PRIVACY PRESERVATION OF HEALTH RECORDS USING BLOCKCHAIN TECHNOLOGY

A Thesis submitted

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS
FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY
IN
COMPUTER SCIENCE AND ENGINEERING

By

YOGESH SHARMA
18SCSE3010007

Supervisor

Dr. B. BALAMURUGAN
Professor

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY
Plot No 2, Sector 17-A Yamuna Expressway
Greater Noida, Uttar Pradesh
INDIA

OCTOBER, 2021

CANDIDATE DECLARATION

I hereby certify that the work which is being presented in the thesis, entitled "**PRIVACY PRESERVATION OF HEALTH RECORDS USING BLOCKCHAIN TECHNOLOGY**" in partial fulfilment of the requirements for the award of the degree of Doctor of Philosophy in Faculty of Computer Science and Engineering and submitted in Galgotias University, Uttar Pradesh is an authentic record of my own work carried out during a period from September 2018 under the supervision of **Dr. B. BALAMURUGAN**, Professor, School of Computing Science and Engineering, Galgotias University.

The matter embodied in this thesis has not been submitted by me for the award of any other degree or from any other University/Institute.

(YOGESH SHARMA)

This is to certify that the above statement made by the candidate is correct to the best of our knowledge.

(Dr. B. BALAMURUGAN)
Supervisor
School of Computing Science and Engineering

Galgotias University Uttar Pradesh
School of Computing Science & Engineering

CERTIFICATE

This is to certify that **YOGESH SHARMA** has presented his pre-submission seminar of the thesis entitled **" PRIVACY PRESERVATION OF HEALTH RECORDS USING BLOCKCHAIN TECHNOLOGY “** before the committee and summary is approved and forwarded to School Research Committee of School of Computing Science & Engineering, in the Faculty of Engineering & Technology, Galgotias University Uttar Pradesh.

Dean – SCSE

Dean – Ph.D & PG

The Ph.D. Viva-Voice examination of **Yogesh Sharma** Research Scholar, has been held on

Supervisor

External Examiner

APPROVAL SHEET

This thesis/dissertation/report entitled **" PRIVACY PRESERVATION OF HEALTH RECORDS USING BLOCKCHAIN TECHNOLOGY “** by Yogesh Sharma is approved for the degree of Doctor of Philosophy

Examiner	**Supervisor**	**Chairman**

STATEMENT OF THESIS PREPARATION

1. Thesis title: Privacy Preservation of Health Records Using Blockchain Technology.
2. Degree for which the thesis is submitted: Doctor of Philosophy in CSE
3. The thesis preparation was done based on the thesis guide.
4. The thesis format and specifications are keenly followed while preparing the thesis.
5. The guidelines for the arrangement of the thesis is adhered carefully.
6. The thesis is prepared in such a way that it does not have any plagiarism from any sources.
7. All the references have been cited appropriately within the document.
8. The thesis is original and has no reference of being submitted anywhere for the award of the degree.

(Signature of the student)

Name: Yogesh Sharma
Roll No. 18SCSE3010007

ACKNOWLEDGEMENTS

First of all, I thank to **almighty** for his blessings, life, health, and positive energy that helped me move at every stage throughout my life so far. Without the support from Maa Saraswati, Lord Sai, nothing would have been possible.

I wish to express my sincere appreciation to my guide, **Dr. B. Balamurugan, Professor (SCSE),** who has the substance of a genius: right from my thought of seeking admission in a doctorate course, he convincingly guided and encouraged me to be professional and do the right things even when the road got tough. Without his persistent help, the goal of this dissertation would not have been realized. You had always been a true source of inspiration for me and I would always look up to you to learn a lot more things. Please accept my vehement protestations of gratitude Sir.

I must owe a special commitment of gratitude to Hon'ble Chancellor Mr. Suneel Galgotias, Mr. Dhruv Galgotias, CEO, and Hon'ble Vice-Chancellor, Galgotias University for their valuable cooperation.

Besides my advisors, I would like to thank the entire research committee, Dean, School of Computing Science & Engineering, Dean Research, Research coordinator for the guidance, help and moral support during course of my research work and all faculties of School of Computing Science & Engineering who helped me in one or the other way.

I would also like to thank, Prof. M.L. Goyal (Vice Chairman, Academics), Dr. Neelam Sharma (Director), Prof. S.S. Deswal (Dean, Academics) and Prof. Namita Gupta (HoD, CSE) of Maharaja Agrasen Institute of Technology, Rohini, Delhi, for providing encouragement and necessary research environment and facilities.

Last but not least, I want to express my deepest gratitude to my family. First and foremost, I would like to thank my father Sh. S.P. Sharma, great love of my family, my mother Mrs. Saroj Sharma and my wife Mrs. Kiran Sharma, for their unconditional, continuous motivation, support and guidance right from the very idea of pursuing doctoral research to the end of it. All of you have been my great pillars of strength and the very reason of achieving laurels in my life. Exceptional mention for my loving son Master Avik Sharma and loving daughter Ms. Avni Sharma to bear with all my absence during your growth years and be very loving and caring kids always.

Yogesh Sharma

ABSTRACT

New technology and innovation have always been a top priority in any organization. Several organizations and industries are in search of new technology which will improve the efficiency as well as growth of an organization. For this, artificial intelligence was focused, but still severity and privacy were compromised. Therefore, to improve the security and privacy of data within an organization and to improve the performance, blockchain technology has emerged. Blockchain is a way of storing and sharing data in a way that is distributed, transparent and temper proof. Blockchain technology has allowed the solution to rapidly scale and to adapt to perform multiple tasks across industries. It provides distinct innovative ways which will boost the economic growth, reduced cost and time, with enormous benefits and progress in several domains. Blockchain can be very useful in healthcare industry. Healthcare generates an enormous amount of data which include laboratory test reports, imaging tests such as Xrays, CTScans, financial documents, previous medications given to the patients, previous medical history and last appointments. So, several patients under healthcare center, constitutes a vast amount of data which is expanding at a very high speed.

In recent studies, in 2012, a report of The Institute of Medicine (IOM), titled “Best case at cover cost: the path to continuously learning healthcare in America” stated that American’s healthcare system has become far too complex and costly to continue business as usual. It has several inadequacies and incapability to achieve quick and deep clinical knowledge which hampers all improvements needed in patients care and safety.

Also, medical data is scattered throughout various medical institutions and data standards are not uniform, resulting in low level of interoperability of medical data. Under these circumstances, there is no assurance of the integrity and reliability of patient’s data. The huge medical data is susceptible to data loss, data security, personal privacy leaks and other issues. Therefore, to overcome challenges and to make healthcare data more private and secure, blockchain technology is used. This ensures integrity of data and is also helpful in distribution of healthcare data among several nodes in a network.

