UNIVERSITY
OF OULU

FACULTY OF INFORMATION TECHNOLOGY AND ELECTRICAL ENGINEERING

DEGREE PROGRAMME IN WIRELESS COMMUNICATIONS ENGINEERING

MASTER’S THESIS

DATA INTEROPERABILITY AND PRIVACY SCHEMES IN HEALTHCARE DATA USING BLOCKCHAIN TECHNOLOGY

Author	Vidhya Ramani
Supervisor	Erkki Harjula
Second Examiner	Tanesh Kumar
Technical Advisor	Tanesh Kumar and Ahsan Manzoor

February 2023

Ramani F. (2023) Data Interoperability and Privacy Schemes in Healthcare data using Blockchain Technology. University of Oulu, Faculty of Information Technology and Electrical Engineering, Degree Programme in Wireless Communications Engineering. Master's Thesis, 48 p.

ABSTRACT

Electronic Health/Medical Records (EHR/EMR) lay the foundation for securely maintaining medical records. The traditional EHR systems are not effectively managed data manipulation, delayed communication, trustless data storage, data cooperation, and distribution.

Blockchain technology can provide great security measure in healthcare cases. This is because it uses decentralized distributed ledgers to securely manage all parties within the network. It also handles individual data through smart contracts, which can be pre-programmed by the patient for access and maintenance of healthcare data.

This thesis focuses on exploring the blockchain in digital healthcare services such as Electronic Health/Medical Records (EHR/EMR). Blockchain-based implementations of Ethereum allow patients to store their medical data with smart contracts that can perform activities such as Registration, Data Append, and Data Retrieve. The challenges involved during the implementation of Blockchain can be discussed and analysed to find a suitable and reliable solution for the system.

Keywords: Electronic Healthcare Record, Blockchain, Smart Contract, Ethereum, Distributed Ledger, Performance Evaluation

TABLE OF CONTENTS

FOREWORD

The focus of the thesis is to study blockchain using healthcare along with the privacy schemes and implementation. The research has been supported by the University of Oulu, Finland.

First and foremost, I would like to extend my sincere gratitude to Assistant Prof. Madhusanka Liyanage and Prof. Mika Ylianttila for giving me an opportunity to work and learn with their valuable guidance and initiated the thesis and provided me the idea about Blockchain.

I am also grateful to my supervisor Assistant Prof. Erkki Harjula, Dr. Tanesh Kumar and Mr. Ahsan Manzoor for their constant support and thought-provoking discussions throughout the postgradu work. It would have been hard to design and write the research and results without their support and guidance.

I would also like to thank the entire Centre of Wireless Communication (CWC) department especially Kari Karkkainen for providing all the required equipment and a chance to learn various new technologies and different concepts.

A very special thanks is due to my friend Ayswarya Padmanabhan who suggested and inducted me into Wireless Communications Engineering programe in the University of Oulu. Having said that, thanks for all her and her husband Dr. Ganesh Venkatraman's immense encouragements, contributions, support, and discussions that we had all these days.

Finally, heartful thanks to my husband Ganapathy Raman Devarajan his patience, assistance, support, unconditional love, and faith in me. Cheers to our adorable and lovable son Vibhava Raman and daughter Viksha Raman, who has been providing endless motivation and supporting me all the time. They added meaning to my life and without any doubt your role is substantial in completing the thesis.

I dedicate this work to my husband, who has always been the most important part of my life and without his support, it would have not been possible.

Oulu, 17 February, 2023

Vidhya Ramani

LIST OF ABBREVIATIONS AND SYMBOLS

p	Patient
d	Doctor
BC	Blockchain
EHR	Electronic Healthcare Report
EMR	Electronic Medical Report
MD	Mobile Device
RC	Registration Centre
T	TimeStamp
k	symmetric key
H(.)	Hash function
M	Patient's record
id_p	Identity of patient
id_d	Identity of doctor
P2P	Peer to Peer
DS	Distributed System
pk_p	Patient public key
pk_d	Doctors private key
$\|\|$	Concatenation Operator
PoW	Proof of Work
PoS	Proof of Stake
ECDLP	Elliptic Curve Discrete Logarithm Problem
C	ciphertext
ECC	Elliptic Curve Cryptography

1 INTRODUCTION

The healthcare industry demands major criteria from people around the globe. With the development of a digital healthcare system, patient care is improving the capability to make faster and more accurate diagnosis. This is achieved by providing emergency care in a faster and more appropriate manner, preventing the duplication of prescriptions, and properly planning treatment.

With the introduction of the Internet of Things (IoT) [38] and smart healthcare, people can communicate with their doctors using remote communication. The Internet of Things allows remote monitoring to keep patients safe and healthy. Smart healthcare offers a solution to integrate all the necessary healthcare documents like lab tests, diagnoses, general check-ups, and medicine details.

Traditional healthcare systems involve centralized ICT systems. Healthcare systems governed by one point are highly susceptible to a single intrusion resulting in the loss of data. Data storage and encryption of data storage should be separate for the effective purpose. Furthermore, the number of records increases the processing time and the cost. Loss of sensitive data from unauthorized data exchange on a large scale.

1.1 Background and Motivation

The first decentralized distributed currency named BitCoin have been introduced in the year 2008 by Nakomata. The decentralized distributed currency has combined with P2P and digital services to implement Blockchain technology [3]. Initially, Blockchain technology has introduced to execute the financial platform. After the platform was successful, the technology has been explored in different platforms. Blockchain technology shows strength toward data transparency, privacy and has proven to be more successful in the IoT domain. Blockchain is a distributed and decentralized ledger for the use of verifying and storing data. The process allows one to send, receive, or update data over networks (P2P) peer-to-peer manner, leading to store large amounts of data [10][16]. A blockchain and mechanism enables decentralized system to record transactions, mainly for global usability, immutability, and other features. The concept of cryptocurrency in terms of blockchain can access the databases publicly [17]. The concept of Blockchain takes the P2P network and consensus mechanism from BitCoin protocol, which is a global decentralized shared ledger and cryptographically ensured. It specifies that the chain in the blockchain gives the security features like integrity, stability, and availability and the copy will be there in all the available nodes in the network for not losses the sensitive data. The advantages of the databases and consensus mechanism enables distributed tamper-proof ledgers. Blockchain technology is currently one of the most disruptive technologies in the field of data security.

At present, the digital economy relies on a trusted third-party channel to verify transactions and build trust among different stakeholders. In this digitally driven world, dependence on third parties has generated a whole bunch of security and privacy concerns. Blockchain technology can be considered a vital solution since it provides decentralized and distributed ways of transferring values without using immediately trusted channels. Blockchain is also considered a trustable solution for people especially the old age people.

Blockchain technology provides the transaction in a decentralized form and follows the characteristics such as decentralization, persistence, anonymity, and audibility. Trusting only the intermediates in the network allows trustable transactions for the data [1] because the blockchain includes cryptographic hash, digital signatures, and a consensus algorithm. Once the data is validated by the Blockchain network, the transactions are not modified by anyone without the proper access permissions by the concerned person signed in to the network [2].

Blockchain technology was developed to address various problems like privacy, security, and performance. Transactions are collected by nodes, and they can be made in chronological order called a block. Details of the sensitive data of the blockchain are distributed on each node in the network. A global network of validators is called miners. Miners store transactions in blocks. The network maintains a consensus algorithm using a hash to resolve what is known as a proof of work algorithm. This algorithm has a trustable model, where each node should solve the puzzle before the next block is executed. Blockchain is a linked list using hash pointers and it solves computational puzzles. Each block contains the hash of the previous block, and each block is generated every 10 minutes. The blockchain will store each transaction. Furthermore, blockchain can help users avoid repeating the same information already stored in databases.

Digital services are becoming more prevalent. Many technologies are already available for different sectors. The healthcare sector is one of the sectors with the highest expectations for digitalization [11]. People who cannot travel often to healthcare facilities and elderly patients can always use digital health services. Another reason for online medical data is that patients can meet many doctors in different locations while the information is saved in one location. In addition, patients can go to the pharmacy and do a lab test can saved in the same place. For tracking their records, all the information should be stored in a specific folder because they cannot keep all the papers at once, and patients might miss something. A doctor can check the patient's previous record online and prescribe medicines according to it if the information is on the computer. Records should have a lifetime/history to help future generations. E-healthcare systems enable people to track their health information and access it. However, patients themselves and medical personnel should have access to the medical record. In addition to security measures, also privacy measures are needed [14]. Furthermore, all healthcare data of a person should be integrated, patient data should be matched, and healthcare management should be provided.

As the use of electronic healthcare systems grows rapidly, there is an essential need for integrating the old handwritten healthcare reports to improve existing data from EHR healthcare systems. Smart healthcare systems increase the efficiency of centralized healthcare systems by storing a large amount of data and ensuring that no data is lost. P2P healthcare platforms may further lead to more benefits such as user preference and easily accessible healthcare systems. It also empowers stakeholders rather than a central authority, and the consensus mechanism helps to improve the EHR systems more efficiently.

The treatment processes for elderly patients or patients who are not able to access the record safely can believe the EHR. In the medical process, there are a variety of entities, such as medical specialists, therapists, lab technicians, general nurses, pharmacists, etc. The exchange or communication of sensitive healthcare information should be secure and occur without any data loss. Involving all these stakeholders will take time, but authenticated information can be provided to all stakeholders. These factors play a critical role in satisfying the health needs of society [12]. A secure and connected healthcare ecosystem plays an essential role in managing patients' information. To provide more privacy and security, e-healthcare can help provide longterm care and low-cost effective services. Current E-Healthcare systems still need to improve data manipulation, delayed communication, trustless data storage, data cooperation, distribution [34], and privacy of sensitive data. Thus, Blockchain-based EHR plays a major role in addressing the issues in existing healthcare systems. Figure 1 explains the blockchain process in a general way.

This thesis presents a novel approach to exploring blockchain in digital healthcare systems for the secure storage of sensitive healthcare data with security features involved within the system. Utilizing current smart technology, such as Blockchain, can enhance the productivity of healthcare systems and reduce risks. In current centralized systems, several issues could lead to the patient's sensitive medical information being compromised. Centralized approaches to managing healthcare systems, for example, prove to be challenging and not safe for patients because attackers can track and access patients' data. Blockchain technology can play a major role in such healthcare cases because of a decentralized distributed ledger can secure all entities within the network [21]. Patient access records can be created by granting access permissions to only authorized individuals. Notifies to the patient when someone tries to track their data in the Blockchain system. The main goal of this work is to employ the blockchain to enable the prospective solution for the current healthcare systems. Figure 1 illustrates how blockchain can be used in healthcare with entities such as Medical Information Systems, Dental Information, Laboratory details, Electronic Health Records, Telemedicine, neuroscience, and pharmaceuticals.

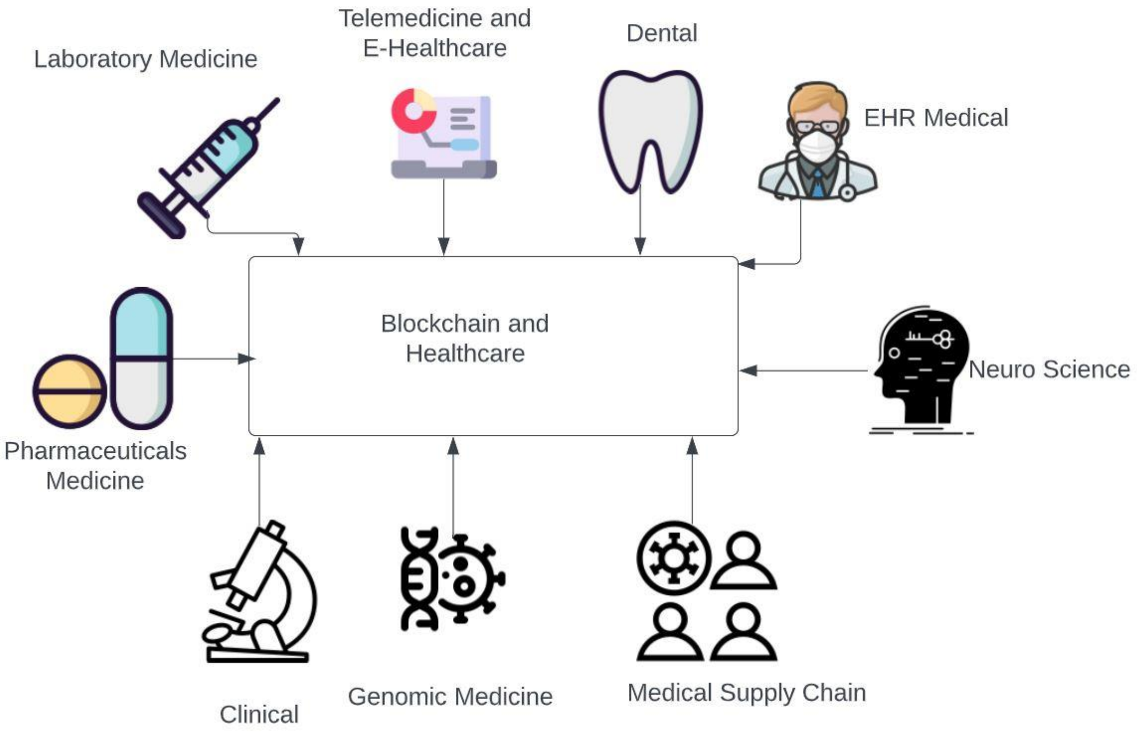

Figure 1. Blockchain and Healthcare.

