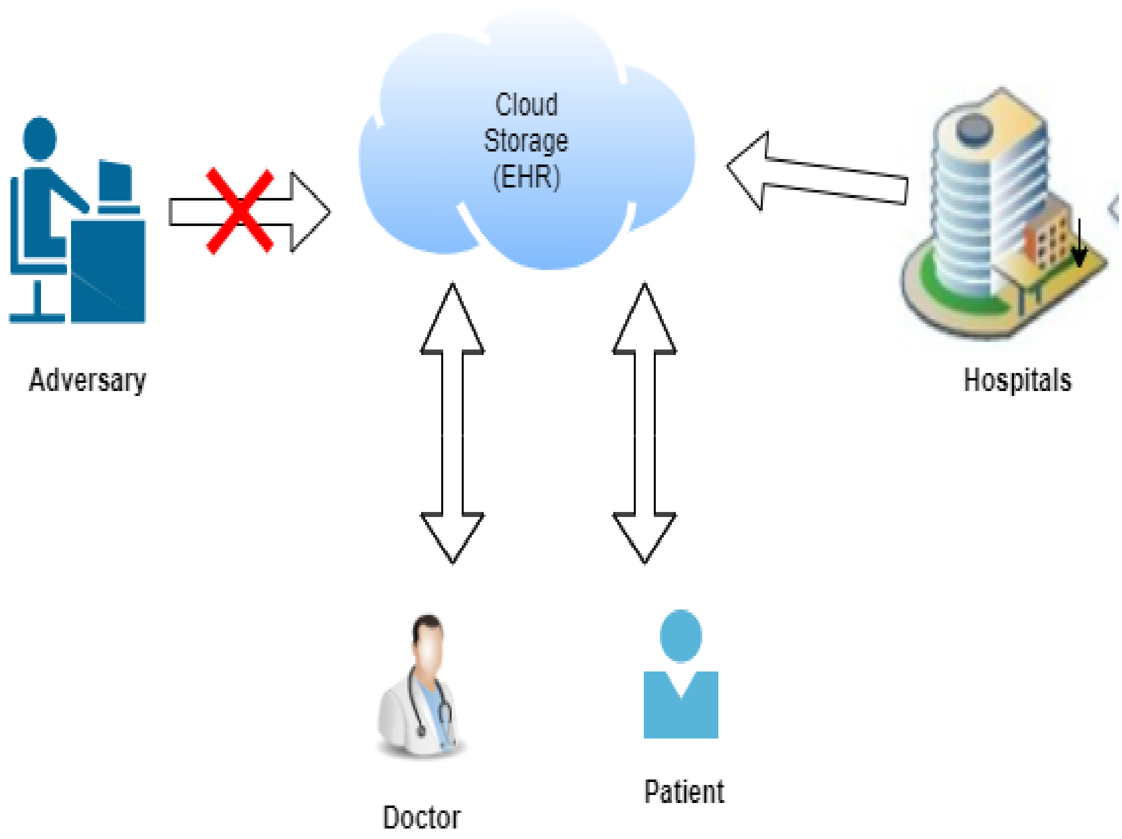


Figure 2-1: EHR data architecture in cloud

Depending on the data storage, cloud architecture for e-health systems might be public, private or hybrid. As EHR data is confidential, proper access control mechanism is required for the sharing of such sensitive data. By managing the operation and access of healthcare records, access control is a security barrier that protects data privacy in the healthcare system. RBAC, ABAC and IBAC are the most common access control approaches used in healthcare systems. Users can be assigned specific roles for data access in role-based systems [11]. ABAC utilizes cryptographic and non-cryptographic techniques [12]. Various parties, such as hospitals, and healthcare organizations, can share data.

Several solutions for securing the privacy of EHR data are already in use. Some security mechanisms can be applied to EHR systems, whereas others cannot owe to privacy and security issues. Zhu et al. proposed a biometric identification scheme for privacy preservation. In this scheme, first biometric data is encrypted. This encrypted data is then stored on cloud server. However, because health records are particularly sensitive, and data is available to the database owner, this method is less acceptable in terms of security.

A CP-ABE scheme was presented in [18]. This approach combined the benefits of both SKE and ABE as it allows multi-privileged access control for EHRs by encrypting data from several patients who are subject to the same access policy. Kaaniche et al. [19] suggested an architecture for safe data management based on Identity based cryptography, encrypting and then transmitting the data with users so that no unauthorized user can read it without the consent of owner.

Huang, Cui and Chi proposed attribute-based scheme in [20] [21] and [22] respectively. Though it is an efficient scheme, still its' unsuitable due to its key management complexity. Although the shift of healthcare systems to the cloud has provided many facilities, it has raised issues of privacy and integrity of data as well. So, to maintain privacy and integrity of data during its' access is very important [23].

Table 2-1: Security Techniques in Cloud Computing

Scheme	Advantage	Disadvantage	Reference
TMACS	Security technique ensures efficient performance	Reuses master key between different authorities causing computational overhead	[14]
Identity based encryption Technique	Reduces the complexity of encryption	A secure connection is required between user & key generator	[15]
Attribute-based encryption	Fine-grained access control providing dynamic user management	To encrypt data, the data owner needs each authorized user's public key.	[16]
PPDP	methodology for disease prediction that is quite effective	The difficulty of computation rise as the number of EHRs increases, and the verification mechanism is not described.	[17]
biometric identification scheme	Provides maximum data privacy that isn't vulnerable to collusion.	Centralized system that leads to trust the cloud server provider	[13]

2.4. Classification of Electronic Health Records Privacy Mechanisms

This section reviews various investigations conducted on two methodologies, shown in Figure 2-2, as well as their challenges in the field of healthcare.

There are two types of encryption schemes:

1. Non- Cryptographic Scheme
2. Cryptographic Scheme

Non- Cryptographic Scheme: Different access control policies are used for this scheme.

Cryptographic Scheme: It includes public key encryption, symmetric key encryption etc.

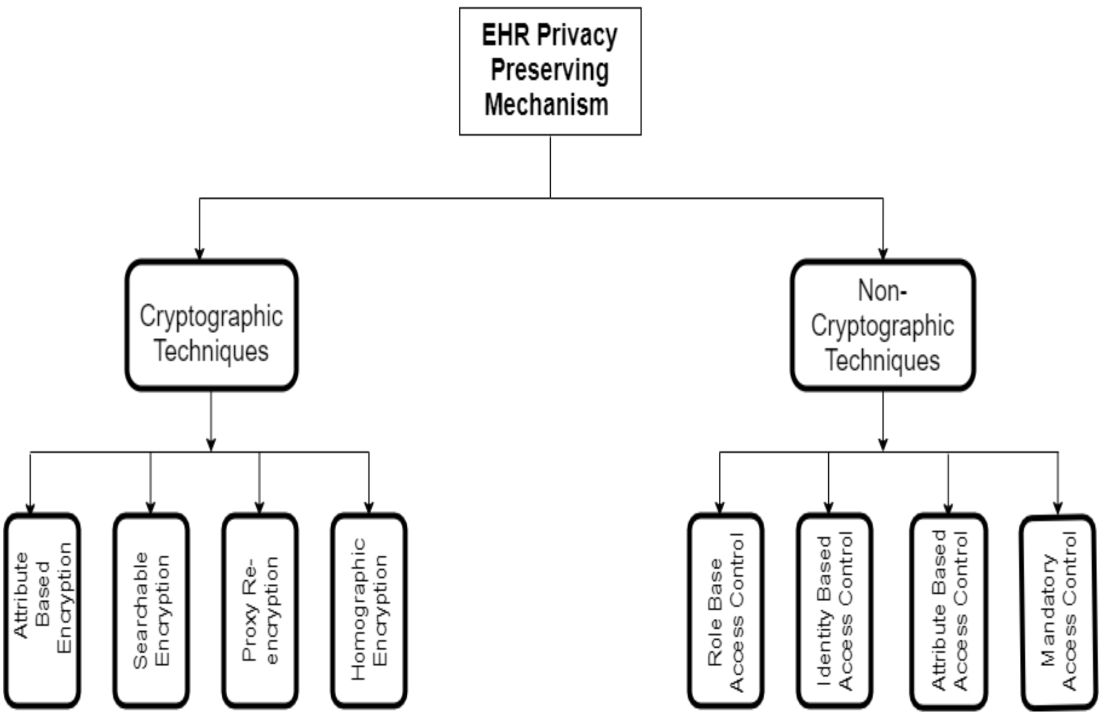


Figure 2-2: Privacy preservation mechanisms of EHR data

2.4.1. Cryptographic Approaches

Symmetric key cryptography and asymmetric key cryptography are two cryptographic systems. Symmetric key encryption utilizes the same key for the process of encryption and decryption. Asymmetric encryption scheme utilizes different keys for performing decryption and encryption. This study includes an overview of few such encryption schemes which is also shown in Table 2-2.

2.4.1.1. Symmetric Key Encryption:

SKE is efficient in EHR systems because it uses the same key to perform encryption and decryption process. However, it inevitably adds to the complexity because it needs extra access control methods for effective EHR sharing. DES and AES are the most commonly used SKE-based algorithms. Li et al. [24] proposed a secure EMR sharing scheme. Li used one time key for encryption purposed and records were saved anonymously. An EMR number was required for this approach. Since each key was used only to encrypt one medical record, confidentiality of each medical record was increased. A symmetric encryption workflow is shown in Figure 2-3.