The work done in thesis, is focused on to overcome some major challenges of security and privacy in healthcare domain. To ensure privacy, the prime objective was to find a suitable method and technology to keep our medical health records of several patients and medical institutions at one centralized place. This will ensure an ease of accessibility in decentralized storage while keeping the security and privacy of electronic medical records.

The Electronic Health Records also known as EHR are the basic health information of a patient such as medical diagnosis, treatment and medication. These medical records can be stored on a network, hence there is strict need for a network where these medical records can be stored safely with high level of security and privacy. The blockchain technology provides that desired level of security and privacy of the data stored on the blockchain. A blockchain works on the concept of decentralized network eliminating the chances of failure of centralized node or altering the data. A blockchain is a chain of blocks connected in the network with each block is secured with the hash value and thus provide security and privacy to the data stored in the block. There are mainly two types of blockchain namely Public Blockchain and a Private Blockchain. Our idea is to create a private blockchain with three nodes/participants as Patients, Clinicians and Lab. The owner of the blockchain creates the IDs for all three participants and could also grants and revoke the access to the participants of the chain. With this type of chain all the medical records are stored and accessible from only one place at any time and from anywhere. The objective is to create a system to implement EHRs using blockchain technology and make EHRs more secure and private in a Permissioned or a Private Blockchain. For this we will use Hyperledger Fabric and Composer platform, which helps in creation of a private blockchain.

After securing the medical health records in a private blockchain using Hyperledger platform, our next objective is to develop a technique or method that could tighten the security and increase the privacy of the electronic medical records. Our approach will start from obtaining the health data as input in a blockchain network, apply the tensor product method and swam intelligent in order to increase the security and privacy of the record. The tensor product operation converts the original data into protected data while the swam intelligence will consists of dragonfly (DA)and crow search algorithm (CSA) for better optimization. The performance will be measured in terms of maximum accuracy and minimum information loss.

TABLE OF CONTENTS

Declaration i

Certificate ii

Approval Sheet iii

Statement of Thesis Prepration iv

Acknowledgement v

Abstract vii

Table of Contents ix

List of Figures xiii

List of Tables xv

List of Abbreviations and Symbols xvi

List of Publications xviii

Chapter 1: Introduction

1.1 Introduction 1

1.2 Major challenges 2

1.3 Electronic Healthcare Records 2

1.3.1. Challenges in Healthcare Records 4

1.4 Blockchain architecture 5

1.4.1Types of Blockchains 6

1.4.1.1 Public Blockchain 6

1.4.1.2 Private Blockchain 7

1.4.1.3 Consortium Blockchain 8

1.5 Structure of a Block 8

1.5.1 Blockchain Process 11

1.6 Privacy Preserving Methods in Blockchains 13

1.6.1 Security 14

1.6.2 Hashing 14

1.6.3 Privacy 16

1.7 Objectives 17

1.7.1 Objective 1: Security and Privacy of Electronic Health Record in a Decentralized Storage 17

1.7.2 Objective 2: Privacy Preservation of Electronic Health Record in a Private Blockchain using Hyperledger Platform 18

1.7.3 Objective 3: Preserving the Privacy of Electronic Medical Records in Blockchain Network using Tensor Product and Hybrid Swarm Intelligence 18

1.8 Conclusion 19

Chapter 2: Literature Review 20

2.1Search and Selection Process 21

2.2Related Work on Blockchain 21

2.2.1 Blockchain Overview 22

2.2.2 Consensus Algorithms 23

2.2.2.1 Types of Consensuses Algorithms 24

2.2.2.2 Proof of Work 24

2.2.3 Bitcoin or Blockchain 25

2.2.4 Workflow of Bitcoin 25

2.3 Healthcare Industry 28

2.4 Cryptography in Blockchain 33

2.5 Related Work on Swarm Intelligence. 36

2.5.1 Dragonfly Algorithm 36

2.5.2 Crow Search Algorithm 37

2.5.3 The Challenges Confronted by Conventional Methodologies 38

2.6 Conclusion 38

Chapter 3: Various Applications of Blockchain Business Models 40

3.1 Introduction 40

3.1.1 Blockchain: Adding Value to a Business Process 40

3.1.2 Consortium Blockchain 41

3.1.3 Smart Contract 41

3.2 Electronic Voting using Blockchain 43

3.3 Smart and Collaborative Transportation 47

3.3.1 Connected Vehicle 48

3.3.2 Maas 48

3.3.3 Atms 48

3.4 Industrial Trading Business Model using Blockchain 53

3.5 Conclusion 54

Chapter 4: Preserving the privacy of electronic health records using blockchain 55

4.1Introduction 55

4.2Blockchain in Preserving EHR 57

4.2.1 Structure Design and Architecture 57

4.3 Structure Implementation 63

4.3.1 Hyperledger Fabric 63

4.3.2 Hyperledger Composer 63

4.4 Conclusion 66

Chapter 5: Preventing the Theft using Blockchain Technology 68

5.1 Introduction 68

5.2 Preventing the Theft of Human Organ and Rare Blood Group 69

5.2.1. IoT Device 70

5.2.2 IoT for Patients 71

5.2.3 IoT for Physicians 71

5.2.4 IoT for Hospitals 71

5.2.5 IoT for Insurance Companies 72

5.3 Proposed Methodology 72

5.3.1 Block 73

5.3.2 Types of Blockchain 74

5.3.2.1 Public or Permissionless 74

5.3.2.2 Private or Permissioned 75

5.3.2.3 Hybrid 76

5.3 RSA 77

5.4 System Architecture 77

5.4.1 Architecture Block Diagram 1: Authentication 77

5.4.2Architecture Block Diagram 2: Creating Block 78

5.4.3 Architecture Block Diagram 3: Public Ledger 79

5.4.4 Architecture Block Diagram 4: Request Access of Safe 80

5.4 Conclusion 83

Chapter 6: Privacy Preservation in Blockchain Network using Tensor Product and Hybrid Swarm Intelligence 84