1.2 Selected Scope

Globally, blockchain is a new phenomenon that ensures stress-free and effective healthcare services [4]. It can provide a secure decentralized system for healthcare data; it is crucial to safeguard patient data. Blockchain technology enables secure features for patient information [17]. Current security measures, such as biometrics, passwords, and other security features are insufficient to safeguard healthcare systems [9]. Blockchain is a potential technology to provide effective privacy and security systems for healthcare systems. Many people check their medical records on their mobile phones, which is why they are not aware of cyber-attacks which can e.g leak their passwords and other information to third parties.

The decentralized nature of blockchains attracts attackers, but these attackers cannot enter those without running cryptographic operations like encryption. Blockchain uses a cryptographic hash function for a transaction. This makes sure that the user is eligible to log in, and therefore the blockchain provides more security to prevent the loss of information. Despite its transparency, it's not easy to access data without the consent of the actual author. However, it has a trustable feature. Using e.g., an Ethereum Blockchain, the doctor and patient can write an agreement in the smart contract and ensure the proper mechanisms are used to protect the data from any third parties or hackers. Integrity, Immutability, and Interoperability are security features of this technology. Blockchain technology uses public-key cryptography to verify the identity of a patient and a doctor. That is also the reason a patient can ensure that the data is protected by securing it with keys. A security feature will prevent anyone from easily tracking the patient's record without their permission. Blockchain offers a practical solution for healthcare data by providing healthcare organizations with the ability to maintain data integrity and with the ability to maintain data security.

1.3 Methodology of the thesis

Currently, the e-health systems being implemented are mostly centralized, possess data ownership, and lack interoperability. With blockchain technology and the required system features, appears optimistic solution for healthcare systems. To proceed, it would be wise to start with the blockchain research discussed in the literature review.

In this thesis, a potential healthcare scenario considered, where the patient's healthcare record can be managed in an enhanced, secure, and smarter way. Blockchain technology secures medical data with integrity, interoperability, and privacy. Blockchain implementation in the health sector is encouraged to ensure accurate and timely data. With the proposed system, using Blockchain technology to replace current traditional smart healthcare systems. Considering the many security features of Blockchain technology, such as Integrity, Interoperability, Access Control, Scalability, etc. As traditional healthcare systems are shifting to the blockchain, many papers need to be read for better understanding and to implement the most appropriate techniques.

1.4 Contribution of the thesis

* Literature Survey of the existing work: To meet the features for enabling the security measures for healthcare systems and efficient solutions for healthcare systems can make certain security and access control for the patient's data by including the entity as the doctor to retrieve or append the patient's data with the patient's permission. These Blockchain-based healthcare systems provide some security features such as integrity, interoperability, authentication, and confidentiality.

* System Model: To present a blockchain-based healthcare system that will enable secure appending or retrieval of a patient's medical records by authorized doctors with the patient's consent by giving them access rights.

* Evaluation and analysis of the proposed system: For executing the implementation, Ethereum blockchain along with smart contracts. The analysis of the proposed system proves the security features are enables to protect the patient data.

1.5 Organization of the thesis

Section II discusses the background information of this thesis related to blockchain in healthcare as well as the basics of EHR, Blockchain, Ethereum, and Smart Contracts in more detail. Section III describes the art of the proposed system and is numerically solved using the cryptographical method. Section IV shows the performance evaluation of both patient and doctor communication with blockchain through a mobile device. It also shows numerical results for the proposed system along with the implementation process and algorithm. Discussion about the system model is defined in Section V. Section VI gives the conclusion.

2 LITERATURE REVIEW

Smart healthcare plays a crucial role in taking care of human health. Using the latest technology, it may be able to track emergency cases intelligently. Edging towards existing smart healthcare systems may also have several disadvantages, such as security features [23]. The explanation of how blockchain technology can be used in smart healthcare by utilizing its advantages to use in current healthcare systems. It has some challenges that are all explained in the previous section and solutions to the issues are also explained along with the healthcare systems [24].

The concept of EHR/EMR in Blockchain-based healthcare was initially proposed in the paper MedRec [22]. A public ledger can provide security measures both for the patient's EMR and their access permissions. MedRec also explains the security measures and performance of the system. There was a clear discussion of blockchain in healthcare, along with an architectural explanation and performance evaluation of the system, in MedRec.

The paper MedShare[30] further explores the concept of EHR with cloud services. By utilizing service providers and cloud services, the paper explains how to improve system performance. MedShare [30] also explains data authentication and data integrity, ensuring there is never any risk to the user’s healthcare systems.

The combination of blockchain-based EHR and smart contracts is very well suited to securely and effectively taking care of the patient's record [25]. Verifying the results through smart contracts is effective and understandable. The implementation of the smart contract can be done e.g., on the Ethereum platform [13]. For more security reasons, blockchain uses smart contracts to ensure patient access and users can control their accounts [27]. Ethereum smart contracts also include such as that specify more about the contracts that make them different from other contracts.

To control healthcare records, digital signatures for more secure identification and biometric authentication schemes are available [28]. In the hospital environment, many users are available for registration or regular check-ups, and this biometric authentication scheme helps to authenticate and prevent the patient’s record from attackers [33]. With password-based authentication, one can keep the signature in any form, i.e., one can store the user credentials on an external hardware device and prevent password breaches. Biometrics can be used to generate keys. Both public keys [35] and private keys are created with key generation mechanisms like RSA or Diffie-Helman. Private keys are useful for safeguarding patient information such as the privacy and confidentiality of patient records.

Mobile applications are particularly useful in healthcare [32]. In an ideal world, mobile device issues should not impact sensitive patient data or the ability of the patient's data to be accessible and smart. In this thesis, Mobile Healthcare systems help to store patients’ data using blockchain-based EHR.

2.1 Medical Information Systems

Online patient data management is provided by medical information systems. This allows the patient to collect, store, manage and transmit patient data to their hospital or to whomever they it needs to be delivered to. Security is the primary concern for medical information systems because medical information systems commonly access, process, or maintain a large volume of patient-sensitive data [14].

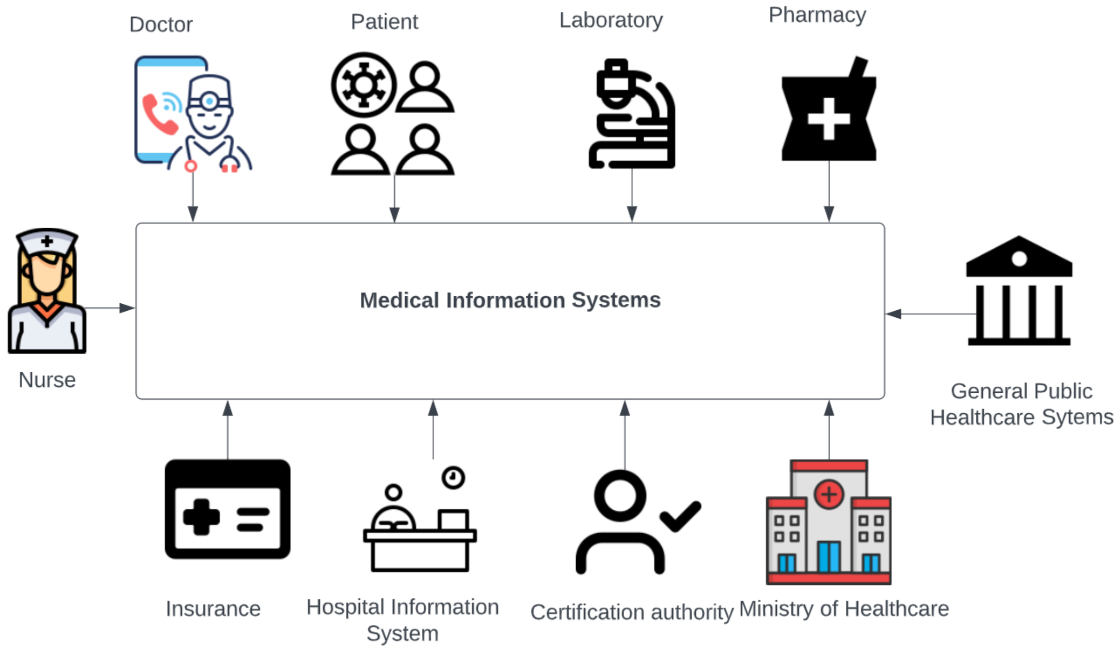

Figure 2. Overview of Medical Information Systems.

Below are some examples of Medical Information Systems:

EHR/EMR: Medical records can be called as either Electronic Health Records (EHR) or Electronic Medical Records (EMR), which include short histories or last updated records of the patient such as prescriptions, reports, or dieting advice from a doctor. A personal health record can be safely maintained in an EHR, and the healthcare system can be tracked at the patient's convenience [25]. The primary purpose of the EHR is to keep patients' medical records safe [36] and to manage them effectively. For accessing and handling a large amount of clinical data [40] and possibly managing to involve complex procedures like surgery and clinical trials in the proven method [41]. Healthcare data-sharing environments make it easier for a patient's healthcare data to reach the public for a more reflective result [42,43]. Data from longitudinal studies can be used to monitor a patient's health throughout their life. Security is a major challenge for EHR/EMR due to highly personal and sensitive data they contain. Health information about patients can be e.g., stolen, deleted, or tampered in the field of e-healthcare. The features of blockchain make it possible to verify the operation of different system components in a distributed manner [45].

Master Patient Index (MPI): MPIs are used to connect patient details across databases in the system. For a patient enrolled in a healthcare system, MPI can index all patient records. This system helps reduce duplicate patient records [66]. MPI helps connect separate hospitals and financial and administrative systems. To organize MPI, there are Data Quality Management tools, MPI Reporting tools, and MPI Access Manager tools [66].

Clinical Decision Support (CDS): Using CDS, patients can check the details of their medicine and clinical care. CDS assists patients and doctors in making decisions about appropriate healthcare depending on clinical circumstances [67]. CDS allows providers to access and evaluate data and provides accurate information about the patient as well as medication administration.

Healthcare Law: There are several aspects of healthcare in different countries. Most of the binding rules and responsibilities set by the government for healthcare organizations. Several laws can be harmful to a patient to a certain degree. HIPAA (Health Insurance Portability and Accountability Act on 1996) or PIPEDA (Personal Information Protection and Electronic Documents Act) is the general and specific privacy law for healthcare [64].

National Health Insurance Law: Hospitals now have different laws for each country and their patient care is different. Under the Insurance Law, a person's income is considered. Taxes cover the cost of healthcare in some countries, and hospitals offer high-quality care [65].

The PIPEDA approach selected the organization-to-organization approach to transferring healthcare data. Sometimes, it proves that data has been accessed without authorization [64].

HIPAA requires the transfer of healthcare data with the consent of the user. We cannot identify the location of the data transfer [64].

GDPR: The General Data Protection Regulation is a European Union law on data protection and privacy. It provides for the free flow of personal data among European countries as well as cross-border data exchange within Europe [61]. Additionally, it allows the secondary use of health information, meaning the data can also be exchanged electronically. Secondary use of healthcare data refers to electronic healthcare records, insurance claims, and health registry data.

2.2 Security Analysis of Medical Information Systems

2.2.1 Challenges

IoT Attacks: The major challenge in medical information systems is safeguarding IoT devices. Attacks on IoT devices can compromise patients' sensitive information. One of the biggest challenges is gaining access to other devices for malicious attacks. There are several forms of attack, and the most common attacks are Ransomware attacks and DDoS [62].

Ransomware Attacks: A ransomware attack involves hacking into sensitive data. A ransomware attack can cause the misuse of patient data in everyday operations which is critical for individual patient [65].

Distributed Denial of Service attack (DDoS): DDoS attacks are frequently used by attackers to hack sensitive data and shut down the internet. Furthermore, this attack can take down a healthcare site for an extended period of time [65].

RFID: A cybercriminal can easily attack the data and stop the exchange of medical data by intercepting the tags. It uses hardware design for encoding patient information [66].

Brute-force Password Attacks: Attackers can break the medical information system and track the password. They try different combinations to crack the medical system and the individual patient system [65,66].

Man-in-the-middle attack: Attackers can access patient confidential data and transmit it to another medical system. They can also modify or disrupt the medical data of each patient [65].