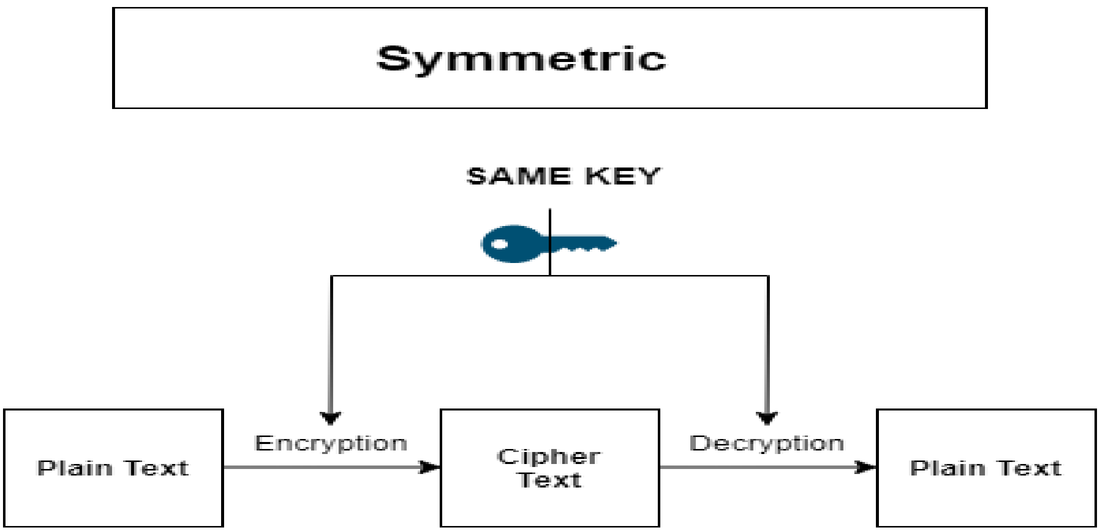


Figure 2-2: Symmetric Encryption

Table 2-2: Cryptographic Techniques

Scheme	Strength	Weakness	Reference
SKE	Ownership of data is ensured	For retrieval, smart card is required	[31]
PKE, ElGamal	Resilient against insider attacks	Expensive computation, Not suited for a policy of dynamic access policy	[32]
PKE, Pseudonymity	Between user and provider, there is anonymity.	The contents of health data may be misused by the service provider.	[33]
SKE	Issue of key distribution is resolved	Multiple user roles are difficult to manage.	[34]
ABE	Data storage entities maintain user anonymity.	Cloud is aware of the policy regarding access to medical records.	[35]
KP- ABE	Access control can be adjusted	Computational overhead	[36]
Hierarchical-ABE	Fine grained access control	It is possible to search for a single keyword.	[37]

2.4.1.2. Assymmetric Key Encryption:

Two different keys, a public and a private, are used in public key encryption or asymmetric encryption techniques as shown in Figure 2-4. When combined with SKE systems, these schemes can be more efficient. SKE can be used for the encryption of content while key pairs of public key encryption are used for encrypting the symmetric key. A framework [25] was given, which used public key for security requirements such as integrity, confidentiality, authentication etc. and a symmetric key was used for encrypting EHR data. In this framework, PKI used different certificates, a registration authority, and a management system to link public keys to unique user identities. This suggested architecture creates a safe EHR sharing framework that allows patients and multiple healthcare providers to share EHRs effectively.

A framework was given by Pecarina et al [26]. He gave a PKE-based system for enhancing privacy in a semi-trusted health cloud by enabling anonymity in data storage.

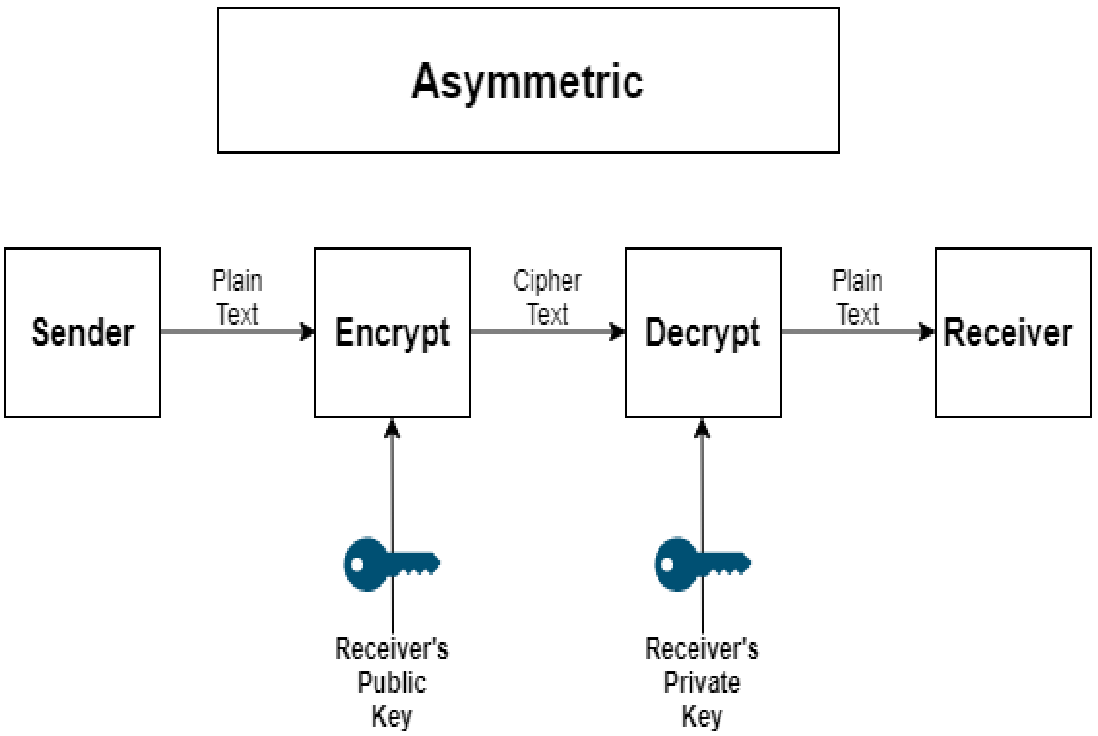


Figure 2-3: Public Key Encryption

A few different types of asymmetric encryption are explained below.

2.4.1.2.1. Attribute-based Approaches

A few other cryptographic ways to protect privacy in healthcare sector are discussed in this section. Sahai and Waters [27] proposed attribute-based encryption, which uses asymmetric key encryption to protect data stored on cloud and encrypts and decrypts data based on user attributes.

The access-structure policy in ABE dictates that the cypher text can only be decrypted if the ciphertext characteristics match the user attributes. There are two types of attribute-based encryption scheme:

1. KP-ABE
2. CP-ABE

In KP- ABE [27] [28], the user's secret key encrypts the access policy, and the ciphertext can only be decrypted if the user’s attribute matches the access policy.

In CP-ABE, ciphertext is linked to a set of attributes which can be decoded only if the user's attributes fulfill the requirements of access policy [27] [28].

2.4.1.2.2. Proxy Re-Encryption

It is a cryptographic technique in which a semi-trusted device i.e., proxy server converts one ciphertext another ciphertext without without the disclosure of secret message to the proxy server.

Yang introduced a timing-based proxy re-encryption function and a tester. For searching mechanism, a keyword is used. This system presents a mechanism that allows a medical facility to decrypt patient's health records by using credentials of user without the revelation of secret key [29]. A time-based proxy re encryption scheme has been proposed in [30]. In this scheme a user can access the medical records of patient by keyword search over a period of time T.

2.4.2. Non-Cryptographic Approaches

To implement data privacy management, non-cryptographic techniques mostly rely on access control-based policies. Data access in EHR systems is very secret, and data is stored on third-party servers. As encryption approaches, access control techniques are unavoidable and essential. Access control provides key security barriers to data

privacy in a health care information system, limiting operation of the EHR system.

Figure 2-5 depicts some of the most common non-cryptographic techniques. Table 2-3 shows summary of few non-cryptographic privacy-preserving techniques.

DAC: The method of limiting access to objects depending on the subject's identity is known as discretionary access control [38].

MAC: In MAC, a central authority has the full control over access policy. Hence, decisions are taken by central authority rather than object’s owner. Owner have no power to change the access permissions. [39].

RBAC: RBAC establishes access decisions based on job functions, in which subjects are assigned roles. Permissions are linked with roles. Roles determine that on which object which action should be performed.

ABAC: In ABAC, access decisions are made based on a set of attributes defined by user. Requesters are granted access based on those qualities satisfying the policy's requirements.

IBAC: It is a method of controlling access based on a person's authenticated identification.

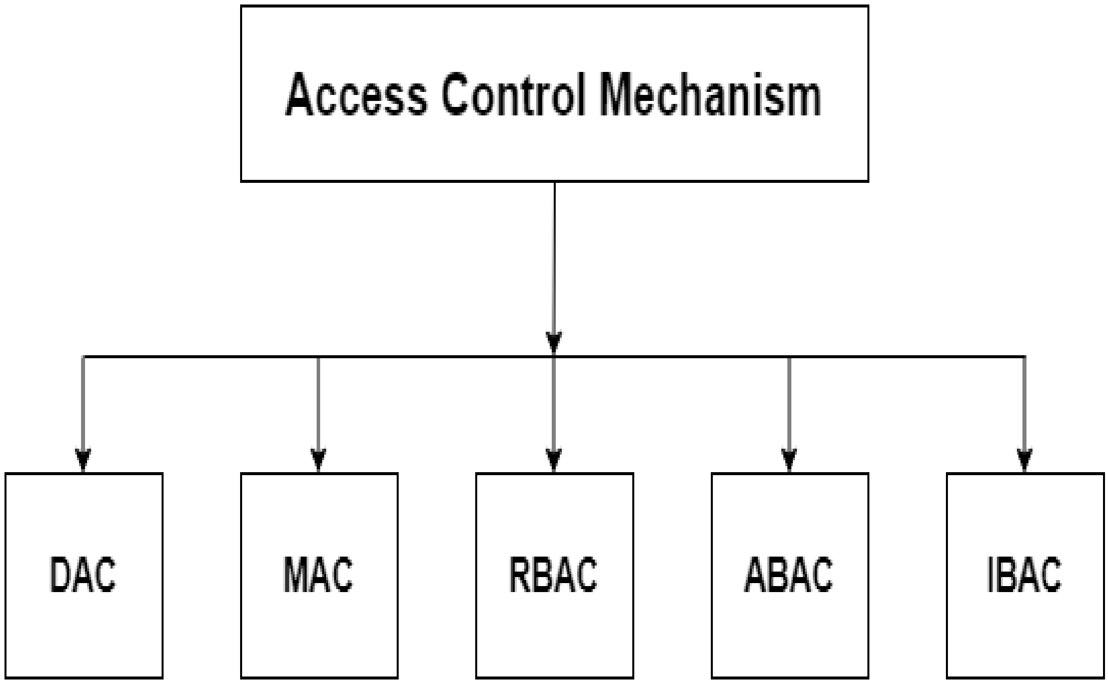


Figure 2-4: Access control mechanisms for non-cryptographic Approaches

Table 2-3: Comparison of non-Cryptographic Techniques

Scheme	**Strength**	**Weakness**	**Reference**
ABAC	Access control policy is dynamic	Large no.of rules required	[40]
RBAC	Access administration is simple	Expensive for defining rules	[41]
MAC, RBAC, DAC	Three models are combined		[42]
ABAC	Provides flexible access control	Lack of Integrity and Confidentiality	[43]

2.5. Conclusion

This chapter brought to light a few research concerns about the privacy of health data in healthcare system. This chapter also examined existing e-health cloud system structures. Different techniques proposed for securing privacy, lying under the categories: cryptographic and non-cryptographic, were analyzed in this chapter. Also, the strengths and weaknesses of existing cryptosystems were discussed.

Chapter 3

Proxy Re-Encryption and Blockchain

3.1. Introduction

EHR data contains sensitive information. Any modification in it or any misuse can cause harmful effect. So, for any EHR system, privacy is the main key component. Different encryption techniques which can be used for the privacy protection of data were analyzed in the previous chapter.