6.1 Introduction 84

6.2 Swarm Intelligence 87

6.2.1. Working Principle 88

6.2.2. Swarm Intelligence-based Algorithms 88

6.2.2.1. Dragonfly Algorithm 88

6.2.2.2. Crow Search Algorithm 89

6.3 Structure of Blockchain 89

6.3.1. Blockchain Network Bridge 89

6.3.2 Blockchain Service 89

6.3.3 Blockchain Wallet 90

6.3.4 Sensor Bridge 90

6.4 Research Methodology 90

6.4.1 Proposed Privacy Preservation 90

6.4.2 Privacy Preservation 92

6.4.3 Proposed Dragonfly-Crow Search Algorithm for the Generation of SU Coefficient 93

6.5. Implementation 99

6.6. Results and Discussion 103

6.6.1 Experimental Setup 103

6.6.2. Dataset Description 103

6.6.3 Evaluation Metrics 103

6.6.3.1. Accuracy 104

6.6.3.2 Information Loss 104

6.6.4 Competing Methods 104

6.6.5. Comparative Analysis 104

6.6.5.1. Analysis by Dataset-1 104

6.6.5.2. Analysis by Dataset-2 105

6.6.5.3. Analysis by Dataset-3 106

6.6.5.4. Analysis by Dataset-4 107

6.6.5.5. Analysis for Average and Standard Deviation 108

6.6.6. Comparative Discussion 109

6.7. Conclusion 109

Chapter 7: Conclusion and Future scope 111

References 114

LIST OF FIGURES

Figure Name	Page No.
Figure 1.1 Public Blockchain	6
Figure 1.2 Private Blockchain	7
Figure.1.3 Structure of Block	9
Figure 1.4 Markel Tree	10
Figure. 1.5 Blockchain Process	11
Figure. 1.6 Blockchain Layers	12
Figure. 2.1 Paper Selection and Review Process	21
Figure. 2.2 ETL Process in Healthcare Industry	29
Figure. 3.1 Basic Structure of Smart Contract	42
Figure. 3.2 Voting Authentication and Vote Casting Process	44
Figure. 3.3 Smart Transportation	51
Figure. 4.1 A Sample Glimpse of An Electronic Health Record	56
Figure. 4.2 Electronic Healthcare Record Process Diagram	57
Figure. 4.3 (A)The Architecture of The Structure	58
Figure. 4.3 (B)The Architecture of The Biological Blockchain	58
Figure. 4.4 The Block Structure of The Biological Blockchain	62
Figure. 4.5 A Biological Service Framework Based on Blockchain Technology	62
Figure. 4.6 Flowchart of The Whole Process	65
Figure. 4.7 Sick Person Node Created and Added to The Network	66
Figure. 4.8 A Record of All Transactions That Executed in The Network	66
Figure. 5.1 A Public Blockchain	75
Figure. 5.2 A Private Blockchain	76
Figure. 5.3 Authentication Process	78
Figure. 5.4 Creation of Block for Blockchain	79
Figure. 5.5 Request to Public Ledger	80
Figure. 5.6 Request to Access Safe	81
Figure. 5.7 (a)Creating the Hash Functions	82
Figure. 5.7 (b)Creating the Hash Functions	83

Figure. 6.1 A System Model of Blockchain with Privacy 91

Figure. 6.2 Block Diagram of Blockchain-Based Privacy Preservation Using Proposed D-CS Technique 92

Figure. 6.3 (A)-(G) Various Steps of Implementation on Four Datasets 99-102

Figure. 6.4 Method Analysis-Based on Iterations by The Dataset-1 with Respect To A) Accuracy And B) Information Loss 105

Figure. 6.5 Method Analysis with Iterations by The Dataset-2 with Respect to the A) Accuracy And B) Information Loss 106

Figure. 6.6 Method Analysis with Iterations by Dataset-3 with Respect to the A) Accuracy And B) Information Loss 107

Figure. 6.7 Method Analysis with Iterations by Dataset-4 with Respect to the A) Accuracy And B) Information Loss 108

LIST OF TABLES

Table Name **Page No.**

Table 2.1 Comparative Study of Different Platforms in Blockchain 26-28

Table 2.2. Various Proposed Methods with its Advantages and Disadvantages 34-36

Table 4.1 Permissions for the Three Types of Transaction Bodies 61

Table 6.1 Analysis Based on Average and Standard Deviation 108

Table 6.2. Comparative Analysis 109

LIST OF ABBREVIATIONS

EHR-	Electronic Health Record
EMR-	Electronic Medical Record
PHR-	Physical Health Record
CBDM-	Controllable Blockchain Data Management
P2P-	Peer- to- Peer
DLT-	Distributed Ledger Technology
SHA-	Secure Hash Algorithm
HD-	Hashed Data
HF-	Hash Function
MD-	Message Digest
RSA-	Rivest, Shamir, Adleman
AES-	Advanced Encryption Standard
DA-	Dragonfly
CSA-	Crow Search Algorithm
MRI-	Magnetic Resonance Imaging
BFT-	Byzantine Fault Tolerance
POW-	Proof of Work
PBFT-	Practical Byzantine Fault Tolerance
FBA-	Federated Byzantine Agreement
ETH-	Ether
IoT-	Internet of Things
HGD-	Healthcare Data Gateway
BSPP-	Blockchain-based Secure and Privacy-Preserving

SIFF - Sibling Intractable Function Families

CBDM - Controllable Blockchain Data Management

V2I- Vehicle to Infrastructure

Maas- Mobility As A Service

ATMS- Advanced Traffic Management System

CITS- Cooperative Transportation System

DAV- Drone Automated Vehicle

V2V- Vehicle to Vehicle Communication

IVTP- Intelligent Vehicle Trust Point

SU- Solidity and Utility

D-CS- Dragonfly-Crow Search

ECDSA- Elliptic Curve Digital Signature Technique

GA- Genetic Algorithm

LIST OF PUBLICATIONS

1. Sharma, Y., & Balamurugan, B. (2020). Preserving the privacy of electronic health records using blockchain. Procedia Computer Science, 173, 171-180.

2. Sharma, Y., & Balamurugan, B. (2020). A survey on privacy preserving methods of electronic medical record using blockchain. Journal of Mechanics of Continua and Mathematical Sciences, 15(2), 32-47.

3. Sharma, Y., Balamurugan, B., & Khan, F. (2020). Blockchain and Distributed Ledger System. In Blockchain, Big Data and Machine Learning (pp. 177-206). CRC Press.

4. Sharma, Y., Balamurugan, B., & Khan, F. (2020). Blockchain and Big Data in the Healthcare Sector. In Blockchain, Big Data and Machine Learning (pp. 207-231). CRC Press.

5. Sharma, Y., Balamurugan, B., Sreeji. (2020). Healthcare analytics. In Blockchain and Machine Learning for E-Healthcare Systems (pp.211–230). IET.

6. Sharma, Y., Balamurugan, B., & Sengar, N. (2021). Electronic Voting—Cloud Storage—Smart and Collaborative Transportation—Blockchain and International Trading—Blockchain Business Models. In Convergence of Blockchain Technology and E-Business (pp. 85-109). CRC Press.

7. Sharma, Y., Balamurugan, B., Snegar, N., & Ilavendhan, A. (2021). How IoT, AI, and Blockchain Will Revolutionize Business. In Blockchain, Internet of Things, and Artificial Intelligence (pp. 235-255). Chapman and Hall/CRC.

8. Sharma, Y., & Balamurugan, B. (2021). Blockchain technology in preventing the theft of human organ and rare blood group. Turkish Journal of Physiotherapy and Rehabilitation, 32, 3.