2.2.2 Security Requirements

Integrity: Medical Information Systems rely heavily on security to protect patient data from being stolen by attackers. This follows the instructions given by the patient. Integrity is improved by using the Merkle tree process [65]. An integrity system should also gather the necessary information.

Confidentiality: Confidentiality also plays a major role in keeping the record safe from others. A patient should be able to give access to anyone they choose. Relatives may view or modify their records [9] or be informed about them. Because a patient is very particular about their medical records. Without the patient’s key, no one can edit or modify the data. The patient never reveals their private key to anyone. Confidentiality is the main source of data security.

Authentication: Authentication plays a significant role in terms of medical information systems. Without user consent, no one can access the patient’s data. By writing smart contracts, it can control access. While writing the contract, the patient can mention who can access their data [14]. Authenticating healthcare data more securely and protecting it with biometrics is also very crucial.

Access Control: A particular patient controls his or her data, and third parties cannot access the record. Without access control, anyone can access the patient’s record. So, it is better to give access control by using some signature.

Interoperability: Concerns about interoperability include the possibility that an unauthorized person can access patient data with some authorized modifications. It is harmful to the patient's well-being. Safety and confidentiality are equally significant for patient information.

Legality: By following the rules, which are written by the patient, a legal agreement can be made while working on the smart contract. This will ensure that the system is as secure as possible.

Immutability: Due to this property, unauthorized individuals cannot change the system because the record is immutable. Immutability gives data consistency.

Trustability: In medical information systems, there is a problem of untrustworthy systems, but a smart contract can help with this problem by bringing trust by the patient's consent or permission granted through the keys, access to the patient's data is very difficult.

Transparency: In theory, medical information systems should be transparent in some areas, so anyone can view the data without it affecting the ability to make changes to the data.

2.2.3 Cryptographical Methods

Cryptography is a method of protecting data and communication based on mathematical formulae. A mathematical form like this requires some calculation in the form of an algorithm. It contains two different text pattern plaintext and ciphertext. Plain text is also known as ordinary text or human-readable. Cipher text is encrypted text. [68] This makes the system secure and resilient to attacks. Figure 3 explains the simple steps of cryptography. The sender sends plain text messages and then converts them into ciphertext messages by encrypting them with the key algorithm. The ciphertext messages are decrypted and received by the recipient without any issues.

Cryptographical algorithms:

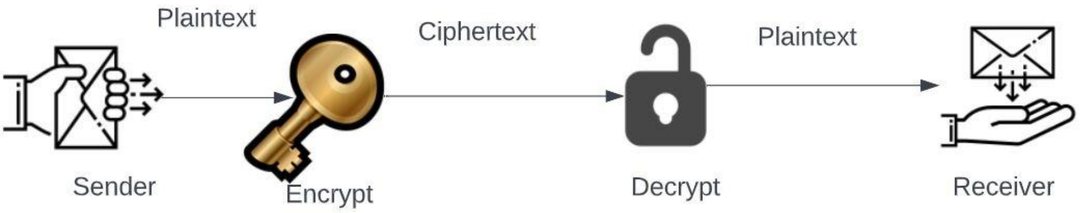

Figure 3. Simple steps for Cryptography.

The process of cryptographical algorithms embedded in protocols and written in software involves:

- Private and Public key generation for encryption/decryption
- Digital signing and verification
- Key exchange

Symmetric-key encryption algorithm:

This algorithm is also known as the Single-key algorithm. It is a single-step process for encryption and decryption. This creates a fixed length of bits known as a block cipher. The block cipher creates a secret key for the sender used for encryption. The same key for decryption can be seen clearly in Figure 4. The AES method is the leading example of this algorithm [70].

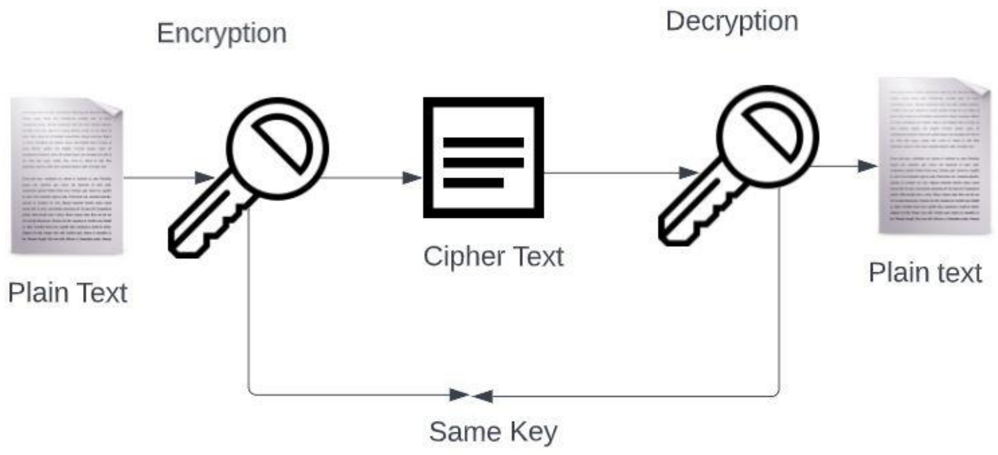

Figure 4. Symmetric-Key Encryption algorithm.

Advanced Encryption Standard (AES): Government computer security, cyber security, and data protection are most commonly used with AES. The symmetric block cipher encrypts data in blocks to produce cipher text.

Asymmetric-key encryption algorithm:

This algorithm uses a pair of public and private keys [70]. In Figure 5, one can clearly see the public key associated with the sender for the encryption process and the private key for use in decrypting the information. Both keys are solved by using the mathematical puzzles. Public keys can be shared publicly, but private keys cannot be shared with everyone. It should be kept secret and safe.

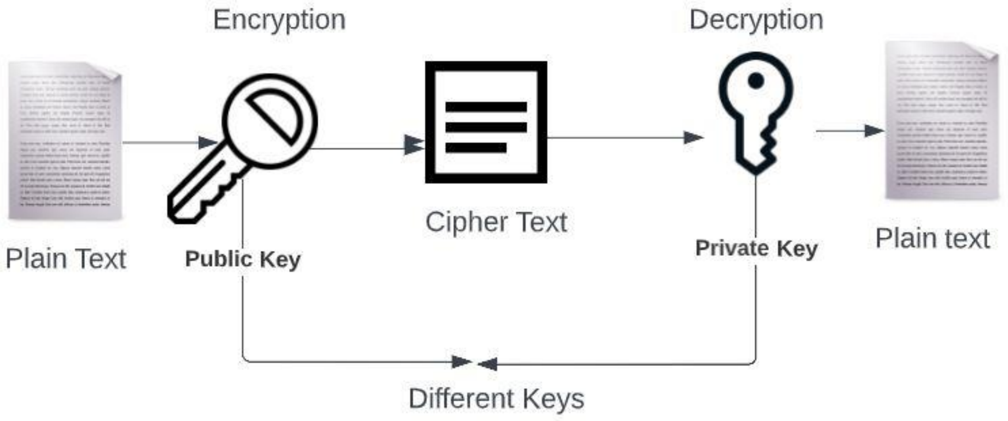

Figure 5. Asymmetric Encryption algorithm.

There are different types of Asymmetric Cryptographical methods:

RSA

Rivest-Shamir-Adleman (RSA) is an asymmetric cryptography algorithm. The asymmetric cryptographic algorithm plays a vital role with two types of keys [69], namely the Public Key and Private Key. Both keys are the core of the actual cryptographic algorithm. A public key may be given to anyone, but a private key may only be used by the owner. RSA is difficult to factorize a large number. Both secret and public keys can be derived by multiplying together the first two prime numbers. RSA keys can range in size from 1024 to 2048 bits long. To avoid giving private keys to someone, we use two different keys for the algorithm in a secure way.

ECDSA

The elliptic Curve Digital Signature Algorithm (ECDSA) provides shorter keys to provide strong security fields while maintaining computational requirements. ECDSA uses an elliptic curve a finite group of points on a curve where some operations are easy to perform in one direction but difficult in the other direction. Blockchains rely on the ECDSA method for solving problems. The computational method, even though it uses shorter keys, is more efficient than RSA [71].

2.3 DLT and Blockchain

2.3.1 DLT

Distributed Ledger Technology is a distributed database that is decentralized means the computers or nodes are connected in a distributed way like peer-to-peer networks as shown in the Figure 6. In DLT, every node will maintain their own ledger. The nodes have equal level of security measures or protocol. Nodes verify the transaction using consensus mechanism.

2.3.2 Blockchain : An Example of DLT

Blockchain is one type of decentralized ledger technology in which every node maintains its own records independently. Additionally, nodes in a blockchain verify transactions using consensus algorithms. Blockchains are distributed ledgers where every node maintains its own ledger. In blockchain transactions, the nodes will also verify the transaction by using a consensus algorithm. Transactions on a blockchain are recorded on a distributed ledger, which is an immutable digital block. Senders and receivers are informed if there is any hacking on the network. This is because P2P connects with different networks which store the data privately and make sure the data is secured [15].

After blockchain technology was first introduced to the finance sector, it was extended to other different sectors. This is because it revolutionized the future of based exchange in various sectors such as insurance, telecommunications, aircraft, and healthcare [50]. There are many other applications across different sectors that have been developed and implemented. Blockchain adoption can be divided into three phases: Blockchain 1.0 is the introduction of blockchain as a cryptocurrency, bitcoin. Blockchain 2.0 is about smart contracts, tracking records, and tracking the ownership of properties inside the Blockchain system. Among the features of blockchain 3.0 are science and education, and education will come in the future [50].

The main purpose of blockchain is to protect data using all security measures available. It is a decentralized distributed ledger connected to a network of nodes [1]. Blockchain came from the concept of bitcoin. All nodes have both a public and a private key and are connected to a peer-to-peer network. For external storage, nodes can access the data but cannot modify it easily without the user's permission. In Figure 6, the WorkCycle of Blockchain and how a network is created are explained by the nodes who are considered miners. This is because they have permission to create a new block [6].

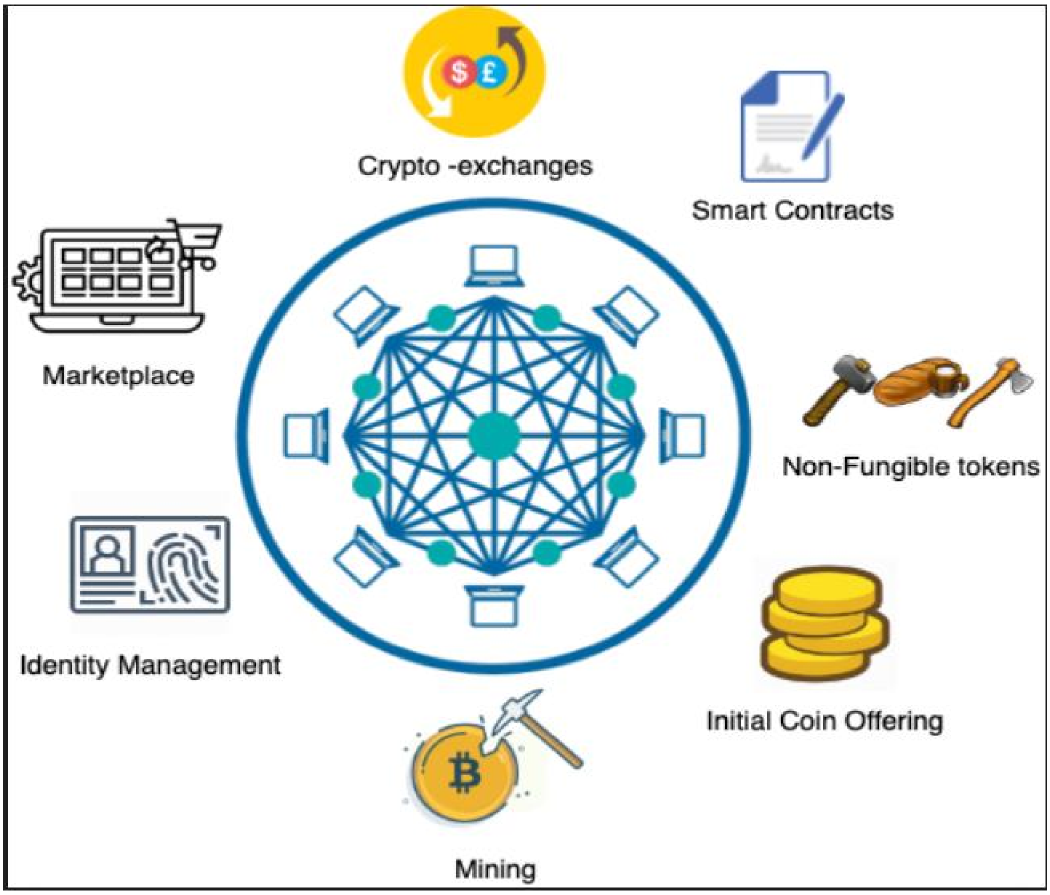

Figure 6. WorkCycle of Blockchain.