Also, this chapter provides an overview of blockchain technology in general as well as its application in e-healthcare systems. This chapter explores blockchain, its various types, and different blockchain platforms.

Despite the benefits offered by existing blockchain platforms, the importance of Hyperledger Fabric as a significant solution for our framework's goals is highlighted in this chapter.

3.2. Proxy re-encryption

3.2.1. Data sharing Scenario

Before going any further, it's important to know that which roles are involved in the data sharing scenario. There are three basic roles in any data sharing situation [44]: data owners, data consumers, and data producers as shown in Figure 3-1.

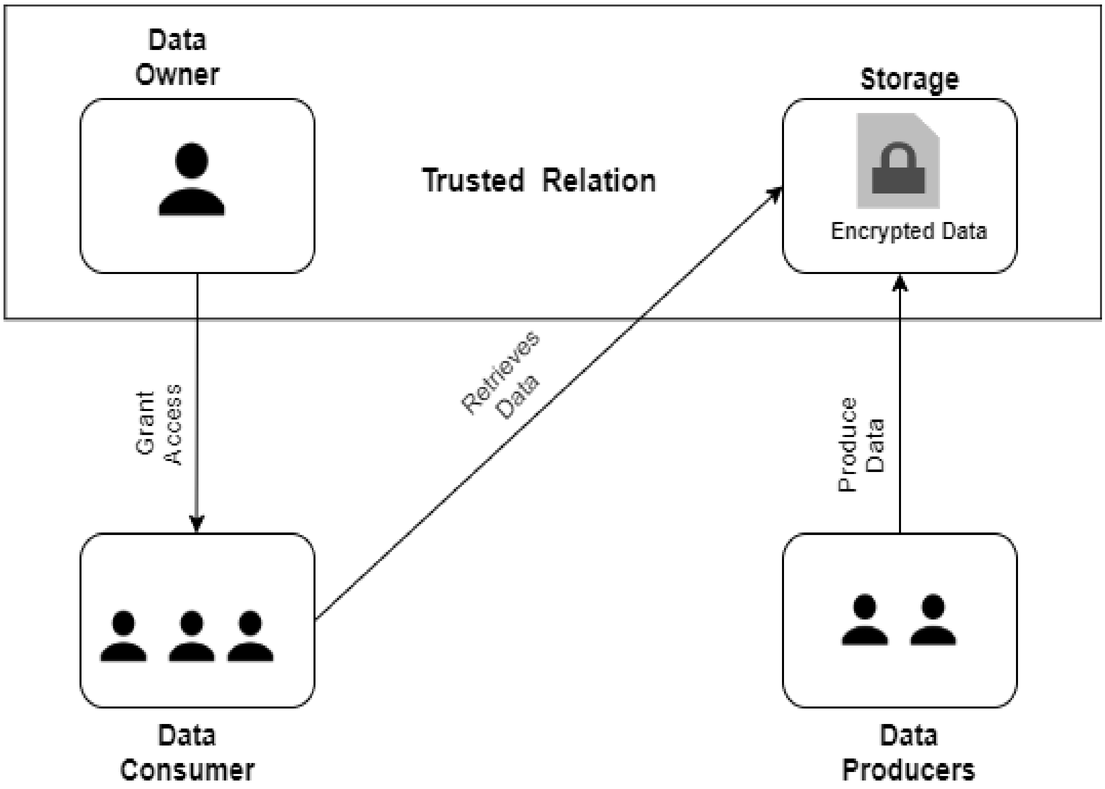


Figure 3-1: Domains in data sharing scenario

Data Producer: Entities that generate data are included in this domain. The distinction between data owner and data producer is necessary, as generation does not guarantee ownership. Data producers can protect the data from the start by encrypting it at the source.

Data Owner: Owner is the person or entity who owns the information that has to be properly shared. The data owner's primary responsibility is to authorize customer for access to his information. It's worth noting that the data owner function as a data producer.

Secure Storage: Information of the owner is stored in this storage. It is governed by the owner of the respected data. Since cloud computing is most common now a days, so this entity can be referred as cloud service provider.

Data Consumer: Legitimate recipients of the data owner's information are included in this category.

Any sensitive data, such as medical records, should be encrypted at the source. Only authorized persons should be able to decrypt it. As a result, in any scenario, the goal in terms of visibility, is for the storage domain.

For this circumstance, a simple solution would be to employ standard encryption techniques (such as RSA, AES) and distribute the decryption key with the data owner's designated parties. Its' not useful to use symmetric encryption only. Since it uses the same key for encryption and decryption. This implies that same key will be shared by the three domains: owners, consumers, producers. Due to the use of same key this encryption scheme alone is inefficient.

One of the most frequent method used is hybrid encryption. In hybrid encryption, data is encrypted by using symmetric encryption scheme and then the key which is used for symmetric encryption is encrypted by asymmetric encryption. The problem is that the producers in advance don't always know who the encrypted data's intended user is.

As a result, they have no choice but to encrypt the data using a common public key controlled by the data owner. This means that the data owner must first decrypt the information before re-encrypting it using the intended users' key. This solution demands data owner's availability online to re-encrypt the data as needed. When several types of data, as well as a variety of producers and customers, are included, the problem becomes much more complicated. To solve this challenge, various cryptosystems have been proposed. One of the most well-known option is Proxy Re-Encryption.

3.2.2. PRE-In Detail

PRE is a type of public-key encryption in which a proxy is involved. Proxy can change ciphertexts without knowing anything about the underlying data. As a result, proxy re-encryption can be considered a way of securely delegating access to encrypted data.

Basic principle of proxy re-encryption is defined by a proxy's ability to modify ciphertexts. Proxy contains the re-encryption key to implement this cryptographic scheme. It cannot access any information about the encrypted data.

At least three parties are involved in a typical proxy re-encryption scenario as shown in Figure 3-2.

1. Delegator
2. Delegatee
3. Proxy

Delegator: One who uses proxy re-encryption to assign his decryption rights can be termed as delegator. The delegator is usually known as "Alice."

Delegatee: The delegatee is given the authority to decrypt cipher-texts that proxy provides him by the consent of delegator. The delegatee is usually known as "Bob".

Proxy: Proxy is responsible for the re-encryption process. It converts ciphertexts decryptable with the delegatee's private key into ciphertexts encrypted with the delegator's public key. During this procedure, the proxy re-encrypts the cipher text, so it cannot learn any extra information.

So, PRE based encryption can be a secure solution for data sharing scenario. Data producers (entity with the correct public key) encrypt private data before sending it to a semi-trusted proxy (that can be cloud storage). The data owner effectively authorizes data consumers. By establishing and supplying the required re-encryption keys to the proxy, access to the data is granted to the delegatee. These access delegations are enforced by the proxy through a re-encryption operation that uses the associated re-encryption keys. However, information remains confidential for unauthorized parties and the proxy.

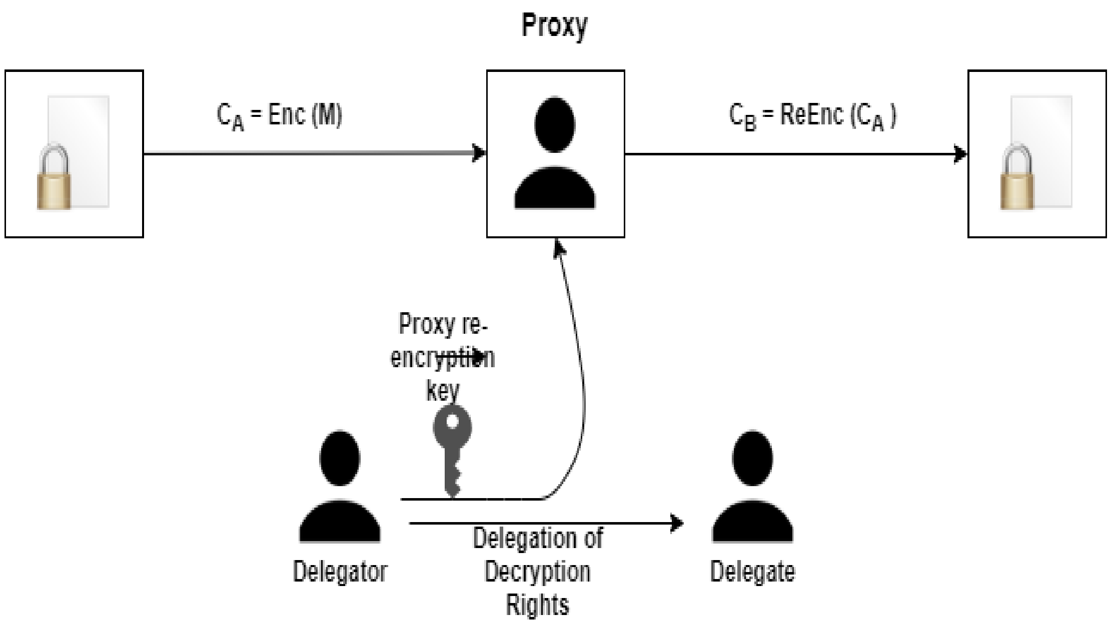


Figure 3-2: A proxy re-encryption process

The re-encryption key is made up of the delegators' private key and the delegatees' public key. In general, there are two types of functions in a PRE scheme as shown in figure 3-3 [44]:

1. One that produce key material (KeyGen & ReKeyGen)
2. One that handles ciphertexts and messages (Enc, ReEnc &Dec)

PKE functions can be defined as:

KeyGen: It generates public and private keys in pairs.

Encryptor: It creates a ciphertext that encrypts a message with the use of a public key.

Decryptor: It uses the associated secret key to decipher the ciphertext

A PRE scheme also includes the following function to support re-encryption:

ReKey- Gen: For Alice and Bob, this generates a re-encryption key. This key is used by Proxy to convert ciphertexts intended for Alice into ciphertexts that Bob can decrypt with his secret key.

3.3. Blockchain

3.3.1. Background

The healthcare business now has the power of data integrity thanks to a blockchain-based solution. Figure 3-3 depicts a typical blockchain architecture.

Blockchain is a decentralized, immutable ledger. It consists of sequence of transactions called blocks' which are linked together to form a chain. Blockchain is protected by cryptographic techniques based on public key encryption [45][46]. Because the blocks are linked, once the data has been entered, it cannot be changed without affecting all following blocks. The blocks are also hashed with a cryptographic hash algorithm to provide anonymity, immutability and tamper resistance [47]. Because it forms a ledger that records and stores all network transactions. Every network peer has a complete copy of the ledger, which is broadcast to the rest of the network whenever new transactions occur. Furthermore, blockchain utilizes the consensus protocol mechanism to originate, update, and validate transactions [48].