9. Sharma, Y., & Balamurugan, B. (2021). A Novel Approach for Privacy Preservation in Block Chain Network Using Tensor Product and A Hybrid Swarm Intelligence. International Journal of Mobile Computing and Multimedia Communications (IJMCMC), Vol.12. Issue 4.

CHAPTER 1

INTRODUCTION

1.1 Introduction

When Satoshi Nakamoto introduced the notion of cryptocurrency known as Bitcoin in 2008, the blockchain technology was born (Nakamoto, 2008). The Bitcoin network made use of blockchain technology to keep track of transactions involving Bitcoin cryptocurrency transfers. For many years, blockchain technology was primarily focused on cryptocurrency. The notion of Bitcoin was presented in the first iteration of blockchain. The most widely used application of blockchain was electronic cash, sometimes known as cryptocurrency, which was created using Bitcoin. It is a decentralised ledger technology with all nodes have access to the ledger, allowing all nodes to be kept up to date at all times. Blockchain technology is immutable because once the ledgers are updated with the information, no node can make any alterations or modifications to the ledger. The blockchain technology intends to decentralise asset transactions on the internet network by using a network of networks known as a ledger (Pilkington 2016). Because this ledger is shared across all nodes in the network, it is referred to as a decentralised ledger, and it operates in a peer-to-peer mode. The blockchain technology allows users to access the technology from anywhere, at any time; all that is necessary is a working internet connection.

Vitalik Buterin introduced Ethereum, a second-generation blockchain network, in 2013. Ethereum is a Blockchain platform that is open source and programmable (Buterin, 2014). Instead of creating separate blockchain networks for different sorts of cryptocurrencies, Buterin recommended that a single programmable blockchain network be utilised to create a variety of applications.

In blockchain two type of permission are used;

1.Permissionless

2.Permissioned

The applications created using this technology are more secure and protect both the user and the customer's privacy. Customers who use the business models may additionally require sensitive data such as their PAN number, Aadhaar number (in India), phone number, and so on. However, if blockchain technology is implemented, sensitive information required by the organisation will not be disclosed or exploited. As a result, blockchain technology would be an excellent choice for developing applications that contain sensitive information.

1.2 Major Challenges

Confidentiality, Integrity, Authentication, and Non-Repudiation are the four basic requirements for any network (Kessler, 2019) Data security has always been a major goal for any technology, and efforts are constantly being made to create a secure network so that nodes may communicate securely with one another.

As a result, the research's goal is to give full proof network security solutions for a system using Blockchain technology. On order all four of these elements must be essentially present. There could be a variety of approaches to ensuring security and privacy.

1.3 Electronic Health Records

Patients' records, such as electronic-health-records (EHR), electronic-medical-records (EMR), and patient-health-records (PHR), must be maintained continually after they are discharged from the hospital, especially for patients with heart disease or cancer. The electronic medical record is extremely beneficial to both the patient and the treating physician. The electronic medical record (EMR) is an important type of healthcare data that is currently receiving a lot of attention. For clinical diagnosis and treatment, EMRs frequently contain highly sensitive private information. EMR sharing is thought to be a viable way for uplifting healthcare quality index, speeding biological discoveries, and reducing the associated expenditure (Jingwei, 2018). Private health information, electronic medical records, and electronic health records have all emerged as valuable assets with the ability to influence people's quality of life all around the world. Personal health information has already been acknowledged as an asset by the World Health Organization, with sharing going far beyond its main medical function (Amofa, 2018). (Jothia, 2015), (Zhang, 2015), (Yue, 2018). Medical data is dispersed throughout numerous medical institutions, and the data grading of various institutions is also bifurcated, ensuring a poor level of medical information system interoperability among agencies. Medical data breaching is an inescapable risk, and these records are constantly susceptible to data security, personal privacy breaches, and other challenges. These medical records require increased security and privacy to prevent leakage or misuse by a third party.

To allow medical data exchange between organizations, a secure data sharing infrastructure is required. Privacy, security, and compliance, on the other hand, are all concerns that must be addressed.

First, health data is extremely sensitive to privacy, especially since more data is accumulated in the public cloud, increasing the danger of data exposure.

Second, present systems are built on a centralised architecture that necessitates centralised trust. Furthermore, efficient health data integration and interoperability amongst healthcare systems remain a difficult issue.

Another challenge is that users have little control over their personal health data (Liang, 2017). Because the health industry is so reliant on information, constraints related to data handling, confidentiality, and protection are increasing at the same time. The term "health data privacy" refers to the robust security handling of patient information, as well as the requirement for authorization to access the information. Furthermore, security refers to the protection of sensitive information from hackers and even visitors (Omar, 2017).

Contemporary blockchain study covers health information confidentiality, healthcare information storage and retrieval, healthcare information implementation, forecast research, and emphasized forthcoming implications, goals, and prospects connected to blockchain technology in medicine. A blockchain-based healthcare data gateway has been developed (Yue, 2016). The paradigm enabled patients to not only possess, administer, and communicate their information in a simple and safe manner, but it also permitted unauthorized external parties to handle medical and health records while ensuring patient confidentiality through reliable multivariate regression processing. Enigma was designed to work in conjunction with blockchain technology to ensure a safe environment for collecting and retrieving patient records. Some blockchain-based strategies and systems have been developed for storing and maintaining patient data (Shrier, 2017). The immutability and built-in autonomy qualities of the blockchain were used to create a blockchain-based data sharing architecture that can address the access control difficulties associated with sensitive data stored in the cloud (Xia, 2017), (Peterson, 2016). Encryption is done and maintained on a consortium blockchain, and information consumers need to get the private keys from the data holder, according to a blockchain-based confidentiality health information framework (Omar, 2017). By encoding information and processing it on a based on blockchain server, the electronic health record portal design protects confidentiality. The health-care data gateway architecture was created to protect data privacy by encrypting it and storing it on a private blockchain cloud. A patient downloads and decrypts encrypted material before deciding whether or not to disclose it. When information is transported, it is re-encrypted, and the beneficiary receives the resulted in the formation and decoding passcode (Yue, 2016).

1.3.1. Challenges in Healthcare Records

- • Gathering, storing, and analysing personal healthcare data information without perturbing security is a major challenge for healthcare data systems. Privacy issues have proven to be a hurdle to adoption for such systems, and a lack of effective security measures has resulted in several data breaches, exposing patients to financial risks, mental agony, and possible social humiliation (Yue, 2016).
- The 95% of healthcare information stored in healthcare facilities, rendering it vulnerable to threats such as intentional manipulation, malware, and environmental catastrophes, which can also contribute to patient information leaks and damage. (Chen, 2019).
- Using the immutability and autonomous qualities of the Blockchain, a Blockchain-based data sharing system is presented for privacy protection and secure storage of medical data, but the methods connected with Blockchain introduce various issues, such as immutability and access control leaks (Hussein, 2018).
- An integrated healthcare database management system makes it challenging to ensure the authenticity of health data. Health information is routinely contained in a medical center's database in such a framework, where the adversary can destroy or modify the information after gaining the required access control. (Tian, 2019).