Essentially, the role of blockchain is to eliminate intermediaries and use chain-based transactions. The blocks are connected to each other. Once the transaction has been approved or agreed between the users, it will be entered into the system for authentication using the cryptographic keys that the user provides. Each user has their own private key and a public key. The block confirms the transaction has been created, and the block sends the data to every node in the network. Nodes will validate the transaction using the Proof of Work (PoW) method. PoW is a mathematical puzzle that protects the network from attackers. Nodes receive a reward for PoW which is cryptocurrency. During this process, the block is added to the Blockchain, and the information is updated across the network in a similar fashion to P2P. The transaction is complete as shown in Figure 7. When the first user enters the blockchain system and requests the first transaction. Initially, the transaction is verified by the chain and sent to the different nodes that hold the block, so the transaction is sent to one of them. The nodes validate the transaction using the block and the information distributed throughout the blockchain. This authenticated transaction is added to the blockchain, and the blockchain transaction is completed in a secure manner.

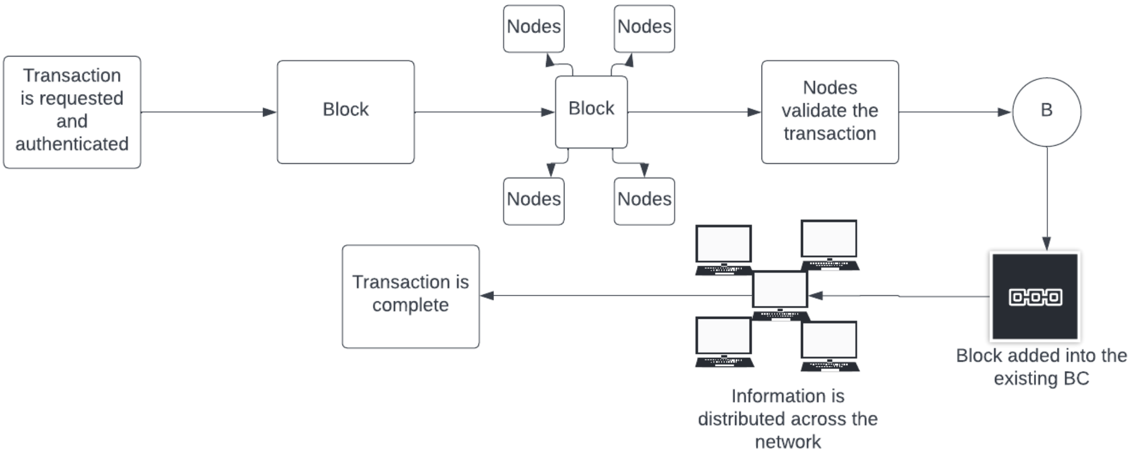
Transaction is requested and authenticated
Block
Nodes
Nodes
Block
Nodes
Nodes
Nodes validate the transaction
B
Block added into the existing BC
Information is distributed across the network
Transaction is complete

Figure 7. WorkFlow of Blockchain.

2.3.3 Example of Applications: CryptoCurrency

Blockchain has several types of applications, but cryptocurrency has so far been one of the most significant. According to a report from the Cambridge Centre for Alternative Finance, only about 300 million people were use or own cryptocurrencies in 2021 [20]. Many well-known companies accept cryptocurrencies as payment but require a third-party firm to access the blockchain [20] and instantly convert payments into fiat currency. One of the biggest concerns for companies using cryptocurrency is the volatility of the market. Between 2012 and 2021, Bitcoin prices increased by over 540%, use of the currency. Despite the high security of Blockchain, cryptocurrencies exist primarily in the digital world, making them vulnerable to cyber-attacks. The most popular digital currency is Bitcoin.

As a digital currency, Bitcoin implements blockchain technology for further development (7). Bitcoin has the original features of a P2P distributed server along with a timestamp. It generates computational proofs in chronological order during transactions for security reasons [34]. Each transaction represents the previous hash pointer. It accepts both private and public keys. Bitcoin is a decentralized digital currency with no intermediaries involved in transactions. The Public Key Infrastructure (PKI) of Bitcoin is based on a pair of public and private keys. [7] discusses how IoT and distributed ledger technology can provide opportunities to develop distributed applications (Dapps) for the sharing economy.

2.3.4 Key Components of Blockchain

Blockchain Platform: For developing the blockchain and running programs and simulations, the blockchain platform is the main tool. Ethereum is one of the blockchain platforms that allows smart contracts to be built on the blockchain. Using the Blockchain network, which has smart contract logic and is widely used for understanding and usability, is a smart way to use it.

Smart Contract: By using a programming language or code called Solidity, smart contracts are able to write the terms between two parties, that are automatically verified by system or applications.

Mining: The mining process adds verified transactions to the blockchain after the request has been added to the blockchain. It also ensures that transactions are valid for further steps.

Consensus Mechanism: The consensus mechanism distributes terms or agreements across all blockchain networks, where the entities are agreed with each other.

2.3.4.1 An Example Blockchain Platform: Ethereum

Ethereum is the first platform with a smart contract along with the Ethereum Virtual Machine [13]. EVM is the runtime environment for smart contracts and every Ethereum node is based on it. Ethereum Platform is expanding support for blockchain in terms of using smart contracts. Ethereum has a chain code and two accounts. One is externally owned, which can be accessed with a private key, and another is a contract account, which can be accessed via a smart contract. The header of the Ethereum blockchain consists of the keccak-256 algorithm. Currently, the platform uses a PoW Proof of Work consensus algorithm called Ethash, but developers are working towards PoS Proof of Stake. Ethereum is introduced to overcome the scripting language limitation and work with the blockchain network. The Ethereum Blockchain has its own language, such as Solidity, which has been used for many applications use in distributed way. As a result, developers can code, develop custom apps and run them on the Blockchain with some agreement written with the consent of the users [8]. Figure 8 explains the workflow of Smart contracts and Ethereum. The terms and agreement between users and stakeholders should be outlined in a signed contract, then converted into Solidity codes. Then, the execution in the Ethereum platform takes place in the Blockchain using EVM.

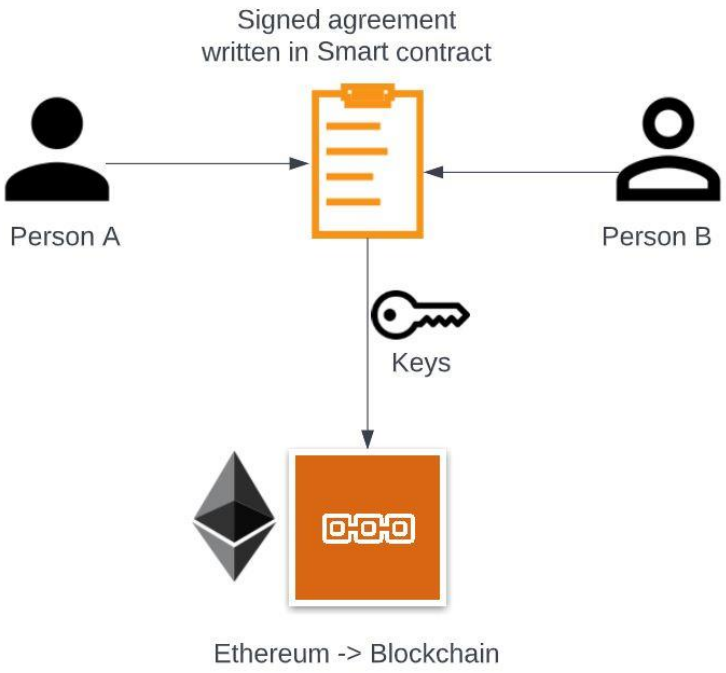

Figure 8: WorkFlow of Ethereum and Smart Contract

Nonce:

The nonce is used to represent the number of transactions that are added to a hash or encrypted way to authenticate the transaction. Furthermore, it verifies and makes the network more difficult to attack, as well as verifying the network.

Ethereum Virtual Machine:

Ethereum Virtual Machine (EVM) is a decentralized machine that can run smart contracts. Gas is a fuel to energize the Blockchain and measured in terms of units and costs. This ensures that the system is running safely against Denial-of-Service attacks. As a gas fee, small amounts of Ether are charged for building the digital currency of the Ethereum network. Ether is the fuel used by the Ethereum platform. Each transaction consists of the recipient's message, the signature of the user, and the amount of ether to be sent. Along with that, another optional field is StartGas and GasPrice [13].

Testrpc:

Testrpc is used by Ethereum JS to make the development process faster. Testrpc is an Ethereum client for testing and developing applications.

2.3.4.2 Smart Contract

A smart contract is a computer protocol introduce to digitally facilitate, verify, or enforce the negotiation or performance of a contract in the blockchain. Blockchain-based smart contracts could offer several benefits, such as fast, dynamic, and real-time updates, low cost of operation, high accuracy, and fewer intermediaries [5].

Smart contracts consist of codes or agreements between users. It also specifies the rules that networks should follow to prevent data from being accessed by unauthorized persons. Smart contracts have two attributes: state and value [26]. Ethereum is one of the most common platforms to implement smart contracts because it offers the Turing complete programming language. Remix and Kovan test networks have been used to deploy smart contracts and testnet ethers for paying transaction fees. Smart contracts can be implemented using Solidity [12] and do so in three stages, such as writing, compiling, and announcing.

Design patterns for Ethereum Smart Contracts

- Tokens can represent coins, tickets, or anything that can be transferred. In addition, it represents user authorization and identities.
- Authorization ensures that contracts are protected by checking the caller's address. It will check the caller's address by verifying the contract address. Users can refuse authorization.
- Randomness helps to check whether all the nodes obtain the same values for user addresses who are already registered in the system.
- Time Constraint is critical for implementing contracts for specifying the action to be performed.
- Termination: On the blockchain, a contract cannot be deleted directly after it is created, because it is immutable. We must think about the account being disabled. The account being disabled can be self-destructed or terminated by suicide.
- Re-entrancy attacks can hinder external functions. Mutex helps to protect the contract by calling the function separately to avoid attacks.
- Solidity is a high-level programming language that can write a smart contract that specifies a special variable (block, text, message) that specifies transactions with blockchains. Security can be defined by the reusability of the function, and Solidity can also inspect the smart Inspect function [10]. Solidity was designed in C++, JavaScript, and Python. Many attacks are possible against Solidity, such as attacks on internal or external calls. Additionally, some attacks are possible, such as replies to attacks. It can however overcome by using some keywords like mutex and planning the solidity using the patient's concern

2.3.4.3 Mining

Mining is a process to secure and verify transactions on the Blockchain. Mining solves the mathematical equations even in the high computational power to verify transactions and add them to a blockchain ledger. Figure 9 explains the workflow of mining. After a transaction is initiated, the transaction details are provided to miners so that they are aware of pending or upcoming transactions for verification on the blockchain. Then, the miners check whether it is a valid transaction or not. Once it is valid, verification is a success. Mining is completed and miners are rewarded for adding transactions to the blockchain. As transactions are added to the blockchain, further actions are taken to complete them [39].

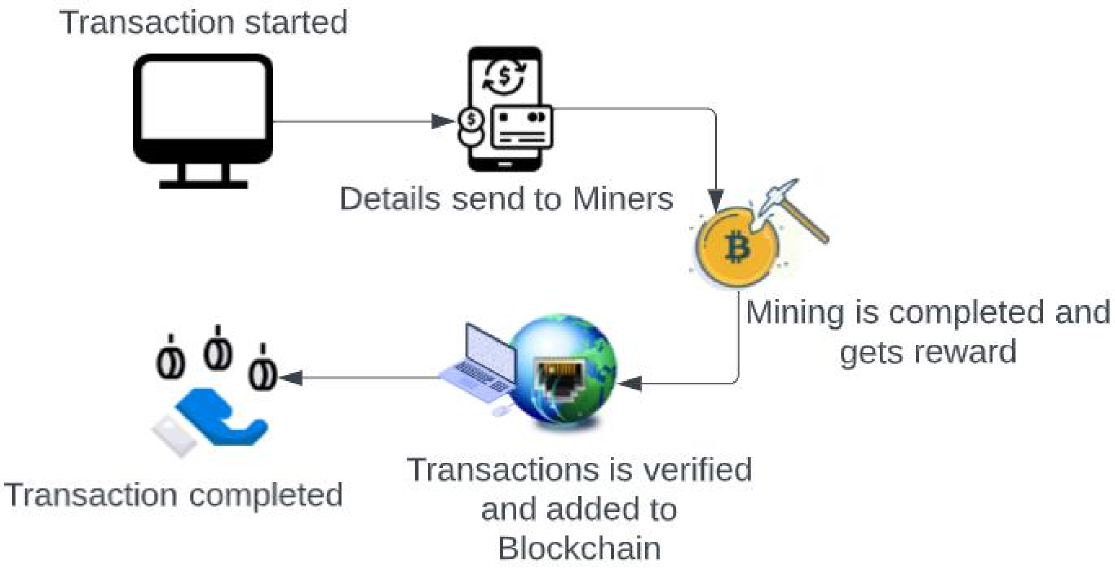
Transaction started
Details send to Miners
Mining is completed and gets reward
Transactions is verified and added to Blockchain
Transaction completed

Figure 9. WorkFlow of Mining.