3.3.2. Models

Over the last few years, blockchains have taken on a number of forms, depending on their design and setup. The data held on the blockchain, as well as the actions performed by the people involved in blockchain networks, can be controlled depending on how the blockchain is built. Public and private blockchains are the two most common types of blockchains. They have been widely used by many business and cryptocurrency networks. Permissioned blockchains, a third kind, has also gained popularity. Let’s have a look at the characteristics of public, private and permissioned blockchain.

Public Blockchain: In a public blockchain, anyone can join and participate in the blockchain network (such as Ethereum, Bitcoin), since public blockchain has no network boundaries. Anyone can read, write, and audit the current operations on the public blockchain network, which helps it maintain its self-governing nature. Since transactions in public blockchain are transparent, this is not ideal for the healthcare industry, as it deals with sensitive health records.

Private Blockchain: To assess whether a new node should be added to the network, private blockchain employs an access control approach [49]. A private blockchain implementation can be used to run a blockchain that only allows certain certified parties to enter, such as for a private company. A participant can only join a private network if they have received an authorized and authenticated invitation.

Permissioned Blockchain: The third form of blockchain is permissioned blockchains. Permissioned blockchains combine private and public blockchains. It offers different range of options e.g., allowing anybody to join the permissioned network after adequate identification verification and providing specific permissions for the particular network operations. These blockchains are established such that each participant has their own set of rights. Users can read, write, and access data on blockchains because of this. Permissioned blockchain networks are getting popular among organizations because they enable them to set boundaries while creating the networks and governing the activities of the numerous users in the relevant roles.

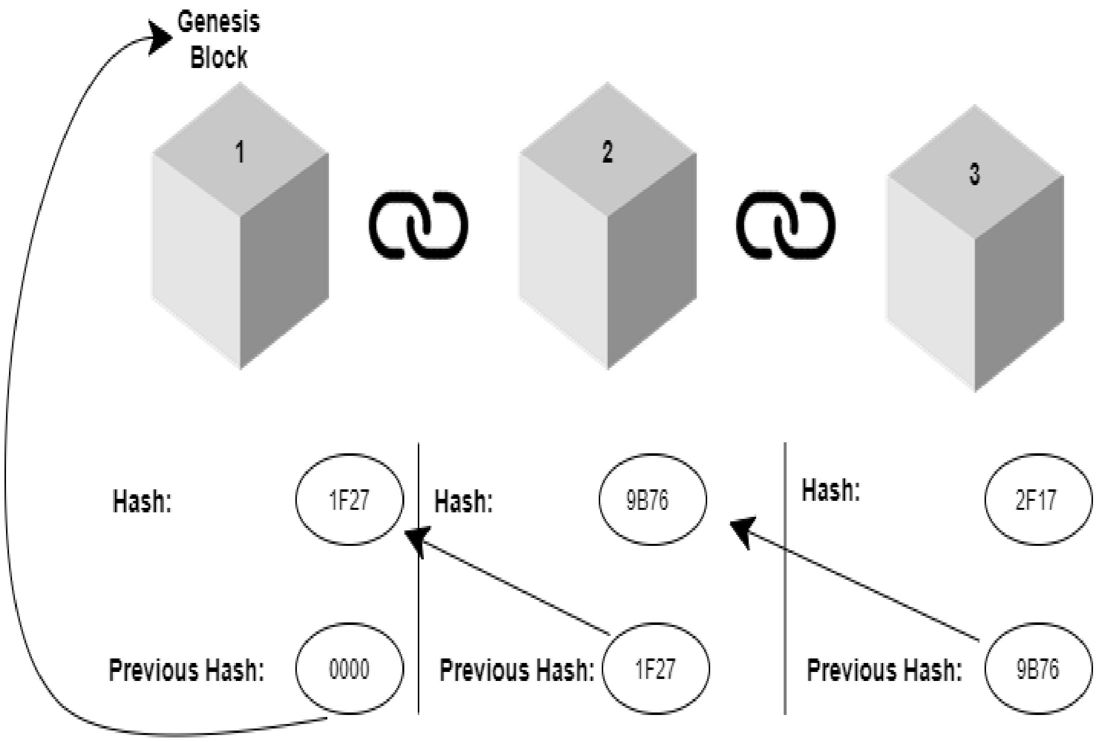


Figure 3-3: Blockchain overview

3.3.3. Hyperledger Fabric: A Permissioned Blockchain

Hyperledger Fabric is the type of permissioned blockchain for enterprise blockchain applications developed by IBM and the Linux Foundation. It features smart contract capability, a consensus mechanism, scalability, confidentiality, and resiliency. It has a ledger, employs smart contracts, and serves as a means for participants to manage their transactions, just like other blockchain technologies. Key features of Hyperledger fabric which ensures its promise of a corporate blockchain solution that is both comprehensive and customizable are:

1) **Assets:** Asset definitions allow nearly anything with a monetary value to be exchanged over the internet. The tangible (hardware) and intangible (intangible

assets) are examples of assets (contracts and intellectual property).

2) **Chain-code:** The business logic that defines an asset, as well as the transaction instructions for changing the asset, are referred to as chain-code. Chain-code enforces the rules for accessing or modifying key-value pairs or other state database information.

3) **Privacy:** Hyperledger Fabric uses an immutable ledger as well as chaincode to edit and modify the current state of assets on a per-channel basis. It can be shared across the entire network based on the assumption that everyone is using the same channel. It can also be privatized to only allow a small number of people to participate. These participants would build a separate channel in the latter scenario, isolating and segregating their transactions and ledger.

4) **Consensus:** Consensus is the full-circle verification of the accuracy of a group of transactions that make up a block.

5) **Ledger Features:**

A sequential, tamper-resistant ledger records all state transitions in the fabric. Every transaction creates, updates, or deletes a collection of asset key-value pairs in the ledger. A chain is utilized to maintain track of current fabric state and a state database is used to store immutable, sequenced records in blocks. Each channel has its own ledger. For each channel in which they participate, each peer keeps a copy of the ledger.

6) **Security & Membership Services:**

Users may trust that all transactions will be identified and traced by authorized authorities and auditors thanks to permissioned membership, which provides a secure blockchain network.

3.3.4. Hyperledger Composer

Under the Hyperledger initiative, Hyperledger Composer is a collection of open-source tools that allow business owners and developers to build blockchain applications and smart contracts to solve business challenges. Hyperledger Composer is written in Javascript, a platform that allows for the usage of built-in libraries as well as the use of existing functions and scripts to make the utilities more scalable. Composer is a development tool that simplifies and accelerates the creation of Hyperledger fabric blockchain apps. So, in a nutshell, it's a tool that enables developing Hyperledger fabric blockchain apps simpler and faster.

The Hyperledger Composer project is deprecated as of August 2019, which means that while it is still in use, no one is actively developing new features or providing support [50]. Due to increase in irreversible differences between the Composer modelling technique and Fabric technology, the project has been deprecated. Hyperledger Composer is End of Life, as of August 2021 [51].

Due to deprecation of Hyperledger composer, Astrakode blockchain is coming into light.

3.3.5. AstraKode Blockchain

The AstraKode Blockchain platform is the appropriate low-code platform for enterprise blockchain solutions. It provides:

1. **Network Composer:** For the building of custom blockchain networks, a visual environment is provided.
2. **Smart Contract IDE:** Smart contract development in a visual environment, is provided.
3. **Cloud Deployment:** To implement and manage networks and smart contracts,

a testing environment and integration with the major cloud service providers, is provided.

Different features of AstraKode blockchain are [52]:

1. Native support for the most common permissioned blockchains (at first, only for Fabric).
2. Custom networks and smart contracts may be designed and developed with speed and ease.
3. Inside one platform, the capacity to design, build, and deploy a production-grade solution.
4. Its low-code strategy facilitates project self-documentation and validation.

3.4. Conclusion

In this chapter, a general overview of proxy re- encryption scheme has been viewed. It is an asymmetric cryptosystem which allows user to share their data with others through a proxy. Even though a proxy is used to share data, the data is not visible to the proxy. As a result, the method of proxy re-encryption is an effective approach for developing a secure data sharing scheme.

Also, this chapter gives a quick overview of blockchain, as well as the types of blockchain. A brief review of Hyperledger fabric and Hyperledger composer has also been discussed. Moreover, AstrtaKode blockchain has been introduced, as Hyperledger composer has been deprecated.

Chapter 4

Proposed Framework

4.1. Introduction

EHR systems will interact with different types of users such as doctors, researchers, patient etc. So, an access control mechanism is required for accountability (which action is performed by which user in a system). As a result, the EHR system must be resistant to tampering and secure the privacy of the EHR owner. The EHR system's underlying cloud infrastructure is described as semi trusted in our model, and further security is provided by the blockchain and other cryptographic techniques.

The proxy re-encryption has been used to protect the privacy of data. Cloud storage is used for storing the electronic health record data. Using proxy cryptography, the EHR data will be encrypted and preserved on a cloud storage. A private blockchain will be used to store the associated metadata. The properties of EHR data will be maintained and stored in the blockchain. All data manipulation will be identified and validated as a result. Astrakode blockchain is used for this prototype. In this chapter, the proposed model will be explained.

4.2. System Architecture

The general architecture with different institutions is shown in Figure 4-1. A same channel is shared between different hospitals. Departments within the organization can built separate channels according to their needs. Medical data is generally too big to be handled on a ledger directly. As a result, data is saved in a separate EHR database, and the ledger simply contains the address. This storage type is referred to as on-chain or off-chain storage depending on whether the data is stored in a ledger or not [53]. A ledger is used to keep track of electronic health data hash values. This protects the integrity of the data as the data written on a ledger is irreversible.