- To provide privacy protection in medical data utilising Blockchain, a Controllable Blockchain Data Management (CBDM) paradigm was developed. Although the Blockchain is regarded as a safe platform since all system participants' actions are recorded on the chain, the extending chain makes it computationally difficult to modify any block without being detected (Zhu, 2019).

1.4 Blockchain Architecture

The P2P network technology is used to create a blockchain network. A fragmented connectivity is a community network in which data is stored and transferred without the use of a central server. The network is less vulnerable to attack since there is no central point of storage for the information in blockchain. A distributed network is a network in which two or more nodes collaborate and produce the same result by sharing the same information. As a result, the distributed network's output will seem to all users as a single logical platform. The P2P network technology is used to create a blockchain network. A fragmented connectivity is a community network in which data is stored and transferred without the use of a central server. The network is less vulnerable to attack since there is no central point of storage for the information in blockchain. A distributed network is a network in which two or more nodes collaborate and produce the same result by sharing the same information. As a result, the distributed network's output will seem to all users as a single logical platform. “A distributed ledger is a ledger in which all transactions, information, and records are recorded from various nodes in multiple locations, and the data may be shared and synchronised across distributed networks, obviating the need for a central authority,” according to Wikipedia. All information and records are cryptographically protected, and only keys with cryptographic signatures can access them. With a distributed ledger, any changes made to the ledger or document are mirrored across all participating nodes in a matter of minutes or seconds, allowing all parties involved to verify their ledgers and use the new record. Because regularly updating and synchronising data across numerous centralised databases can be inefficient, putting the databases on a shared ledger would make it easier to access and view the updated database on demand when needed.

Each DLT is unique in terms of the data it uses and the technology it employs, all DLTs are based on three well-known technologies: public key cryptography, distributed ledger technology, and distributed ledger technology. (Thakkar, 2006).

1.4.1 Types of Blockchains

1.4.1.1 Public Blockchain

Because no permission is necessary to join a public blockchain network, it is also known as Permissionless Blockchain. A public blockchain is open to everyone, and anyone who wants to read and write to the network can do so. A public blockchain is a decentralised network that is not under the jurisdiction of a single authority. As demonstrated in fig. 1.1, once data is published on the blockchain, it cannot be changed. In a permissionless blockchain, no single user has the ability to change the blockchain's rules on their own. The users of the network confirm any information about the transaction based on a mutual consensus among the users of the blockchain. All blockchain users operate on a trust-based system, with each member of the public blockchain relying on one another to authenticate a transaction beforehand. Public Blockchains are primarily used in the creation of cryptocurrencies, such as Bitcoin and Ethereum, and are accessible to anybody with a computer and access to a high-speed internet connection.

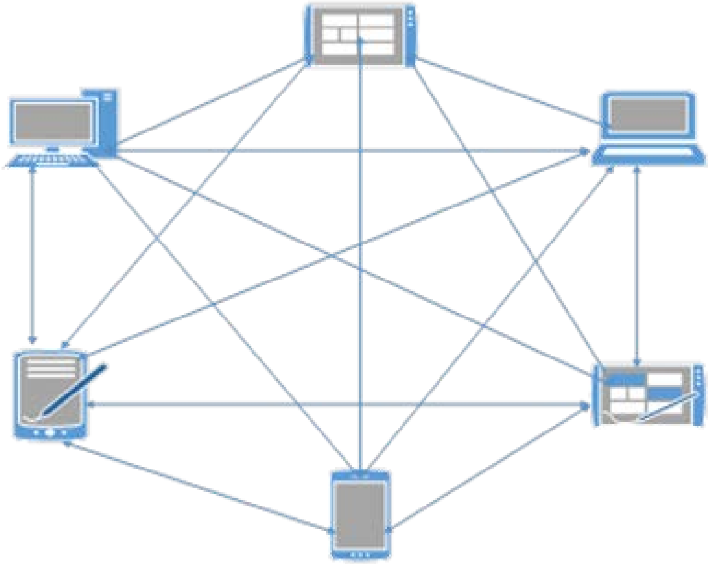


Figure 1.1 Public Blockchain

The 51 percent assault (Zhang, Xue, and Liu 2019) is a problem with the public blockchain that occurs when a group of more than 50% of the network's users verify an incorrect transaction. However, several research have concluded that this form of attack is unrealistic and requires a lot of money.

1.4.1.2 Private Blockchain

A public blockchain network, as contrary to a private blockchain, enables everyone to participate, read, and write to the chain only on permission basis. A private blockchain, as shown in Fig. 1.2, is a type of blockchain that is not open to the public and requires permission to join. A private or permissioned blockchain is the name given to this sort of blockchain.

In a private blockchain, users are not permitted to join the network at their leisure, nor are they permitted to view or issue transactions on their own. Companies, industries, and governments choose this sort of blockchain since only authorised individuals are allowed to enter and join the blockchain. Only these approved individuals can validate a transaction, issue a transaction, or even execute a smart contract transaction. In contrast to public blockchain, a private blockchain allows the organisation that runs it to simply change the rules of the blockchain, reverse transactions, and even change the balance. When the speed of the two blockchains is compared, private blockchains are faster than public blockchains because private blockchains have less hurdles with high trust levels and also for transaction verification (Dinh et al. 2017).

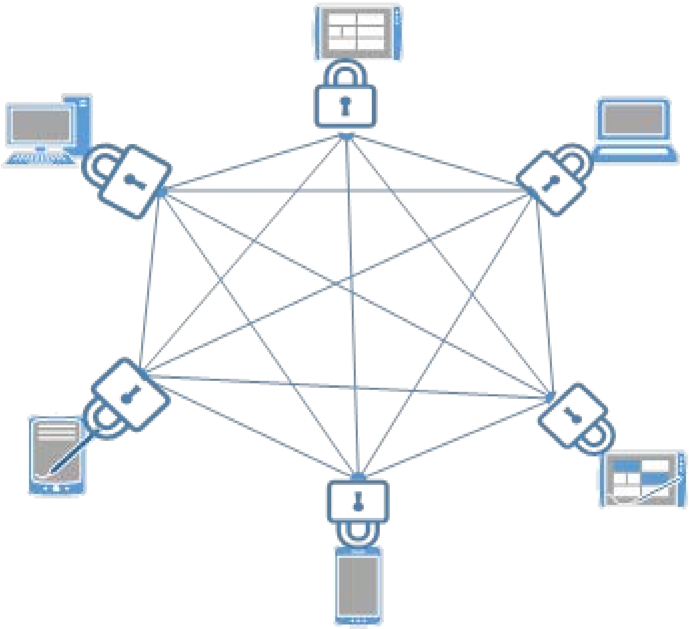


Figure 1.2 Private Blockchain

Private blockchains are utilised in a variety of industries, including banking, healthcare, government, and a variety of commercial sectors like as pharmaceuticals, agriculture, retail chain management, and other supply chain management, which we shall cover in more detail in future chapters.