2.3.4.4 Consensus Mechanism

Most blockchain mechanisms have function similarly, but the way they reach consensus on transactions can be unique to each. Consensus Algorithms follow mathematical protocols [15] that make sure all the nodes are synchronized and agree on which transactions are legitimate and can be added to the Blockchain. Without a reliable consensus mechanism, the blockchain is at risk of various attacks under different circumstances.

1. Proof of Work: PoW is the first consensus mechanism and was used in the blockchain network. The blockchain network is secured by solving a complex computational puzzle with a mathematical puzzle. The first node to solve the puzzle gets to create the block and receives a reward incentive. The major disadvantage of PoW is that it consumes a lot of time to find the answer to the mathematical puzzle. This can consume a lot of computational resources, but it is always helpful to verify the answer for increasing chain security [15].

2. Proof of Stake: PoS is an understandable and easy consensus mechanism that randomizes the selection of the user to produce the next block. It requires people to prove their ownership of the amount of currency because it is believed that people with more currencies would be less likely to attack the network. The PoS mechanism takes a couple of factors into account, depending on the blockchain. The user with the highest data has the highest chance of producing the next block. Energy-efficient and faster than PoW, it can be selected depending on the blockchain's usage and network demands.

3. Other Consensus mechanisms: Apart from the above most popular consensus mechanisms, concepts for other mechanisms exist but no implementation has been

proven. Proof of Capacity (PoC) uses a technique called pre-storing the solution that is necessary for the block creation process, as well as assuming the solution. Proof of Elapsed Time (PoET) is another consensus mechanism that aims to decide randomly and fairly who gets to produce a block based on the time that they have waited. A random process assigns a wait time to each node, and the first node to complete the wait time generates the first block. This mechanism only works if there is a system to verify the randomization process and make sure nobody runs multiple nodes [15].

2.3.5 Types of Blockchain

SideChains:

Sidechains allow digital assets and tokens from the sidechains to be securely used and then be moved back, if needed, to the original chain of the ledger. The sidechain runs independently of its main chain and takes care of its security and validation protocols. If the sidechain is compromised or fails, the main chain continues to operate and vice versa. Each decentralized application or game will run on a chain connected to the blockchain. The sidechain can use alternative consensus mechanisms, like Proof of Stake, that are optimized for high scalability. On the main chain, a more power-intensive consensus algorithm, like PoW, can be used for a higher level of security guarantee. Sidechains also divide the assets on the ledger and at the network-level multiple unsynchronized chains interact with each other which further complicates things. Another downside of the sidechain is the requirement for federation and this extra layer could prove to be a weak link for attackers and hackers. If the implementation works properly, side chains can solve scalability and interoperability problems, without compromising the integrity and security of the blockchain [7].

Off-Chain Transaction:

An off-chain transaction is a moment when value is transferred outside of the blockchain. The off-chain state channel is a two-way communication channel between users that enables them to interact with the blockchain. This channel allows the processing of a significantly higher number of transactions without a miner validating each transaction, and additionally, less data is recorded on the main chain. To work, a segment of the blockchain is locked using multi-signatures or smart contracts, agreed upon beforehand by users. Each transaction is signed by both users and the entire transaction set is then included in the main chain of the ledger. Off-chain solves several problems. It is designed to make transactions faster on the blockchain by adding a layer on top, without compromising its security. It also focuses on reducing the validation time and size of blocks to further scale the blockchain. Off-chain transactions will also help to reduce transaction fees as less validation will be required on the blockchain [15].

Permissioned Blockchain:

Permissioned blockchain networks permit access to a group of candidates into the network and verify the nodes to validate transactions. It has mathematical computation for validating the public blockchain and it has a clear authorized structure that helps to modify the chain faster. The participants can have control to operate the individual full node as in the structure and rules of the network and the amount of computation used for validating the public blockchain gives a great performance. when they get multiple individual nodes for consensus to activate the update on the network becomes slow to update the network [72].

Consortium Blockchain:

The consortium blockchain combines multiple private blockchains from different organizations. Collaboration between private blockchains in consortium blockchains leads to many benefits for minimizing time and costs. Improving time and costs leads to faster transaction speeds and higher scalability. The Consortium Blockchain is open to private blockchains but closed to public blockchains. The consortium then maintains a secure chain of the network [72].

Permissionless Blockchain:

Blockchain networks with permissionless access work in opposition to permissioned blockchains. In a permissionless blockchain, the public blockchain is available without restriction or control from any system. A decentralized public blockchain platform that works with everyone or unknown parties. It ensures high levels of transparency and accepts a large number of participants [72].

Table 1. Comparison of Various Blockchain Components:

Technology	Consensus	Performance	Smart Contract	Side Chains
BitCoin	PoW	5-6Tps	No	
Sigwit2xBitCoin	PoW	10-12Tps	No	Yes
RootStock BitCoin	PoW	-	Yes	Yes
Ethereum	PoW(Planning POS)	15Tps	Yes	No
Loom Network	Delegated POS	Upon 1000Tps	Yes	Yes
EOS.io	Delegated POS	3996Tps	Yes	Yes
Hyperledger Fabric	PBFT	Upon 1500Tps	Yes	No
R3 Corda	RAFT	600Tps	Yes	No

2.3.6 Blockchain for HealthCare

Blockchain technology has the potential to secure and maintain the healthcare system safely and increase the level of security, privacy, and interoperability of health data. Healthcare systems still need Blockchain to keep track of medical records [2]. However, the business potential in this area is limited by high transaction fees and minimum transaction sizes. Blockchain holds the potential to integrate healthcare systems with real-world systems, paving the way for future uses. Blockchain knowledge by comparing healthcare systems with and without the use of Blockchain development according to the applications. Healthcare systems that integrate with blockchains are more efficient than those without [17]. In addition, it accepts biometric signatures, which makes it more secure than manual reports. To ease the digital access of data, data immutability, handling large amounts of healthcare data, and patient identification throughout the world can explain and discussed further to enable the patient-centric control of healthcare data sharing on blockchain technology [46]. There are numerous benefits of blockchain technology in the healthcare sector [47]. Patients with different backgrounds, or from different age groups, or different geographical locations, can access the blockchain data system. This would allow a wide range of data to be uploaded [48, 49]. Improving technology helps common people understand and use it properly.

Key aspects of Blockchain in healthcare:

Security:

Blockchain is primarily considered to provide security and immutability by decentralizing and encrypting data. Signing schemes are used to encrypt data, ensure access control, and provide digital signatures. By using the Ethereum blockchain to store medical data, smart contracts allow patients to securely control their own data [51].

Privacy:

Privacy is one of the major concerns in healthcare. Blockchain tackles the issue by using encryption techniques between patients and their medical data which should be confidential. Privacy techniques can be implemented [52] which require users to sign messages. Cryptographic technologies such as encryption and proxy re-encryption can be implemented within the Ethereum platform to optimize privacy.

Access Control:

Access control is an control mechanism of healthcare data and is closely related to data ownership. Medical records are encrypted using the owner's public key, but the re-encryption key and other information required to authorize the process are stored on a trusted proxy called a gateway server [53]. Access is only granted once to data owners, and access management is on the blockchain and can be traced and reported transparently.

Data Immutability:

The immutability of data allows for modified the healthcare data. The immutability of the transaction and the modification of healthcare data. It combines cryptographical operations with the blockchain hashing process to ensure immutability.

Data Integrity:

Data integrity is generally in use for both centralized and decentralized data storage. The data can be encrypted using the public key cryptography employed by blockchain in order to resolve this issue. The system only allows authorized users to access records for a particular activity or session. Patients have complete control of granting and revoking access to their medical records to preserve the confidential nature of health data [55, 56].

Confidentiality:

Confidentiality is another issue related to privacy. Using blockchains and encryption of signatures, data is protected from malicious agents. The encryption method ensures the size of the ciphertext is constant. Using this technology, healthcare systems can implement a flexible and confidential access control system [54], which they require more frequently.

Authentication:

Healthcare domain requires authentication for protecting the data. Blockchain technology is combined with data aggregation and group authentication. Members of a group can view encrypted information with a key if they have the patient's consent and a joint agreement [57]. This allows participants to compare stored datasets, and they can access the database set by providing the digital certificate of Blockchain.

Data Ownership:

Data ownership is the issue of expressing the fear of third parties accessing their confidential healthcare data. The solution to this issue is blockchain technology with employed encryption schemes [58]. The integration of smart contacts and Ethereum ensures patients maintain ownership of their data.

Availability:

Healthcare, which is less accessible and less secure, faces a critical lack of accessibility. Keychains use smart contracts, cryptographic methods, and distributed technology to solve the challenges and to be more secure and accessible [61].

Data Validity:

Data validity is the applicable for verifying the validation. When the data collection queue increases at the same time, certain errors can occur. Several schemes in the blockchain can verify the private key of the user when validating the signature on each transaction. The public key can then check the generated signature using the validated private key.

Transparency:

Blockchain networks maintain a history of patient transactions within a network, making it easy to track their data in a transparent manner. Transparency makes data traceable, permanently stored, and publicly accessible across a network.

Auditability:

Blockchain networks provide auditability as a major benefit. It provides a digital timestamping service, increased process reliability, and effective cryptographic primitives. Healthcare systems use all the auditability benefits to prevent the improper use of patient data.

3 PROPOSED SYSTEM

3.1 Healthcare Scenario

Healthcare scenario in the proposed system carries two entities like patient and the doctor. To achieve this objective, I used blockchain technology in the scenario to ensure the integrity and interoperability of medical systems. In healthcare systems, cryptographic methods play an imperative role in security. Both the patient and the doctor can access data using the address and key. The patient and doctor are both authorized to see the patient's record, with the patient's consent. In the proposed system, both the patient and the doctor have access to patient records. Medical data also includes laboratory reports, insurance, prescription, and billing information. Specifically, this thesis proposes a cryptographic mechanism for adding to or updating a patient's medical records and ensuring the security of the blockchain. For more explanation, Figure:10 explains the entities and workflow of each entities along with the operations.

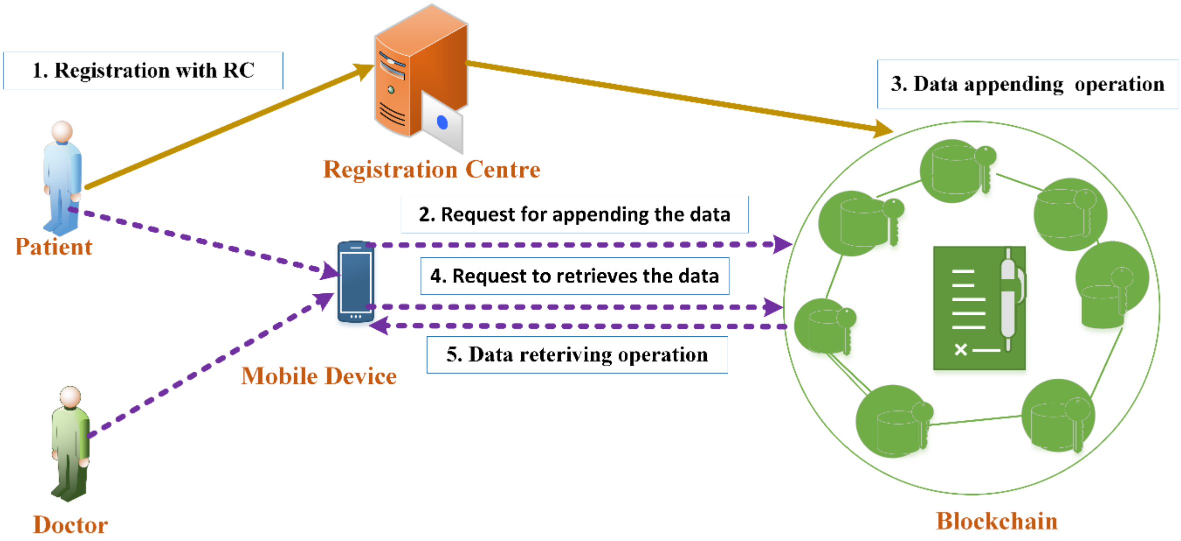
1. Registration with RC
Registration Centre
3. Data appending operation
Patient
2. Request for appending the data
4. Request to retrieves the data
5. Data reteriving operation
Mobile Device
Doctor
Blockchain

Figure 10. System Model of the Proposed System.