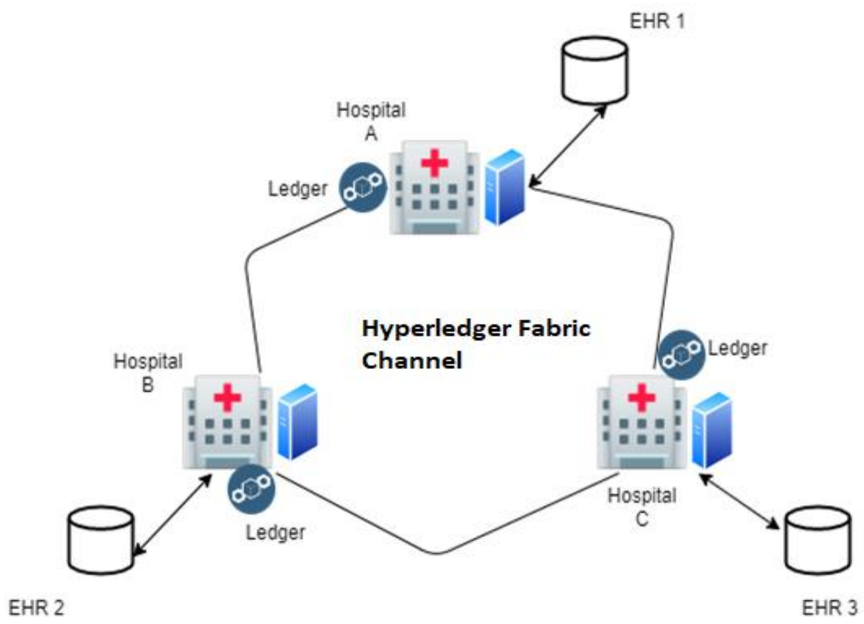


Figure 4-1: General architecture of proposed framework

Figure 4-2 depicts the suggested model's overall detailed architecture. To preserve confidentiality in our framework, The EHR master key (owner's public key) will be used to encrypt the real EHR data and this encrypted data will be kept in a cloud storage. A proxy re-encryption process will be used to share the EHR. So, gateway server also known as proxy server will contain the re-encryption keys as well as other authentication information The metadata of electronic health records will be kept on a blockchain, for help in the search and for providing tamper resistance feature. AstraKode blockchain, that basically implements Hyperledger fabric, has been used to support our framework. EHR data can be accessed by the EHR owner or other healthcare providers such as doctors, nurses etc.

Our framework includes following entities as follow:

EHR Owner:

EHR owner is the person to whom the EHR data is related. Owner wishes to store and access the data in a secure manner. EHR owner has complete control on his/her EHR information. The data can only be upload or modified by the user, only if the owner has authorized him to do so.

Gateway server:

This gateway server will act as a proxy server. Proxy server performs tasks such as re-encryption of EHR data, preserving metadata, adding the metadata's link to the blockchain.

User(U):

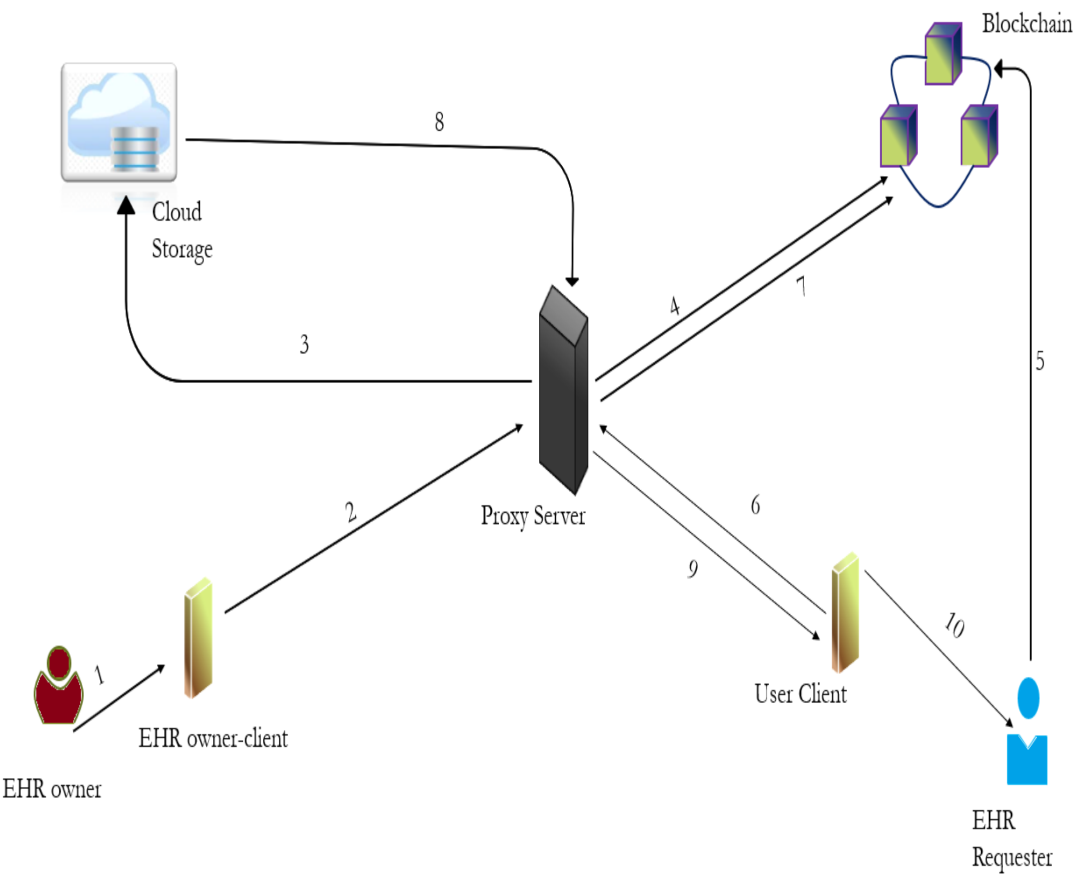
A user is a person or entity who asks access to EHR data with the consent of the EHR owner. Typical users can be doctors, nurses etc. One can use the blockchain to search for and obtain metadata, and then request to access EHR data from the proxy server. User can update or add new EHR data, if delegated authority is given to them.

Cloud Storage (CS):

It is in charge of storing the encrypted EHR data itself.

Blockchain (BC):

It is in charge for storing the system's metadata. Also, it is used for accessing the record. Hyperledger fabric and AstraKode blockchain has been used for this framework.



1) EHR owner sends encrypted data and other information through EHR owner client to the proxy server.
2) Proxy server receives the all information along with encrypted EHR.
3) Proxy server sends the encrypted EHR to the cloud storage.
4) Proxy server sends meta-data and hash of the encrypted data to the blockchain.
5) User searches meta-data of the required EHR.
6) User requests encrypted EHR through user client.
7) Proxy server stores request information of user.
8) Proxy server retrieves encrypted EHR from cloud server.
9) Proxy server sends encrypted EHR after re-encrypting it with the proxy re-key.
10) User receives plain text iof data through user client.

Figure 4-2: The detailed architecture

4.2.1. Proposed Model: Workflow

In this section, the proposed model's workflow will be presented. Consider the following scenario's:

- Storing EHR
- Retrieving EHR

4.2.1.1. Storing EHR

The EHR data storing process will be as shown in Figure 4-3:

1. The hash of the data is calculated once a new record about EHR data is created. This is done to provide data integrity verification of EHR in the system. Using the hashing algorithm, this hash will be calculated.
2. Data is encrypted using public key of EHR owner.
3. Metadata for EHR is created. This data is created to provide a search feature for electronic health records.
4. By signing hash of the record with the EHR owner private key, the digital signature is formed.
5. For each person that has access to the EHR data, re-encryption keys are generated. That person will be added to the access list of the users, who are allowed to access the data.
6. The EHR owner's private key is combined with the user's public key to form the re-encryption key.
7. The proxy server receives the CT (encrypted EHR), metadata, message digest, access list and signature.
8. The EHR owner signature is authenticated by the gateway server.
9. The encrypted EHR will then be uploaded to cloud storage and the encrypted

data's link is gathered.

10. The proxy server then assigns the data-id and that id is then associated it with a link.

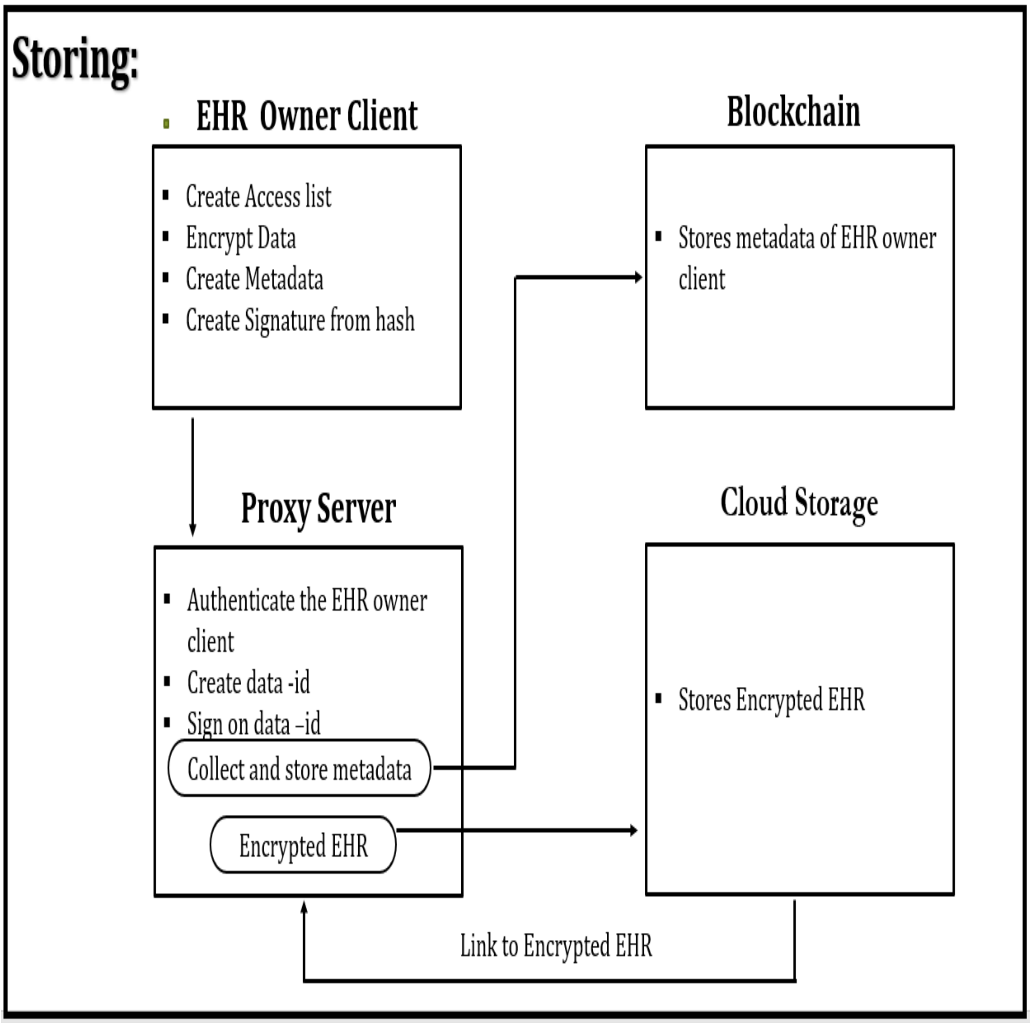


Figure 4-3: Process for storing the data

11. On the proxy server, the data-id, access list and link to the data, are all stored.
12. The gateway server then signs the data-id with its signature.
13. At last, these things are kept on blockchain: hash of electronic health data, metadata, id of the data and signature of the owner and proxy server.