1.4.1.3 Consortium Blockchain

The public and private blockchains are combined in a consortium blockchain. It allows users to add to the network without needing authorization just like a public blockchain, but unlike a private blockchain, the network's ownership does not pass to a single owner or company.

1.5 Structure of a Block

The containers are the blocks, which are linked together to constitute a chain. A blockchain is a collection of blocks that form a chain. The data is stored in a block connected to the chain. The information recorded could be in the form of a text, a number, a programme that can run, or, most crucially, a cryptocurrency transaction. Because blockchain is a distributed ledger technology, all blocks are spread across all machines linked to the network, making it impossible to change the content of any block. Each block generates a hash value of the transaction or data placed in the block, which is safeguarded by the Secure Hash Method-256 or SHA-256 strong hashing algorithm. For each transaction in the block, a hash value is created automatically. As a result, modifying the content of the block alters the associated hash value of the block, and since all subsequent blocks utilise the prior hash value, the previous hash value in all blocks is a miss-match, as illustrated in Figure #2, where the previous hash value is the one generated by Block#1. The block's structure includes elements such as Block Number, which indicates the number of blocks in the chain, Moment Stamp, which indicates the time the block was generated, and Transaction, which is the actual data, information, or any transaction value created by the user and placed in the block. The hash value created for the transaction made in the block. It's worth noting that the freshly formed block's current hash value will become the previous hash value for the next block created and added to the chain. Figure 1.3 shows the structure of a block.

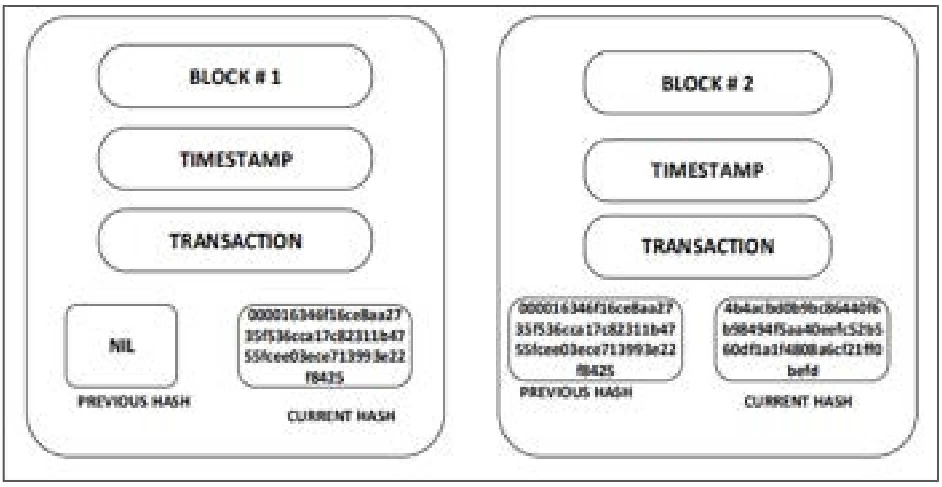


Figure.1.3 Structure of Block

Ralph Merkel patented the Merkel Tree, commonly known as the hash tree, in 1979. In the world of cryptography, a Merkel Tree, also known as a binary hash tree, is extremely valuable. Merkle Trees are data structures made up of cryptographic hash values. A Merkle tree is constructed by periodically hashing the pair of child nodes until only one hash value remains; this node at the top is known as the Merkel root.

The leaf node is located at the bottom of the Merkle tree. These leaf nodes contain data, which could be a file or any other valid piece of information. The values on the leaf nodes are not encrypted or hashed at first, therefore they aren't considered part of the Merkle tree. The data values are hashed using the SHA-256 technique, and the resulting hash value is placed on the Merkle tree's leaf node. The same procedure is followed, only this time the leaf node's child nodes are joined and hashed together to form a parent node. This process is repeated until only one node remains at the top of the tree, which is known as the Merkel Root Node. This type of security is now used in a blockchain network, where each transaction is secured with a hash value, and the hash value of each new transaction is derived from the previous transactions' hash value. As a result, if the data changes or is tampered with by an unauthorised entity, the root hash value will change. As a result, all parties involved in the blockchain network are informed about the modifications made. As a result, blockchain provides a more secure network for all businesses and industries.

The Merkle tree is built from the bottom up, as shown in fig. 1.4. TxD1, TxD2, TxD3, TxD4 are the four transactions depicted in the diagram. Although transactions are never saved on the Merkle tree, just the hash values of the data are kept on the leaf of the tree as HD1, HD2, HD3, HD4 when the data is hashed.

The mathematical function for deriving the hash value of D1 can be seen as

HD1= SHA256(SHA256(TxD1))

Each transaction is hashed twice with the SHA 256 method in the same way. By concatenating and hashing the two hashes together, the sequential pair of nodes is merged into a parent node. The process goes higher until we reach Merkel Root Node, a single node at the very top of the tree.