There are different entities in the proposed healthcare scenario,

1. Registration Centre,
2. Patient
3. Doctor
4. Mobile Device
5. Blockchain

All these above five entities have a great role in our proposed healthcare system and the proposed entities operations are explained well.

- A patient should be able to install the required applications on their mobile device. They should also know the details of the doctor they are going to visit, as well as the hospital details.

- Prior to the appointment, the doctor should be familiar with the patient's details and report. Also, doctors should be able to handle mobile devices.

- The patients should identify another trusted person who can handle their report in any case of emergency.

- The patient and doctor need to be aware of the passcode details either through biometric authentication or password protection. They can decide and provide details in the app.

3.1.1 The Functionality of different entities

1. Patients should first register through the Registration Center by providing their IDs and biometric signatures. Registration is only for first-time apps. The patient does not need to see the Blockchain (BC) because the keys will be given to the patient after registration is completed. A patient can then download the app onto their mobile device and follow the instructions.

2. The app should be installed on the patient's mobile device using their biometrics. Then, the registration Centre generates ID for the patient after the registration and a secret key pair (private/public key pair) using the installed app on the mobile device to authenticate the keys on the patient and doctor.

3. To ensure access rights, the patient should provide the access rights to the doctor. Then, both patient's and doctor's public keys are automatically added to the Blockchain by the system. In the process of registering the patients can provide the doctor's information as well as the information of another person who may be their relative or friend. In that case, the doctors will get the public key along with the patient's details. In blockchain, the patient details are stored along with all their necessary information.

4. It is possible for a patient to visit a doctor for a regular check-up or for the first time. Further, doctors can update patient records with the help of patients' consent using their biometrics. Both the doctor and the patient should authenticate at the same time. Afterward, authentication is verified through the Schnorr Scheme. If both the public keys are the same, then the further action proceeds, or else, it will exit the request.

5. After receiving the correct request, the Blockchain will provide the patient data to the doctor. The doctor can update the patient's information. Patients can see the updates given by the doctor about their medical report, but the patient cannot append the data or update the report.

6. Data can be shared or retrieved, and details can be reviewed by the patient. Both appending and retrieving data can be done by a doctor. The patient can also show the report to a pharmacy to buy medicines. This is also true for lab technicians if they need to take any kind of lab test prescribed by the doctor. Figure 10 illustrates the process of getting from the different entities to BC.

3.2 System Model

The Healthcare scenario with Blockchain gives a feasible solution for both patients and doctors. To overcome the challenges of the traditional healthcare scenario and protect sensitive data, the system model has phases with cryptographic schemes [1].

To implement cryptography for the proposed healthcare system, ECC (Elliptic Curve Cryptography) offers a more comprehensible and lightweight approach. This will be easier and more feasible to implement than algorithm like RSA, classical discrete algorithm and so on. Considering the cryptographical scheme from ECHLP and ECDHP in our proposed system with encryption and decryption of the one-way hash function. The cryptographical method in the EC (Elliptic Curve) purpose the contants a and b as $y2 = x3 + ax + b$ and $D=4a3 + 27\ b2 \neq 0$, also, relying on the multiplication for ECC as $R=rP$ and addition as $R1+R2$. Following the values, the ECDLP and ECDHP $Q=xR$ and $R=xP$, $Q=yP$. Followed by encryption as $C=E_k(M)$ and decryption as $M=D_k(C)$

For clarity and understandability, cryptographical operations are used in the proposed scheme.

In Figure 10 represents the five phases in the scheme:

1. Data Registration Phase
2. Request for Data Append
3. Data Append Phase
4. Request for Data Retrieve
5. Data Retrieve Phase

Each Phase carries different roles [1] for the healthcare scenario as specified below.

3.2.1 Data Registration Phase

The data registration phase explains the registration format for both the patient and the doctor. As a precaution, patients and doctors should bring their mobile phones with them to hospitals. The purpose of this is to allow them to use the mobile app to register within the blockchain network.

A new patient must first register in the registration phase to become part of the Blockchain network. Doctor's information can be provide by the patient. In addition, the doctor will be part of the network. As it is a one-time registration, the patient and the doctor will each need to provide their details using a mobile device that they can easily access by giving their own identity id_p, their public key pk_p, and the pk_d public key of the doctor(s) id_d treating the patient. Patients can also add trusted relatives or friends along with both identities. In this scenario, the patients are treated one at a time to avoid unnecessary changes.

Then, the registration phase sends (id_p, pk_p, pk_d) to the BC signed by the patient and doctor. All the necessary information (id_p, pk_d) was already sent to BC during registration. Additionally, the Blockchain keeps verifies the signatures of the patient and doctor from RC. BC keeps copies of the signatures on it. Public keys should be used whenever the patient/doctor needs to access the data for further operations

3.2.2 Request for Data Append

The data append phase represents the append operation for the patient's data request to BC. The doctor can be able to append or update the data from BC with the approval of the patient. So, the doctor submits a request to BC along with patient approval. In that case, the doctor and patient must possess the MD on which the health app runs. Therefore, the doctor first gives the signature in the form of a public key which is already in the registration form. BC checks the signature given by patient and doctor and proceed with the following steps:

First, BC validity the signature with T denotes the current timestamp. App in the doctor's mobile device determines $r = H(sk_d ,T),$ *and* computes $R=rP$. Further, mobile device from the doctor's app derives the key $k = r\ pk_p$ and the corresponding ciphertext $C_1 = Ek(m, T)$. This value $C1$ together with T, R *i*s transmitted to the patient.

An app from the patient's mobile device can also compute $k = sk_p$R, decrypt from the above steps $C1$. The decrypted message can send to the doctor and the messages can be proceeded to append the patient's data.

Based on the BC check, BC generates a signature by calculating $C_2= sk_P H(pk_p|pk_d|C_1|R|T) \oplus kH(id_p|R|C_1\ |T)$. For signature verification, BC computes $K = kP$. After receiving tuple information from the BC to patient $C_{SR}\ = (id_p, pk_d ,T, R, K ,C_1, C_2)$ patient sends this to the doctor, which results in the doctor appending the patient data and making changes.

3.2.3 Data Retrieve Phase

Upon sending the request to BC by the patient or the doctor, the BC will check the timestamp values T and after the timestamp, those public keys of the patient and the doctor, which should both be registered during the registration phase.

Further, signature should be verified by the BC and checks the $C_2P= pk_P H(pk_p|pk_d|C_1|R|T) +KH(id_p|R|C_1\ |T)$.The BC check also verifies that the data comes ID of the patient id_p and pk_d public key of the doctor should be there for the next steps with BC. Upon validating the public keys with the verification process, BC will move on to appending data.

Finally, BC stores the C_{SR} . After many steps of verifying the request given by the corresponding doctor or patient, BC will send the data to the doctor id_d

3.2.4 Request for Data Retrieve

In order to ensure that both the patient and the doctor have shared the timestamp, the doctor and patient must send a separate request to the BC for data retrieval while using their public key to the BC (id_p,id_d,T_p), in the same time interval to ensure that both parties use the timestamp T_p, and before sending the request to the BC, the patient must approve the doctor prior to logging into the system to ensure both parties are trustworthy.

3.2.5 Data Retrieve Phase

When the doctor or patient wants to send the retrieve request, BC will process it further

Step 1: The patient should approve the doctor's request before sending the request to the BC. Then both doctor and patient send the request for retrieval of data along with the timestamp for further verification in the BC.

Step 2: After sending the information of both parties, BC confirms the signatures of doctor and patient along with the timestamp, and then the patient's record is received over a certain period. The retrieved data has the form $C_{SR'} = (pk_p, T, R, C_1, C_2)$. Since the stored tuple is removed and informed to the doctor as it is known by doctor so id_p is changed to pk_p and pk_d. Once BC verifies the validity of C_1, the information is enough for the doctor to calculate $k = H(sk_d, T)\, p$ and values for the decryption C_1.

4 PERFORMANCE EVALUATION AND SECURITY ANALYSIS

4.1 Simulation Environment: Ethereum

The motive of this section is to provide simulation details of the proposed system with Ethereum. The Ethereum Blockchain plays a major role in the proposed healthcare scenario by executing the actual working system and by writing the code into the smart contract. An explanation of the process of executing the Blockchain is also provided in the previous section. The Ethereum platform is primarily based on Blockchain and smart contracts. Ethereum carries miners and transaction fees.

4.1.1 Miners

Ethereum uses mining techniques for validating incoming transactions. Each mined block contains the last transactions and is marked for every 13 seconds, adding the transactions to the new block. Mining verifies the first block and stores it in the Blockchain network. This technique follows the Proof of Work concept and creates a new network block. The major benefit of Ethereum is that every block contains the patient's identity. When the Blockchain receives an incoming request, the miners create a new block and provide information to another block about the newcomers.

4.1.2 Transaction Fee

Every blockchain transaction should be added to the ledger to be considered completed or valid. These transactions are prioritized by the completed validation of ledger. The transaction of gas is validated by miners using the higher gas fee. Depending on the gas used for each transaction, the main transaction fee for the network can be calculated. The transaction fee on a blockchain cannot be achieved by having a large amount of microtransactions. When a fee is charged for every transaction, it limits the types of transactions that a decentralized network can process. Healthcare blockchain will require transactions for which gas fees are required to solve the algorithm, and this can be seen in Algorithm 2.

Table 2. Gas Usage of the proposed system.

Operation	**Gas Used**	**Price in Dollars**
Algorithm deployment	973,772	63.29
New data	502,326	32.65
Retrieve data	0	Free
Append data	312,305	20.29

Average Gas Price: 20 GWEI and the one ETHER COSTS 2692 dollars

Gas price is calculated by using automatically setting the transaction fee (base fee + recommended priority fee.

4.2 Implementation

I have proposed healthcare systems incorporate a smart contract that plays a major role in executing the entities in the healthcare system. The developed smart contract codes involved with the agreement signed by entities, such as a patient or doctor, which is then forwarded to miners for further verification. With the keys provided by the blockchain is the signature for both patient and the doctor. The data should be shared with the entire patient database within the patient's network, which holds all the patient's and doctor's details. Smart contracts can include the consent of the corresponding people, but they cannot be invisible to patients outside BC. Furthermore, the blockchain-based system that we propose enables trustable, transparent, and traceable transactions. Smart Contract uses the language called solidity for developing the Ethereum Blockchain.

Append/Add the patient record and retrieve the healthcare document. These are the two main operations we perform for our healthcare entities. By using the proper signature along with patient consent, both patient and doctor can participate in our case. For appending the healthcare data, modifying/updating the healthcare data can access only the corresponding doctor with the patient’s permission. To retrieve or append the owner’s data, a patient should approve and authorize their concerned, as stipulated in the registration contract. As well, the patient is only able to edit the doctor's information and they can only add another person to see the patient's record. Above the steps have been completed, the records can send to the doctor or patient with the given signature can be clearly shown in the Algorithm 1.

The steps from the Algorithm 1 involved in implementing our proposed system. In this phase, data about the patient or doctor is registered, data is retrieved, data is appended, and data is updated. Information can be retrieved by either the doctor or the patient. As patients cannot edit their records during both operations, data must be added by the doctor. The timestamp also plays a vital role in completing the BC.

Algorithm 2 has the steps carried out inside the Smart contract about the PlaceBid, Cancel Bid, or withdraw.