4.2.1.2. Retrieving EHR

EHR data can retrieved as shown in Figure 4-4:

1. The metadata available on the private blockchain can be used to obtain information about the required EHR data, by the user.
2. User can verify data through the signatures of the owner and proxy server.
3. The user then signs it if the meta data related to his required EHR data is accurate.
4. The user then sends the proxy server the signed data-id, to retrieve the actual EHR data.
5. The user signature is used by the proxy server to verify the user's authenticity.
6. Proxy server checks whether the user is authorized to access the required EHR data or not.
7. The proxy server then uses data-id to obtain data from the cloud
8. Then re-encryption is done by the proxy server using re encryption key of the user so that requested encrypted EHR data is provided to the user without the disclosure of actual EHR data to the proxy server
9. The proxy server will retrieve the re encryption key from the access list. It will then modify the encrypted data so that the requester(user) can decrypt it. Ciphertext A(C_A) will be converted into Ciphertext B(C_B).
10. After that, new ciphertext (C_B) is sent to the requester who has made the request.
11. User can decrypt C_B by using his secret key.

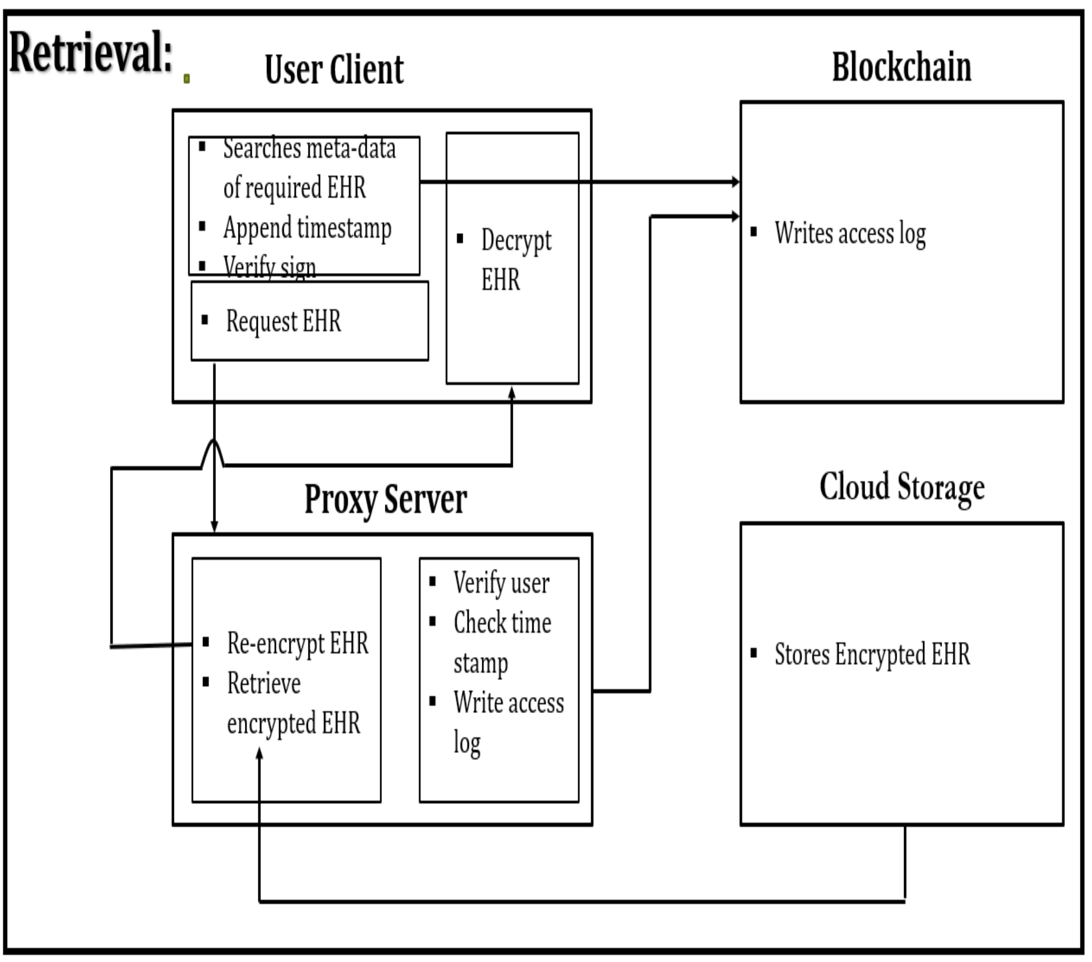


Figure 4-4: Process for retrieving the data

4.3. Conclusion

In this chapter, a blockchain-based model has been proposed for secure sharing of EHR using proxy re- encryption scheme. The proposed approach addresses the EHR system's requirements. The qualitative need of tamper-resistant storage, as well as the functional need of revocable access control, are required to maintain privacy in the EHR system. The blockchain provided the tamper-resistant property while proxy re-encryption is used for the privacy of EHR.

Chapter 5

Implementation and Analysis

5.1. Introduction

A framework was proposed for the secure sharing of EHR in the previous chapter. This chapter presents the implementation of proxy re-encryption and Hyperledger fabric on AstraKode blockchain. The suggested model's performance and privacy and security analysis are analyzed in this chapter. Also, a comparison is shown between proposed scheme and existing techniques.

5.2. Implementation

5.2.1. Proxy re -encryption

A proxy re-encryption code given by [54] was executed by making few changes in the code. System specifications, on which this code was executed, are given in Table 5-1.

Table 5-1: System Specifications

Version	Ubunto 14.04 LTS (Linux installed on virtual machine)
Assigned RAM (Virtual Machine)	2.5 GB
Processor	Core i5, 10^{th} Generation, 160 GHz
OS-Type	32-bit

In the Figure 5-1, encryption, re-encryption, decryption, and the re-keys (produced for the users) can be seen.

```
Encrypt...
r => 21925284358800119198629026456207694960565603959 3
sigma => [2356637938545578155598000505408758280378454456634308652719030445301423
0825499735999804443859371099726830493898641713118174781205375159093339924984796 3
1286, 7176552598926748702314400202858205340434627354643560376871151051840115820 4
8975504509954042742383503730724035124208568286990490722330745839066653873602999 0
]
enc_M => 13876633263561410002727386034713559888 1
('time(ms):', 35.249948501586914)

Re-encryption key for id1 => 'nikos fotiou' to id2 => 'test user2'
N => 5244933319073973063162069422354669011703462348697659048019949888923348607 06
9379842219217057932720395532646301984757151100269419922837046152309686069588034 6
4205890242164428646999349247678921325724638301072735612729575812472608891898014 9
64260254700610187746444318485723627061235962656781282808842713301087041 39
K => [6785677512188899204875602254629778116168054717458379706925288381328018687 0
3612869449213506620100167968275886414908949423884463600849727304829353906350883 5
, 840635679288212934198524557079825119827283824683694471454410903203353729550088
750647162131430302643104163501466772881016810908020051228800077428013652161 4]
('time(ms):', 14.209985733032227)
Re-Key generation for 2 users

Re-ncrypt...
H => [5123755417845272500815035052540649311360459875276321653137765412897101399 6
6748665076931711066273437708060146082418157182215901282320960235642584684143085 2
, 7259146977479586751990087147414511851428170394791460148084764513910324297479 67
942404688953217393835145137257256602454237649798483900164895507325625024160]
t => 401066941719880588748546044052526489945639446089
B' => [3211790155759030791894644817500788373397674513445203360636776826239607616
8541069434260523375707280913019996376975243115573493998764347978019979242324659 3
9, 263525928759718654652875172108843767346481568499800344276453472294597683163 60
14012359116615390839783384529385316807966983652219303526875707057421316837211]
('time(ms):', 22.98903465270996)


Decrypting Second Level...
K => [6785677512188899204875602254629778116168054717458379706925288381328018687 0
3612869449213506620100167968275886414908949423884463600849727304829353906350883 5
, 840635679288212934198524557079825119827283824683694471454410903203353729550088
750647162131430302643104163501466772881016810908020051228800077428013652161 4]
sigma => [2356637938545578155598000505408758280378454456634308652719030445301423
0825499735999804443859371099726830493898641713118174781205375159093339924984796 3
1286, 7176552598926748702314400202858205340434627354643560376871151051840115820 4
8975504509954042742383503730724035124208568286990490722330745839066653873602999 0
]
hello world!!!!!
('time(ms):', 20.124197006225586)
Successful Decryption!
```

Figure 5-1: A Proxy Re-encryption Implementation

5.2.2. Blockchain

An environment for implementing Hyperledger fabric was created on AstraKode blockchain as shown in figure 5.2. Hyperledger fabric version 2.2 is implemented. Three organizations (Hospital A, Hospital B, Hospital C) are involved in this network. Two consortium channels are formed. One is between hospital A and Hospital b. Other one is between Hospital A and Hospital C. Ordering service is defined for both the channels separately.