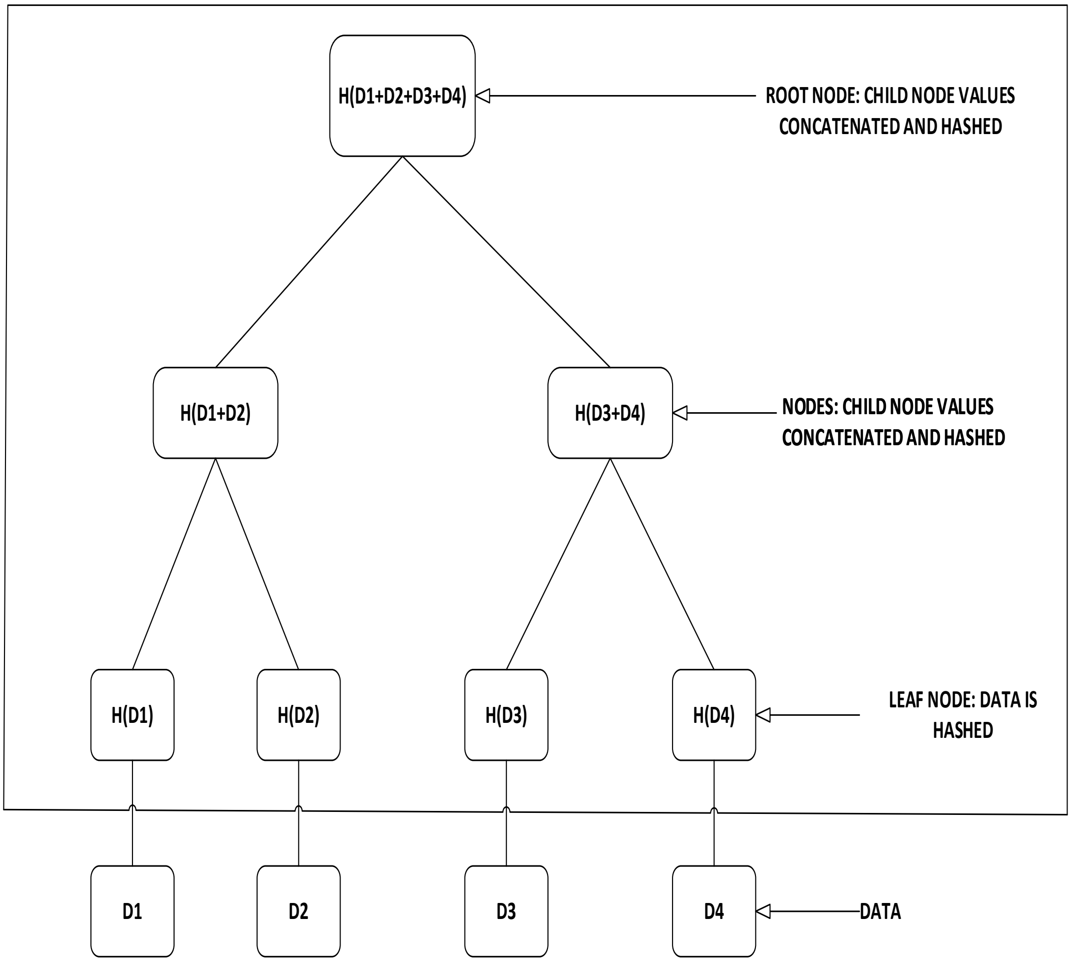

H(D1+D2+D3+D4)
ROOT NODE: CHILD NODE VALUES CONCATENATED AND HASHED
H(D1+D2)
H(D3+D4)
NODES: CHILD NODE VALUES CONCATENATED AND HASHED
H(D1)
H(D2)
H(D3)
H(D4)
LEAF NODE: DATA IS HASHED
D1
D2
D3
D4
DATA

Figure 1.4 Markel Tree

1.5.1 Blockchain Process

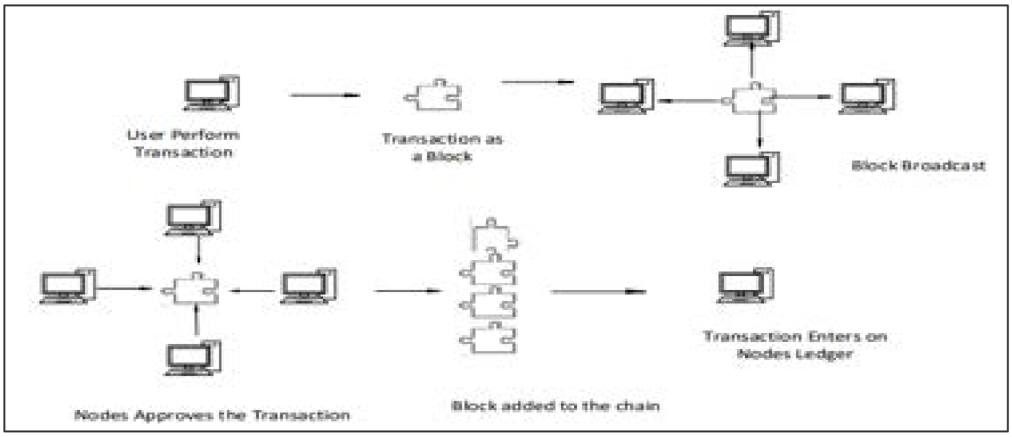


Figure 1.5 Blockchain Process

As shown in Fig. 1.5, a blockchain procedure is dependent on a consensus mechanism for a transaction to be validated and genuine. A blockchain network is made up of a number of nodes that are connected in a dispersed and decentralised manner. A transaction must be written in a block by any node that needs to complete one. A block can be conceived of as a container-like data structure that can hold up to 1MB of data and contain roughly 500 transactions on average (Marr, 2018). The node executes a transaction in a block, which is then forwarded to other nodes in a distributed network. Because the blockchain network is decentralised, the block of transactions made by one node is broadcasted to all other nodes in the network. The blockchain network is a consensus-based network, which means that all nodes must agree on a transaction based on a consensus algorithm. A consensus algorithm is a method for numerous nodes in a distributed network to reach an agreement on a decision (Xia, 2017). As illustrated in the diagram, after a block is checked and validated by all nodes in the network, it is added to the chain of blocks already existent in the blockchain. The freshly added block will always refer to the chain's prior block, making the chain more secure. The receiving node can now update the ledger with the additional information after the block is added to the chain of blocks. Blockchain technology is one of the most fascinating and secure technologies in the last decade, falling under the category of Distributed Ledger Technology (Rouse, 2017). As previously said, blockchain is based on a layered approach, and we have examined the block chain levels and how they work here.

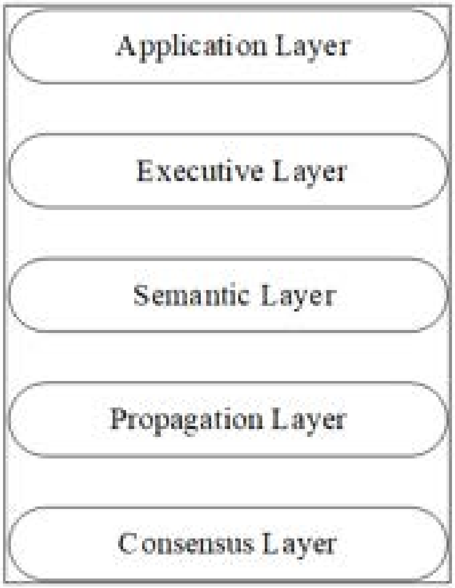


Figure 1.6 Blockchain Layers

Application Layer- As we all know, blockchain technology is tamper-proof, decentralised, and shared ledger technology. As a result, numerous applications can be developed on the blockchain's properties. The application layer, which is built into some apps, can also interface with the other layers, therefore it is on top of this layer suit. The application layer is where a user can programme the needed functionality and create the application for the application's users. Due to the fact that blockchain is a decentralised technology, the application must be loaded on each node. Although there are some cases when blockchain is used in the backend and applications must be hosted on a web server and require server side programming, it is preferable if no server is engaged in the blockchain network because this would negate the purpose and benefit of the technology.

Execution Layer- This layer is in charge of executing all of the instructions issued by the application layer for all nodes on the blockchain network. The collection of instructions could be anything from simple to complex. Smart contracts, for example, are short pieces of code that must be executed when funds must be transferred from one person to another. As a result, if one request exists on each node in the blcokchain network, the application will run without interruption from the other nodes. To eliminate inconsistencies in the result, code execution on a set of inputs should always give the same output for all of the nodes on the blockchain.