Algorithm 1. Algorithm for our Proposed System.

```
mapping (bytes 32 => device) Patient List
mapping(address=> uint 256) balances
Init: uint256 total_Medical_Report
Constructor(InitialSupply):
balanceOf[Owner] = InitialSupply

Event Transfer(Sender, Receiver, amount);

struct {
  string patient
  string doctor
  address patient
  address doctor
  uint256 price
  } mobile devices

Function EHRPatient ID,Doctor ID,Mobile device, Requester,price;
   newKey=stringToBytes32(ID)
   total_Medical_Report+=1
   PatientlList[newKey].name=Patient_ID
   PatientList[newKey].PatientID=Mobile_device
   PatientList[newKey].name=Doctor_ID
   PatientList[newKey].creator=Requester
   PatientList[newKey]. price = price

FunctiongetPrice
    Key=stringToBytes32(Patient_ID)
    Key=stringToBytes32(Doctor_ID)
    return Patient List [Key].price;

Function retrieve data (name, time)
     ⇨ Function getPrice
     Receiver 1= Patient List [Key].Patient_ID;
     Receiver 2= Patient List[Key]. Doctor_ID;
     Price= Patient List[Key].price x time;
     return true;
     return total_Medical_Report;

Function Append Data
     ⇨  Function getPrice
     Receiver 1= Patient List [Key].Patient_ID;
     Receiver 2= Patient List[Key]. Doctor_ID;
     Price= Patient List[Key].price x time;
     return true;
return total_Medical_Report = Doctor_ID;
```

Algorithm 2. Algorithm for Smart Contract.

```
Init: uint StartBlock;
Init: unit EndBlock;
Init: bool Canceled;
Init: uint new registration;
Init: address patient_Bidder.

mapping(address=>uint256)Register
constructor(_startBlock,_endBlock):
StartBlock=_startBlock_new
EndBlock= _endBlock_new

Function placeBid():
     if msg.value == 0 then
           revert()
     else
           uint new patient_Bid = msg.value
     end
    if new patient_Bid <= patient_Bidder then
          revert()
     else
         fundsBypatient_Bidder[msg.sender_patient] = new patient_Bid
         patient_Bidder = newBid
         Bidder = msg.sender
     end
     return True

Function cancelBidding():
    canceled = true
    return True

Function withdraw():
    if canceled then
        msg.sender_patient.transfer(fundsBypatient_Bidder[msg.sender_patient])
    else
         if msg.sender_patient == owner then
         msg.sender_patient.transfer(highestBid)
    else
        msg.sender_patient.transfer(fundsBypatientBidder[msg.sender_patient]
    end
    end
   return True
```

4.3 Performance Evaluation and Results

4.3.1 Performance Analysis for Ethereum

Gas fees represent a successful transaction in the running of smart contracts and transactions, and for the Ethereum performance analysis, the gas fee is 30 million. Gas fees also depend on how much computational power is used for each transaction. The base fee is determined by block size. Assume that the block size with 15 million gallons of gas consumed is 15 million. Table 3 suggests that the appended data uses around 300,000 gas, and the new data uses around 500,00 gas. The calculated average time for 100 transactions is approximately 13 seconds due to an upper limit. This means we can reach the maximum transaction rate of 7 transactions per second.

Table 3. Number of transactions per gas consumed.

Amount of Transactions per gas consumed	Gas Consumed in normal Transaction
1	502,326
2	1004,652
5	2511,63
25	12558,15
50	25116,3

4.3.2 Scalability

We measure the scalability of the proposed system. The entire process takes less time compared to the actual Blockchain network [1]. Time can be calculated by the response time of the transactions in the Blockchain network. The average time for the proposed system generates 13 seconds for each transaction blocks. The time measurement is same for smart contract transactions. Depends on the gas price the transaction takes 36 seconds for each confirmation and generates the next few blocks before the confirmation which takes around 90 –120 seconds.

Depends on the request for the patient’s data, Data retrieval operation achieves in 54 seconds, and the append operation achieves in 1-2 minutes.

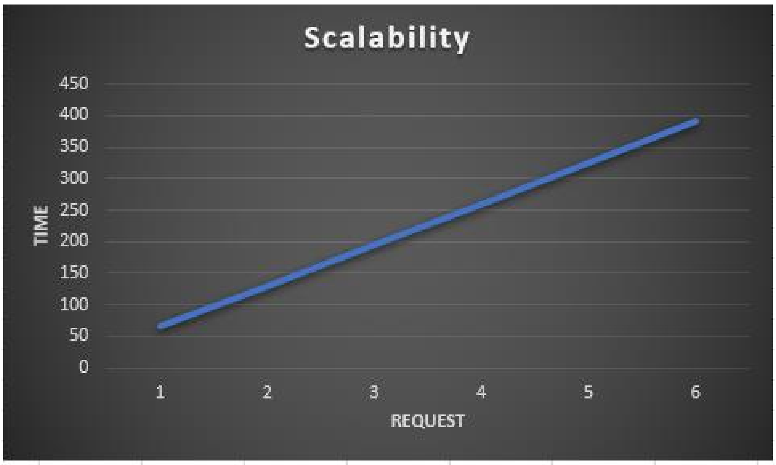

Figure 11. Calculation of Scalability.

Figure 11 explains that scalability is always a linear process and maintains the level of performance according to our suggested system. This graph explains the efficiency of the proposed system along with the request for each operation with the time and increasing the calculation of scalability clearly shows that the performance is good and achieves the criteria for the proposed system.

4.3.3 Access Control

In the smart contract agreement, which requires a signature from the patient, access control can be clearly demonstrated. Whenever a third party/unknown entity tries to use the system, the smart contract denies the request and aborts the process. This clearly demonstrates how safe and reliable the system is. A particular patient controls the data, so third parties cannot access the record. A patient holds access control for his or her records and can access their record information to avoid unnecessary security issues.

4.3.4 Integrity

Integrity is a major aspect of healthcare and one way to prove it is through communication can create through the agreement signed in the smart contract by the patient. The patient can signed the agreement while registering with the proper concerns like relatives or friends who can be able to see the data so no one has access rights to get the healthcare data without patient's authorization. In the proposed system, only the patient can be possible to alter the signed agreement.

4.4 Security Analysis of the proposed system

The Security Analysis explains more about the efficiency of proposed Healthcare system.

4.4.1 Confidentiality

The Security feature includes allowing only a patient and a doctor to communicate at one time in a pre-defined period and during the Registration Phase. Only one person at a time can register with a specified doctor. BC already saved the information about each doctor and patient in the format $(id_p, pk_d, T, R, K, C_1, C_2)$. To begin with, only patients and doctors can be able to achieve with the proper format for the healthcare data. Registered keys for patient and doctor should be used for this format. For more confidentiality features, both entities should use private keys. The doctor's private key equals $H(skd, T)\ pk$, and the patient's key equals pk_pR.

Note that $H(skd, T)$ should be used instead of a random value r because for security reasons a doctor cannot store all the different data and communications of different patients. Another thing, doctor should satisfy the conditions mentioned in the agreement along with the patient consent signed to the BC.

As a result of the timestamp, signature of the patient and doctor cannot be changed without the patient's consent, which is predefined during the smart contract signature process.

4.4.2 Data Integrity

Security features are defined in our proposed system without the patient’s knowledge no one can be able to retrieve the records. If someone is trying to do it, the system notifies to the patient through the app installed on their mobile.

Integrity is achieved by validating the signature given by both entities, i.e. the doctor and the patient, inside the BC.

The BC checks the validity of the signatures of both entities being stored in the BC. Everyone who has the public key of a patient will also be enabled to view the healthcare data from the BC, which is called public verification; our algorithm is also used in the process. The proposed cryptographic signature mechanism uses a method called the Schnorr scheme.

4.4.3 Authentication

This security feature takes care of authentication between the doctor, the patient, and the BC. When entities send messages for validation, the previous feature is used. This feature uses the Schnorr Scheme for authentication. As a result, no one other than the individual who needs the data will be able to access it. An attack could be any type like man-in-the-middle or impersonation attack.

4.4.4 Data Interoperability

Data access and data sharing are provided for the patient's convenience, but securely. A security feature based on proper IDs will be developed by BC to allow access to and sharing of data. A patient's signature and identification must be used otherwise BC will not execute the contract agreement.

4.4.5 Legality

In a smart contract, a legal agreement can be made while working on it. According to this agreement, the system is more secure because it follows the rules set by the patient. In the proposed system, legality is maintained between the patient and doctor by signing the agreement in the smart contract. BC provides legal certainty, which is more significant than any other system. Also, every phase of our proposed system includes security features to prevent unauthorized access to data. Security Analysis of our proposed system proves that the system is secure, which is helpful for the patient to trust the system.

Table 4. Comparison of different healthcare systems using blockchain with the proposed system.

Feature	[22]	[34]	[36]	[37]	Proposed System
Access Control	Yes	Yes	Yes	Yes	Yes
Confidentiality	No	Yes	No	Yes	Yes

Integrity	Yes	Yes	Yes	Yes	Yes
Authentication	Yes	No	No	Yes	Yes
Scalability	Yes	Yes	Yes	No	Yes

It can clearly explain that the proposed system is more secure than the other system [22, 34, 36,37,16] which has all the necessary security features. Table 3 explains more about the comparison of the performance evaluation of each highlighted with the Figure 11 with proposed system. Hence forth it proves along with the implementation results that proposed system has most of the security features.

5 DISCUSSION

In the digital era, the services are based on the internet setup and can be accessed any form of data at any time anywhere. Instead, the future of these services will be based on multiple stakeholders working collaboratively and sharing common resources and infrastructure. The advent of recent enabling technologies, including Blockchain is crucial to secure such networks and establishing trust among them. Blockchain integration in healthcare would likely add key features to the healthcare industry, including transparency, asset trading, and mobile healthcare apps.

The way toward the healthcare revolution is not very straightforward and needs to overcome major obstacles on its way to ensure complete success, such as scalability and transaction fees. While defining the regulations seems much more difficult, there has been no significant progress made in this area for Blockchain technology. The regulations in healthcare systems be as strict as for financial applications but still, they must cover all the required aspects. They must also be agreed upon by the relevant stakeholders. A second key hurdle is the lack of established developer knowledge on this transition. This is i.e. a limited developer's expertise and no clear picture of how and where Blockchain would add value to healthcare. Thus, it is crucial to integrate blockchain into healthcare, as this can easily be achieved with other suitable approaches. According to our vision, Blockchain will be used to add key characteristics to the healthcare systems.

Enable the security features of the blockchain technology helps to integrate the system. Providing secure healthcare systems for patients and securing their records will be achieved in this manner. The proposed system requires learning and executing blockchain technology as well as overcoming challenges regarding traditional healthcare systems. Among the blockchain platforms, there are the most effective systems available to achieve the expected results. Using Ethereum's blockchain for our proposed system makes it easier and more efficient for developers to create and design it. Ethereum supports decentralized applications along with smart contracts. Users of Ethereum can create public and private digital ledgers that are more convenient for them. According to the algorithm used in the proposed system secures the healthcare data.

Basically, studying blockchain and healthcare systems along with security features encourages us to improve the system. The main two entities in this thesis are the patient and the doctor. They use their own devices with consent from the patient to use the keys issued during the registration phase. The proposed system requires patient consent and verification at each phase to make the security features more effective. A patient can monitor if someone tries to access their record. By using their own devices, the patient gets a notification if someone tries to hack or open the record. Blockchain can provide key entities such as confidentiality, Scalability, Integrity, and Interoperability for the record. As long as the patient/doctor can append or retrieve the data, all key entities will verify the signature by means of a public key. The smart contract captures the patient's concern and implements the patient's signature and requirements into code developed by the developer. Each time, the blockchain verifies the code before the login process.

Having a secure way to protect healthcare systems through the blockchain is an advantage. The process of developing cryptographic mechanisms and implementing those increases the feasibility of the system. It's a fact that the blockchain miner works perfectly with written codes. The ether price is also determined by the append and retrieve phases, phases that are very simple and easy to understand. From these simple codes, patients and doctors can verify records based on these simple codes. With this implementation, the scalability ratios are more efficient without wasting a lot of time. It takes only a few seconds to make the system much faster and safer. Furthermore, security in our proposed system is guaranteed by the use of a cryptographic mechanism with keys and by the implementation of smart contract codes. As a result, we propose a security-based system to achieve the abstract of our thesis.

The future work of this thesis needs to include multiple other entities in smart healthcare use cases, including nurses, and medical laboratories. These include relatives and multiple other hospitals, which can help improve interoperability. Moreover, if a patient needs to be referred to another doctor, this framework can allow secure and easier data accessibility than the traditional system. However, in order to fully deploy this work in the healthcare sector, several improvements are required, in addition to the creation of novel privacy-preserving authentication schemes considering various actors in the system. In the future, privacy and other network parameters can also be evaluated such as network utilization, latency, and energy consumption. Nowadays, the cost of running a blockchain is quite high, so it is critical that healthcare systems consider cost-efficient blockchain solutions. Blockchain for EHR proves that healthcare systems are more efficient than electronic healthcare systems without Blockchain. A few new techniques are also emerging to enhance health systems within Blockchain that will help us to improve our existing system in the future.

6 CONCLUSION

In the current healthcare systems, main challenges are to make sure the data of patients can be accessed by entities with the security features, such as doctors, nurses, and other medical personnel. Recently, blockchain technology has shown immense potential in the domain of healthcare. This is because it enables key characteristics such as immutability, data security, and privacy, a trusted computing environment, and process monitoring/tracking among others. In this thesis, the main contribution is to design a patient data accessibility mechanism in a hospital use case scenario using blockchain technology. The mathematical authentication scheme is used in the proposed healthcare system. The feasible solution can be shown in the results for the proposed system.

The healthcare sector is very demanding at the moment. Utilizing current technology to protect healthcare data by focusing on the patient and a future recording system. We should also consider smart healthcare systems to make hospital care more effective. Blockchain technology provides privacy schemes to protect healthcare data, which are proven by cryptographic operations and implemented in applications to serve better healthcare system and helps in patient well being. With the help of proposed system concept, healthcare systems can keep the patients record safely and maintain full control of their privacy.