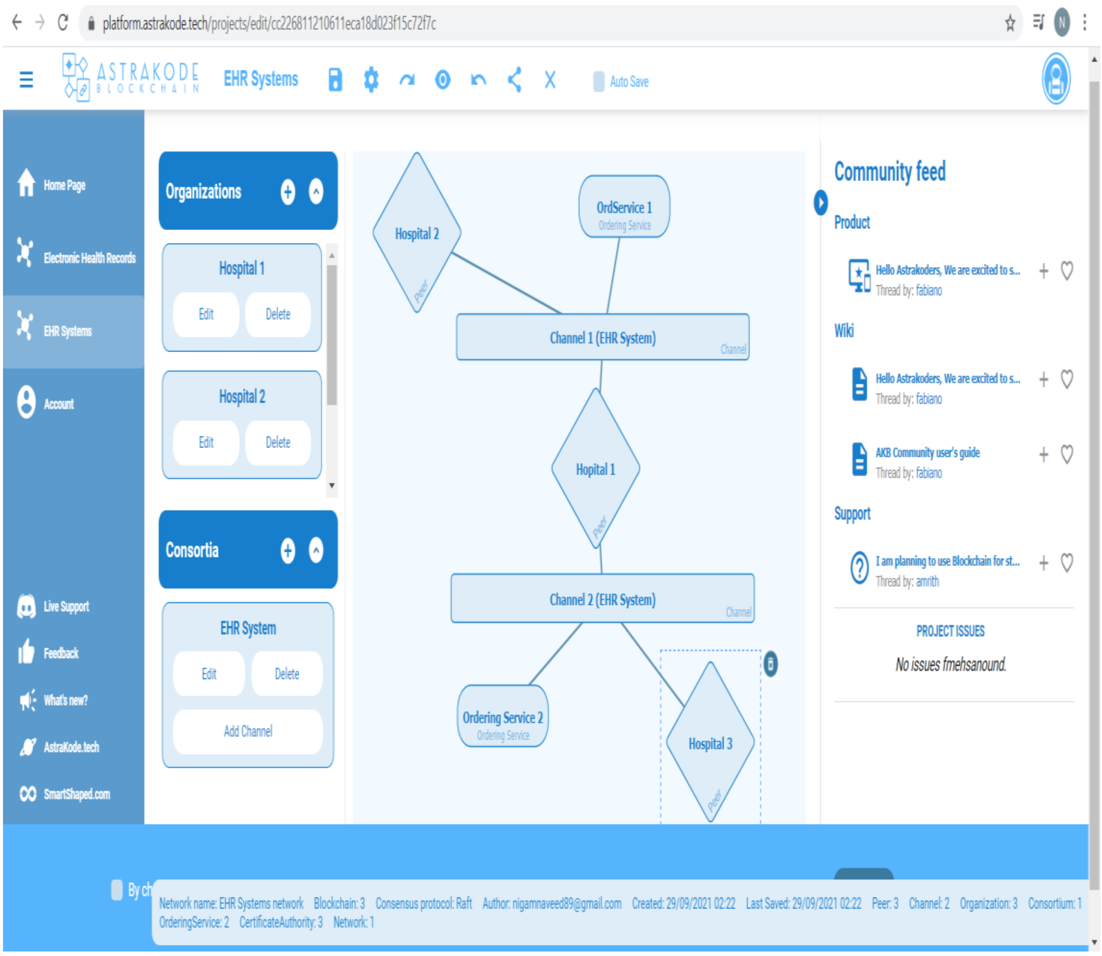


Figure 5-2: Blockchain network on AstraKode blockchain

5.3. Analysis:

5.3.1. Performance analysis:

Time taken by encryption, decryption, re-encryption, and production of re-keys was noted for different no. of users as shown in Figure 5-3.

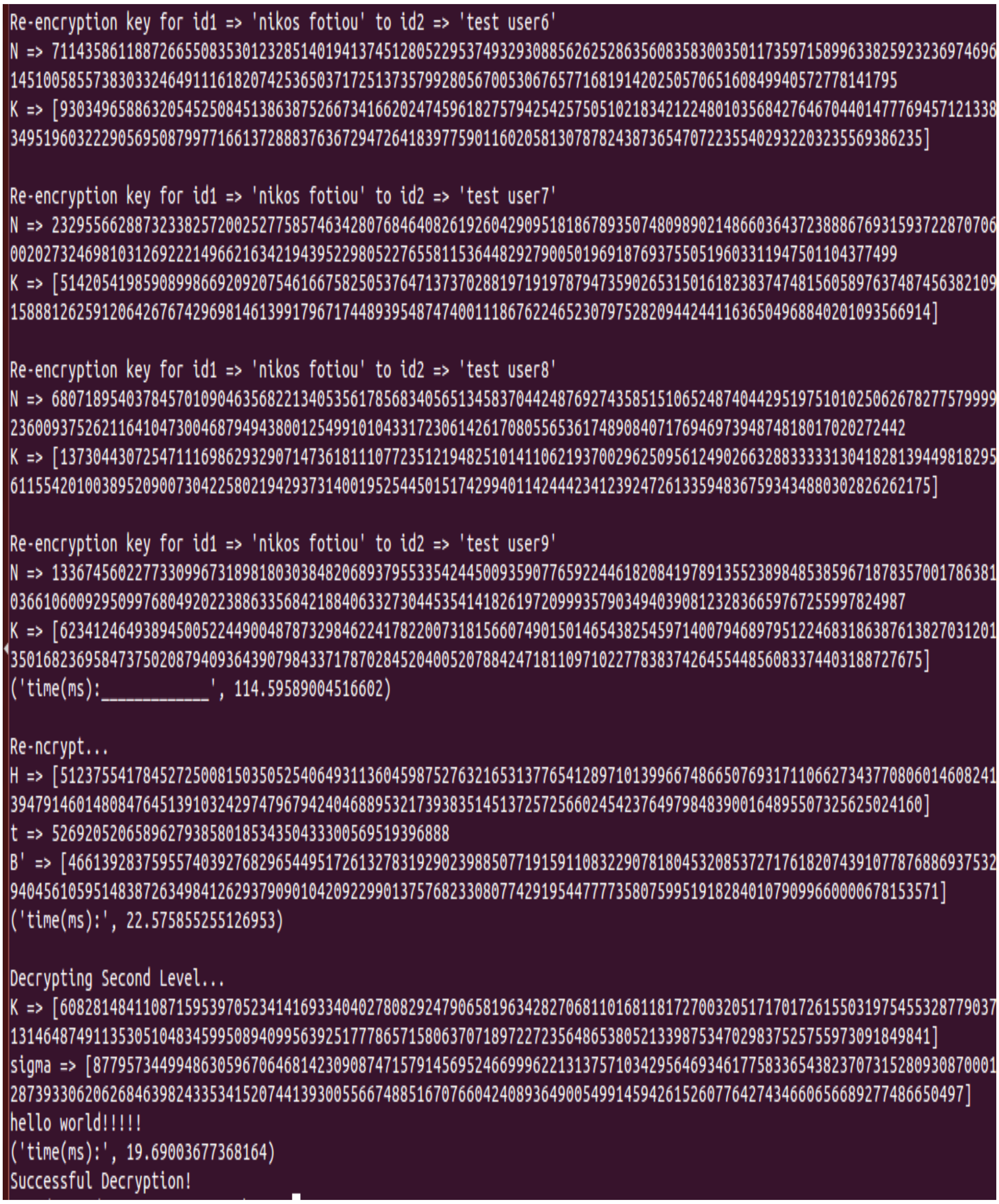


Figure 5-3: Proxy Re-Encryption Performance Analysis

It can be analyzed from the Table 5-2 that this encryption takes very less time for execution. Also, we can see that encryption and decryption time for different users remain same. This is because proxy re encryption process is performed on individual basis, not on group basis.

Table 5-2: Time analysis of Proxy Re-Encryption

No. of Users	Reg Key (ms)	Encryption Time (ms)	Re-encryption (ms)	Decryption Time (ms)
1	14.74	35.41	23.9	16.69
2	28.33	35.41	38.6	16.69
3	44.26	35.41	42.9	16.69
4	58.06	35.41	57.8	16.69
6	88.61	35.41	69.4	16.69
8	120.77	35.41	80.9	16.69

5.3.2. Privacy and Security Analysis

The following is how the security and privacy analysis is carried out. A few cases have been presented.

5.3.2.1. Case 1

Tampering attack:

The suggested EHR approach is resistant to security attacks such as data alteration by a third party.

Threat model:

The adversary intends to modify certain medical data, such as diagnosis report, lab test etc., in the EHR system.

Argument:

The EHR data is present in encrypted form on a cloud server. The proxy server is the only one that knows about the encrypted EHR link. The true encrypted EHR data cannot be tampered with by the opponent. Even if the attacker changes the encrypted EHR data, the blockchain hashing property will detect such actions.

5.3.2.2. Case 2

Malicious access attack:

The proposed EHR approach is resistant to security threats such as access to unauthorized user.

Threat model:

A malicious user wants to access the EHR data without any permission.

Argument:

For the decryption of EHR data, the user must comply with the access control list. To begin, the user must search the private blockchain for the data-id. The adversary will be unable to access the private blockchain unless they receive a valid identification certificate from an authorized user. The proposed model uses a proxy server to secure it against malicious readers and writers. The proxy server first verifies from the access list that whether the user who has requested to access the data is authorized or not. Also, proxy re encryption key, used to perform re encryption process, is available for authorized users only. So, proxy server can only reencrypt the encrypted EHR with the re encryption key, for authorized users. So, this process prevents access to the unauthorized users.

5.3.2.3. Case 3

Collusion attack:

The suggested EHR approach is protected against a security attack such as adversary-gateway server collusion.

Threat model:

The proxy server performs the process of reencryption. The adversary and the proxy server can team up to get the original EHR data. Also, proxy server can re-encrypt the EHR for the attacker.

Argument:

The information about the secret key of the owner which is used for generating the re key is not known to the proxy server. So, the proxy server cannot re-encrypt the data for the attacker. Since the secret key is in the EHR owner's possession, the proxy server's re-encryption keys are produced by the EHR owner only. So, a re-encryption key for the attacker could not be produced by the proxy server.

5.4. Comparison of proposed scheme with the existing techniques

A comparison between our scheme and different schemes proposed in [55], [56], [57], [58], is shown in Table 5-3.

Table 5-3: Comparison between proposed scheme and existing schemes

Properties	Liu [55]	Wang [56]	Sandro [57]	Liu [58]	Proposed scheme
Blockchain based	×	×	✓	✓	✓
Access control	✓	✓	✓	✓	✓
Authentication	×	✓	×	×	✓
Privacy preservation	✓	✓	✓	✓	✓
Secure search	×	✓	×	✓	✓
Collision resistance	✓	×	×	×	✓

5.5. Conclusion

In this chapter, to guarantee that our original goals are met, the suggested model's privacy and security are examined using three models: a collusion attack, a tampering attack, and a malicious access. Also, performance analysis of proxy re-encryption has been analyzed by implementing this scheme. A blockchain network was built on AstraKode blockchain.

Chapter 6

Conclusion & Future Work

This chapter concludes the thesis by summarizing the research study's major contributions, as well as its limitations. We will see how this research can further be carried out in future.

6.1. Conclusion

In recent years, privacy breaches and illegal access to EHR data in healthcare systems have been reported. Misuse of EHR data has the potential to damage patient and lower health-care quality. Security is a big concern because the majority of the data is insensitive and absolutely confidential. This study also looked into the best way to transmit confidential information amongst multiple members in a secure way. For this purpose, a framework is proposed using blockchain and proxy re-encryption scheme. The suggested framework was implemented. The proposed framework is also compared with the existing techniques. Security and privacy analysis as well as performance analysis of the proposed framework has also been discussed.

6.2. Future Work

In the healthcare industry, blockchain is still in the development stage. In 2016, the first research literature in this topic was published. A wide range of research opportunities exists for the healthcare sector.

Moreover, all the previous research done to implement Hyperledger fabric is on Hyperledger composer. But Hyperledger composer has been deprecated now. It’s time for Astrakode now. To the best of my knowledge, no research is done on the AstraKode Blockchain till now. A lot of research can be carried out on Astrakode blockchain.

REFERENCES

[1] Chenthara, S., Wang, H., and Ahmed, K. (2018). Security and privacy in big data environment.

[2] Thatcher, C. and Acharya, S. (2018). Pharmaceutical uses of blockchain technology. In *2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)*, pages 1–6. IEEE.