REFERENCES

[1] Ramani V., Kumar T., Breaken A., Liyanage M., Ylianttila M. (2018) Secure and Efficient Data Accessibility in Blockchain-Based Healthcare Systems. IEEE Global Communications Conference.

[2] Kumar T., Ramani V., Ahmad I., Breaken A., Harjula E., Ylianttila M. (2018) Blockchain Utilization in Healthcare: Key requirements and Challenges. IEEE 20th International Conference on E-Health Networking, Applications and Services.

[3] Kumar T., Breaken A., Ramani V., Ahmad I., Harjula E., Ylianttila M. (2019) SEC-BlockEdge: Security Threats in BlockChain-Edge Based Industrial IoT Networks. 11th International Workshop on Resilient Networks Design and Modeling.

[4] Beck R. (2018) Beyond BitCoins: The rise of BlockChain World, p. 54- 58.

[5] Aste T., Tasca P., and Matteo T D. (2017) Blockchain technologies: The foresecable impact on society and industry, p. 18-28.

[6] Manzoor A., Hu Y., Liyanage M., Ekparinya P., Thilakarathna K., Jourjon G., Seneviratne A., Kanhere S., and Ylianttila M. (2018) Demo: A Delay-Tolerant Payment Scheme on the Ethereum Blockchain. 19th IEEE Internation Symposium on a World of Wireless, Mobile and Multimedia Networks.

[7] Tiago M., Fernandez-carames., Paula Fraga-Lamas. (2018) A Review on the Use of Blockchain Technologies for the Internet of Things. IEEE Access.

[8] Li X., Jiang Peng., Chen J., Luo X., Wen Q. (2020) A Survey on the security of blockchain systems, p. 841- 853.

[9] Siyal A., Junejo A., Zawish M., Ahmed K., Khalil A., Soursou G. (2019) Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives.

[10] Watanabe H., Fujimura S., Nakadaira., Miyazaki Y., Akutsu A., Kishigami J. (2016) Blockchain contract: Securing a blockchain applied to smart contracts. IEEE International Conference on Consumer Electronics.

[11] Weiner J., Campos C., Urrutia M., Sigulem D. (2008) Security Requirements for a Lifelong Electronic Health Record System: An Opinion. The Open Medical Informatics Journal.

[12] Radler M., Li W., Karame G., Davi L. (2018) Sereum: Protecting Existing Smart Contracts Against Re-Entrancy Attacks.

[13] Wood G. (2022) Ethereum: A secure Decentralised Generalised Transaction Ledger. Yellow Paper.

[14] Mandl K., Szolovits P., Kohane I. (2001) Public Standards and Patients control: How to keep electronic medical records accessible but private. BMJ Clinical Research.

[15] Kishigami J., Fujimura S., Watanabe H., Nakadira A., Akutsu A. (2015) The Blockchain-Based Digital Content Distribution System. IEEE Fifth International Conference on Big Data and Cloud Computing.

[16] Sudarsono A., Yuliana M., Darwito H. (2017) A secure data sharing using identity-based encryption scheme system. International Conference on science in Information Technology.

[17] Conti M., Kumar S., Lal C., Ruj S. (2018) A Survey on Security and Privacy Issues on BitCoin. IEEE Communications Surveys and Tutorials.

[18] Holotescu C., Holotescu V., Holotescu T. (2018) Understanding Blockchain Technology and how to get involved.

[19] Henry R., Herzeberg A., Kate A. (2018) Blockchain Access Privacy: Challenges and Directions. IEEE Security and Privacy.

[20] Khan L., Wei Y., Muhammed A., Siyuan W., Kai L. (2018) A Multiple Blockchains Architecture on Inter-Blockchain communication. IEEE International Conference on Software Quality, Reliability and Security Companion.

[21] Dasaklis T., Casino F., Patsakis C. (2018) Blockchain Meets Smart Health: Towards Next Generation Healthcare Services. International Conference on Information, Intelligence, Systems and Applications.

[22] Azaria A., Ekblaw A., Vieira T., Lippman. (2016) MedRec: Using BlockChain for Medical Data Access and Permission Management. International Conference on Open and Big Data.

[23] Qiu J., Liang X., Sheety S., Bowden D. (2018) Towards Secure and Smart Healthcare in Smart Cities Using BlockChain. IEEE International Smart Cities Conference.

[24] Alexaki S., Alexandris G., Katos V., Petroulakis N. (2018) Blockchain-based Electronic Patient Records for Regulated Circular Healthcare Jurisdictions. IEEE International Workshop on Computer Aided Modeling and Design of Communications Links and Networks.

[25] Mondal S., Shafi M., Gupta S., Gupta S. (2022) Blockchain based Secure Architecture for Electronic Healthcare Record Management. GMSARN International Journal.

[26] Bartoletti M., Pompianu L. (2017) An Empirical Analysis of Smart Contracts: Platforms, Applications and Design Patterns.

[27] Kumar T., Breaken A., Liyanage M., Ylianttila M. (2017) Identity privacy preserving biometric based authentication scheme for Naked healthcare environment. IEEE International Conference on Communications.

[28] Liu X., Wang Z., Jin C., Li F., Li G. (2019) A Blockchain-Based Medical Data Sharing and Protection Scheme. IEEE Access.

[29] Xia Q., Sifah E., Asamoah K., Gao J., Du X., Guizani M. (2017) MeDShare: Trust-Less Medical Data Sharing Among Cloud Services Providers via Blockchain. IEEE Access.

[30] Jo J., Seo J., Lee H. (2007) Biometric Digital Signature Key Generation and Cryptography Communication Based on FingerPrint. Frontiers in Workshop, First Annual International Workshop FAW.

[31] Huang C., Lee H., Lee D. (2012) A Privacy- Strengthen Scheme for E- Healthcare Monitoring System. Journal of Medical Systems.

[32] Halpin H., Piekarska M. (2017) Introduction to Security and Privacy on the Blockchain. IEEE European Symposium on Security and Privacy Workshops.

[33] Pham H., Tran T., Nakashima Y. (2018) A Secure Healthcare Systems for Hospital Using Blockchain Smart Contract. IEEE Globecom Workshops.

[34] Zhang P., Walker M., White J., Schmidt D., Lenz G. (2017) Metrics for accessing blockchain-based healthcare decentralizes apps. IEEE International Conference on e-Health Networking, Applications,Services.

[35] Morita H., Schuldt J., Matsuda., Hanaoka G., Iwata T. (2016) On the Security of the Schnorr Signature Scheme and DSA Against Related-Key Attacks. International Conference on Information Security and Cryptology.

[36] Xia Q., Sifah E., Smahi A., Amofa S., Zhang X. BBDS: BlockChain-Based Data-Sharing for Electronic Medical Records in Cloud Environments. p.44.

[37] Yang H., Yang Y. (2017) A Blockchain-based Approach to the secure sharing of Healthcare Data.

[38] Suryadevara N., Mukhopadhayay M. (2018) Internet of things: A review and future perspective.

[39] Mueller P., Bergsträßer S., Rizk A., Steinmetz R. (2018) The BitCoin Universe: An Architectural Overview of the BitCoin Blockchain.

[40] Khatoon A. (2020) A Blockchain-Based Smart Contract System for Healthcare Management.

[41] Litchfield., A T., Arshad K. (2019) A Review of issues in Healthcare Information Management Systems and Blockchain Solutions. CONF-IRM.

[42] Skiba., D.J. (2017) The Potential of Blockchain in Education and Health Care. Nursing Education Perspectives.

[43] Heston., T. (2017) A case study in blockchain healthcare Innovation.

[44] Dimitrov., D.V., (2019) Blockchain Applications for HealthCare Data Management. HealthCare Informatics Research.

[45] Genestier P., Zouarhi S., LimeuxP., Excoffier D., Prola A., Sandon S., Temerson., J.M. (2017) Blockchain for Consent Management in the ehealth environment: A nugget for privacy and security challenges.

[46] Gordon., W.J., Catalini C. (2016) Blockchain technology for healthcare: Facilitating the transition to patient-driven interoperability. Computational and Structural Biotechnology Journal.

[47] Kuo T., Kim H., Machado M. (2017) Blockchain distributed ledger technologies for biomedical and health care applications. Journal of the American Medical Informatics Association.

[48] Brennan. B. (2017) Blockchain HIE Overview: A Framework for Healthcare Interoperability. Telehealth Med.

[49] Radanovic I., Likic R. (2018) Opportunities for use of blockchain technology in medicine. Applied Health Economics and Health Policy.

[50] Hoy., M.B., (2017) An Introduction to the Blockchain and its implications for Libraries and Medicine. Medical reference services quarterly.

[51] Wang H., Song, Y. (2018) Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain. Journal of Medical Systems.

[52] Hylock, R.H and Zeng, X.A, "A Blockchain Framework for Patient-Centered Health Records and Exchange (HealthChain): Evaluation and Proof-of-Concept Study," Journal of Medicine, 2019.

[53] Guo R., Shi,H .,Zhao, Q.,Zheng, D. (2018) Secure Attribute- Based Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems. IEEE Access.

[54] Syed E., A I; Abdelaziz M., Meghahed M., Azeem M. (2020) A New Supervision Strategy based on Blockchain for Electronic Health Records. International Conference on Electrical Engineering.

[55] Thwin T., Vasupongayya S. (2019) Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Security and Communication Networks.

[56] Yang X., Li T., Xi W., Chen A., Wang, C. (2020) A Blockchain- Assisted Verifiable Outsourced Attribute-Based Signcryption Scheme for EHRs Sharing in the Cloud. IEEE Access.

[57] NagaSubramanian G., Sakthivel R., Patan R., Gandomi A., Sankayya M., Balusamy B. (2018) Security e-health records using keyless signature infrastructure blockchain technology in the cloud. Intelligent Biomedical Data Analysis and Processing.

[58] Huang J., Wei Qi., Asghar M., Meads A., Tu Y. (2019) Med Bloc: A BlockChain-Based Secure EHR System for Sharing and Accessing Medical Data. IEEE International Conference on Trust, Security and Privacy in Computing and Communications.

[59] Roehrs A., Costa C., Righi R. (2017) OmniPHR: A distributed architecture model to integrate personal health records. Journal of Biomedical Informatics.

[60] Kalaipriya R., Devadharshini S., RajMohan R., Pavithra M., AnanthKumar T. (2020) Certain investigations on Leveraging Blockchain Technology for Developing Electronic Health Records. International Conference on System, Computation, Automation, and Networking.

[61] Pronaya B., Tanwar S., Umesh B., Sudhanshu T., Kumar N. (2020) BinDaas: Blockchain-Based Deep-Learning as-a-Service in Healthcare 4.0 Applications. IEEE transactions on Network Science and Engineering.

[62] Vukovic J., Ivankovic D., Habl C., Dimnjakovic J. Enablers and barriers to the secondary use of health data in Europe: general data protection regulation perspective. Archives of Public Health.

[63] Djenna A., Saidouni D. (2018) Cyber-Attacks Classification in IoT-based-Healthcare Infrastructure. Cyber Security in Networking Conference.

[64] Sadki S., Bakkali H., Mohammed A. (2017) Towards Conflicts prevention among privacy policies: A Comparative study of major Privacy laws and regulations for Healthcare. International Conference of Cloud Computing Technologies and Applications.

[65] Marshal R., Gobinath K., Venkateswara Rao V. (2021) Proactive Measures to Mitigate Cyber Security Challenges in loT based Smart Healthcare Networks. IEEE International IOT, Electronics and Mechatronics Conference.

[66] Krenchel D., Hartbaurer M. (2008) The LENUS Master Patient Index: Combining Hospital Content Management with a Healthcare Service Bus. International Symposium on Computer-Based Medical Systems.

[67] Muro N., Larburu N.,Torres J., Kerexeta J., Artola G., Arrue M., Macia I., Seroussi B. (2019) Architecture for a Multimodal and Domain-Independent Clinical Decision Support System Software Development Kit. Annual Intenational Conference of the IEEE Engineering in Medicine and Biology Science.

[68] Tan C., Ji Q. (2016) An approach of identifying cryptographic algorithm from ciphertext. IEEE International Conference on Communication Software and Networks.

[69] Liu Q., Li Y., Hao L., Peng H. (2010) Two efficient variants of the RSA Cryptosystem. International Conference on Computer Design and Applications.

[70] Henriques M., Verneker N. (2017) Using Symmetric and Asymmetric Cryptography to secure communication between devices in IoT. International Conference on IoT and Application.

[71] Farooq S., Hussain S., Ustun T. (2019) Elliptic Curve Digital Signature Algorithm (ECDSA) Certificate based Authentication Scheme for Advanced Metering Infrastructure. Innovations in Power and Advanced Computing Technologies.

[72] Liu B., (2021) Overview of Basic Principles of Blockchain. International Conference on Intelligent Computing, Automation and Applications.