[3] Kruse, C. S., Mileski, M., Vijaykumar, A. G., Viswanathan, S. V., Suskandla, U., and Chidambaram, Y. (2017a). Impact of electronic health records on long-term care facilities: Systematic review. *JMIR medical informatics*, 5(3).

[4] Griebel, L., Prokosch, H.-U., Köpcke, F., Toddenroth, D., Christoph, J., Leb,I., Engel, I., and Sedlmayr, M. (2015). A scoping review of cloud computing in healthcare. *BMC medical informatics and decision making*, 15(1):17.

[5] Li, P., Guo, S., Miyazaki, T., Xie, M., Hu, J., and Zhuang, W. (2016a). Privacy-preserving access to big data in the cloud. *IEEE Cloud Computing*, 3(5):34–42.

[6] Matturdi, B., Zhou, X., Li, S., and Lin, F. (2014). Big data security and privacy: A review. *China Communications*, 11(14):135–145.

[7] Katal, A., Wazid, M., and Goudar, R. H. (2013). Big data: issues, challenges, tools and good practices. In *2013 Sixth international conference on contemporary computing (IC3)*, pages 404–409. IEEE.

[8] Chenthara, S., Ahmed, K., Wang, H., and Whittaker, F. (2019). Security and privacy-preserving challenges of e-health solutions in cloud computing. *IEEE access*,7:74361–74382.

[9] Ahmed, M. and Ullah, A. S. B. (2017). False data injection attacks in healthcare.

[10] Yi, X., Miao, Y., Bertino, E., and Willemson, J. (2013). Multiparty privacy protection for electronic health records. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 2730–2735. IEEE.

[11] Sandhu, R. S., Coyne, E. J., Feinstein, H. L., and Youman, C. E. (1996). Role-based access control models. *Computer*, 29(2):38–47.

[12] Yuan, E. and Tong, J. (2005). Attributed based access control (abac) for web services. In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*. IEEE.

[13] Zhu, L., Zhang, C., Xu, C., Liu, X., and Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. *IEEE Access*,6:19025–19033.

[14] Zhu, L., Zhang, C., Xu, C., Liu, X., and Huang, C. (2018). An efficient and privacy-preserving biometric identification scheme in cloud computing. *IEEE Access*,6:19025–19033.

[15] haranya, R. and Aramudhan, M. (2016). Survey on access control issues in cloud computing. In *2016 International Conference on Emerging Trends in Engineering, Technology and Science (ICETETS)*, pages 1–4. IEEE.

[16] Cui, H., Deng, R. H., and Li, Y. (2018). Attribute-based cloud storage with secureprovenance over encrypted data. *Future Generation Computer Systems*, 79:461–472.

[17] Hu, V. C., Ferraiolo, D., and Kuhn, D. R. (2006). *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology.

[18] Chi, P.-W. and Lei, C.-L. (2018). Audit-free cloud storage via deniable attribute-based encryption. *IEEE Transactions on Cloud Computing*, 6(2):414–427.

[19] Kamara, S. and Lauter, K. (2010). Cryptographic cloud storage. In *International Conference on Financial Cryptography and Data Security*, pages 136–149. Springer.

[20] Huang, C., Yan, K., Wei, S., Zhang, G., and Lee, D. H. (2017). Efficient anonymous attribute-based encryption with access policy hidden for cloud computing. In *2017 International Conference on Progress in Informatics and Computing (PIC)*, pages 266–270. IEEE.

[21] Cui, H., Deng, R. H., and Li, Y. (2018). Attribute-based cloud storage with secureprovenance over encrypted data. *Future Generation Computer Systems*, 79:461–472.

[22] Chi, P.-W. and Lei, C.-L. (2018). Audit-free cloud storage via deniable attribute-

based encryption. *IEEE Transactions on Cloud Computing*, 6(2):414–427.

[23] Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, 2017(4):1–14.

[24] Li, Z.-R., Chang, E.-C., Huang, K.-H., and Lai, F. (2011b). A secure electronic medical record sharing mechanism in the cloud computing platform. In *Consumer Electronics (ISCE), 2011 IEEE 15th International Symposium on*, pages 98–103. IEEE.

[25] Ibrahim, A., Mahmood, B., and Singhal, M. (2016). A secure framework for sharing electronic health records over clouds. In *Serious Games and Applications for Health (SeGAH), 2016 IEEE International Conference on*, pages 1–8. IEEE.

[26] Pecarina, J., Pu, S., and Liu, J.-C. (2012). Sapphire: Anonymity for enhanced control and private collaboration in healthcare clouds. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 99–106. IEEE.

[27] Sahai, A. and Waters, B. (2005). Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 457–473. Springer.

[28] Bethencourt, J., Sahai, A., and Waters, B. (2007). Ciphertext-policy attribute-basedencryption. In *Security and Privacy, 2007. SP'07. IEEE Symposium on*, pages 321–334. IEEE.

[29] Rabieh, K., Akkaya, K., Karabiyik, U., and Qamruddin, J. (2018). A secure and cloud-based medical records access scheme for on-road emergencies. In *Consumer Communications & Networking Conference (CCNC), 2018 15th IEEE Annual*, pages1–8. IEEE.

[30] Bhateja, R., Acharjya, D. P., and Saxena, N. (2017). Enhanced timing enabled proxy re-encryption model for e-health data in the public cloud. In *Advances in Computing, Communications and Informatics (ICACCI), 2017 International Conference on*, pages2040–2044. IEEE.

[31] Lee, W.-B. and Lee, C.-D. (2008). A cryptographic key management solution for hipaa privacy/security regulations. *IEEE Transactions on Information Technology inBiomedicine*, 12(1):34–41.

[32] Yi, X., Miao, Y., Bertino, E., and Willemson, J. (2013). Multiparty privacy protection for electronic health records. In *Global Communications Conference (GLOBECOM), 2013 IEEE*, pages 2730–2735. IEEE.

[33] Löhr, H., Sadeghi, A.-R., and Winandy, M. (2010). Securing the e-health cloud. In *Proceedings of the 1st ACM International Health Informatics Symposium*, pages 220–229. ACM.

[34] Zhang, R., Liu, L., and Xue, R. (2014). Role-based and time-bound access and management of ehr data. *Security and Communication Networks*, 7(6):994–1015.

[35] Boneh, D., Di Crescenzo, G., Ostrovsky, R., and Persiano, G. (2004). Public key encryption with keyword search. In *International conference on the theory and applications of cryptographic techniques*, pages 506–522. Springer.

[36] Yu, S., Wang, C., Ren, K., and Lou, W. (2010). Achieving secure, scalable, and fine-grained data access control in cloud computing. In *Infocom, 2010 proceedings IEEE*, pages 1–9. Ieee.

[37] Barua, M., Liang, X., Lu, R., and Shen, X. (2011). Espac: Enabling security and patient-centric access control for ehealth in cloud computing. *International Journal of Security and Networks*, 6(2-3):67–76.

[38] Punithasurya, K. and Jeba Priya, S. (2012). Analysis of different access control mechanism in cloud. *International Journal of Applied Information Systems (IJAIS), Foundation of Computer Science FCS*, 4(2).

[39] Hu, V. C., Ferraiolo, D., and Kuhn, D. R. (2006). *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology.

[40] Yuan, E. and Tong, J. (2005). Attributed based access control (abac) for web services. In *Web Services, 2005. ICWS 2005. Proceedings. 2005 IEEE International Conference on*. IEEE.

[41] Khan, M. F. F. and Sakamura, K. (2015). Fine-grained access control to medical records in digital healthcare enterprises. In *Networks, Computers and Communications (ISNCC), 2015 International Symposium on*, pages 1–6. IEEE.

[42] Gajanayake, R., Iannella, R., and Sahama, T. (2014). Privacy oriented access control

for electronic health records. *electronic Journal of Health Informatics*, 8(2):15.

[43] Calvillo-Arbizu, J., Roman-Martinez, I., and Roa-Romero, L. M. (2014). Standardized access control mechanisms for protecting iso 13606-based electronic health record systems. In *Biomedical and Health Informatics (BHI), 2014 IEEE- EMBS International Conference on*, pages 539–542. IEEE.

[44] Nuñez, D., Agudo, I., & López, J. (2017). Proxy Re-Encryption: Analysis of constructions and its application to secure access delegation. *J. Netw. Comput. Appl.*, *87*, 193-209.

[45] Nakamoto, S. et al. (2008). Bitcoin: A peer-to-peer electronic cash system.

[46] Adams, C. and Lloyd, S. (1999). *Understanding public-key infrastructure: concepts,standards, and deployment considerations*. Sams Publishing.

[47] Sun, W., Guo, H., He, H., and Dai, Z. (2007). Design and optimized implementation of the sha-2 (256, 384, 512) hash algorithms. In *2007 7th International Conference on ASIC*, pages 858–861. IEEE.

[48] Baliga, A. (2017). Understanding blockchain consensus models. *Persistent*, 2017(4):1–14.

[49] Ahmed, M. and Ullah, A. S. B. (2017). False data injection attacks in healthcare.

[50] https://www.investopedia.com/terms/h/hyperledger-composer.asp

[51] https://www.hyperledger.org/use/composer

[52] https://www.astrakode.tech/

[53] Barni, M., Failla, P., Lazzeretti, R., Sadeghi, A.-R., and Schneider, T. (2011). Privacy-preserving ecg classification with branching programs and neural networks. *IEEE Transactions on Information Forensics and Security*, 6(2):452–468.

[54] Green M., Ateniese G. (2007) Identity-Based Proxy Re-encryption. In: Katz J., Yung M. (eds) Applied Cryptography and Network Security. ACNS 2007. Lecture Notes in Computer Science, vol 4521. Springer, Berlin, Heidelberg.

[55] J. Liu, X. Huang and J. K. Liu, "Secure sharing of Personal Health Records in cloud computing: Ciphertext-policy attribute-based signcryption", *Future Gener. Comput. Syst.*, vol. 52, pp. 67-76, Nov. 2015.

[56] X. Wang, A. Zhang, X. Ye and X. Xie, "Secure-aware and privacy-preserving electronic health record searching in cloud environment", *Int. J. Commun. Syst.*, vol. 32, pp. e3925, May 2019.

[57] S. Amofa, E. B. Sifah, K. O.-B. Agyekum, S. Abla, Q. Xia, J. C. Gee, et al., "A blockchain-based architecture framework for secure sharing of personal health data", *Proc. IEEE 20th Int. Conf. e-Health Netw. Appl. Services (Healthcom)*, pp. 1-6, 2018

[58] J. Liu, X. Li, L. Ye, H. Zhang, X. Du and M. Guizani, "BPDS: A blockchain based privacy-preserving data sharing for electronic medical records", *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, pp. 1-6, Dec. 2018.