Semantic Layer- The logical layer of the blockchain layer suit is also known as the semantic layer. Validation of all transactions completed in the blockchain network, as well as validation of blocks generated in the network, takes place at this layer. Different types of instructions are completed on the execution layer when a transaction is run on a node, and all of these instructions are validated on the logical or semantic layer. The semnatic layer is similarly concerned with the connection of the network's blocks. Since the hash of the preceding block is included in every block in the blockchain (except the gensis block). As a result, block linking has to be defined on this layer.

Propagation Layer- A Propagation Layer is responsible for peer-to-peer communications between nodes, allowing them to discover and sync with other nodes in the network. A transaction is broadcast to all other nodes in the network when it is completed. Furthermore, when a node proposes a block, it is instantaneously broadcast across the whole network, allowing other nodes to use and operate on the freshly generated block. As a result, the propagation of a block or a transaction in the network is defined at this layer, which ensures the network's overall stability.

Consensus Layer - This layer serves as the foundation for most blockchain systems. The primary goal of this layer is for all nodes to agree on a common state for the shared ledger. The layer also looks after the blockchain's safety and security. There are a variety of consensus algorithms that can be used to generate cryptocurrencies such as bitcoin and ethereum. These algorithms use a Proof-of-Work method to choose a node at random from the network's nodes that can propose a new block. Once a new block is formed, it is propagated to all other nodes to see if it is valid with the transactions it contains, and if it is, the new block is added to the blockchain based on the consensus of all other nodes.

1.6. Privacy Preserving Methods in Blockchains

Cryptography techniques improve the security of blockchain technology and ensure the privacy of data stored on it. Cryptography has two primary goals: the first is security, which prohibits unwanted access to data, and the second is authenticity and integrity, which protects data from change. We have private and public keys, hashing algorithms, digital signatures, and other tools that could help the blockchain network succeed.

1.6.1 Security

Blockchain technology employs encryption and hashing techniques to ensure that the data saved is unchangeable. Although blockchain technology offers higher security than other existing technologies since it is a decentralised technology that does not require a single authority to control the network while preserving trust between the network's nodes, it is less secure than other existing technologies. With the usage of blockchain technology, there has been an advance in securely storing and exchanging information with other nodes utilising encryption techniques, giving the user complete control over the information (Taylor, 2019). Data security is particularly important when the data is either a transaction or electronic medical data. Any patient's electronic medical record is sensitive and confidential information, and a security breach could result in the information being disclosed to any unauthorised person. As a result, this information must be protected from manipulation and unauthorised access. Digital signatures or hashing algorithms are examples of approaches that can be used to secure data in a network.
Data security is particularly important when the data is either a transaction or electronic medical data. Any patient's electronic medical record is sensitive and confidential information, and a security breach could result in the information being disclosed to any unauthorised person. As a result, this information must be protected from manipulation and unauthorised access. Digital signatures or hashing algorithms are examples of approaches that can be used to secure data in a network.

1.6.2 Hashing

When a huge document is run through a hash function, the result is a fixed length output in hexadecimal format. The hash value created for the document is this fixed length output. A hash function is a mathematical function that breaks down material into smaller digests. The information could be secured using the hash value created by the hash function. Any input value's hash value will always be different and can never be the same value. Any modifications to the input value will result in a change in the hash value. The user will then notice that the original input value has been altered. The cryptographic hash function has grown in popularity in the realm of security and privacy since the advent of cryptography. Other technologies are proved to be less secure than hashing approaches. The following is the author's definition of a hash function: A function HF ()

that generates an MD message digest of a fixed length from any arbitrary length message. If M satisfies the following characteristics, it is considered a One-Way Hash Function (Zhu, 2019):

- The Function HF () should be publicly known and there should be no secret information associated with the operation of this function.
- For the given message M, it should be easy to calculate HF(M).
- With the given Message Digest MD, it would be difficult to find the message M such that HF(M)= MD, with given HF () and M, it would be difficult to extract a message M`≠M such that HF(M`) = HF(M).

For safeguarding information, hash functions such as SHA0(1993), SHA1(1995), SHA2(2001), SHA3(2014), and the most recent SHA256[XIII] have been developed. Secure Hash Algorithms encrypt data using a one-of-a-kind hash function and generate a fixed-length output based on the input value. The Microsoft Enhanced RSA and AES Cryptographic Provider supports SHA256, the most modern and widely used approach in blockchain technology (One-way Hash Function, n.d.). Almost all blockchain networks utilise the SHA-256 cryptographic method, which gives an output of 32 bytes represented by 64 hexadecimal characters. This means that SHA256 has a total of 2256 1077 potential digest results. SHA-256 is believed to be the most collision resistant of all the SHA algorithms since, on average, the method must be running 2128 times to identify a collision, making it extremely difficult for a hacker to break (Yaga, 2018). As a result, SHA256 is employed in blockchain technology, making it more secure and providing greater privacy than any other technology. For example, we utilised a website called https://www.fileformat.info to calculate the hash value. We passed the function a text value as input, and the function returned the following hash value:

Original Text: Hello, how are you, I have high cholesterol value.

SHA256Value:

1fa6e4f59486f72e3e504cfca9981416297213541967c2c4682791e161106be0

Modified Text: Hello, how are you, I have low cholesterol value.

SHA256Value:

26bccd725246b89cbdd74cca64014ed399ccf0c24011068ab89a9eabf4dcef5b

Small changes to the document's hash value could affect the entire hash value. This demonstrates how crucial the hash algorithm is for data security and privacy.

1.6.3 Privacy

Data is the new money in this era of big data. Every second, any e-commerce or social media site generates a massive amount of data. Users of these websites provide complete information without realising that it could be leaked at any time. According to a Forbes study, about 1.5 billion people are active on Facebook every day, 5 new users join every second, and around 300 million people share photos in a single day (Marr, 2018). Other digital and electronic records are maintained on the cloud and in an organization's database, such as medical records, transactions, supply chain information, and data created by IoT devices. The confidentiality of this private information must be maintained in order to prevent it from being leaked and misused. To ensure that security and privacy are not jeopardised, the user should have the authority to own and control their personal information. Zyskind et al. have created a framework that stores data on an offline blockchain. The user has access to information regarding data gathering and how it will be utilised in an offline blockchain (Zyskind, 2015). The blockchain can identify the data's authenticated user, ensuring the security and privacy of the user's personal information. Blockchain can help to protect and support healthcare.

When a patient attends various healthcare organisations, such as a hospital or a doctor's office, there are several key issues that develop. Whenever a patient visits a doctor, he or she must keep track of all documents and medical reports. When a patient is unable to track down his medical history or essential paperwork, the circumstance causes him anguish. Due to the unavailability of a previously completed test, patients may be need to repeat part of the tests. Healthcare data is considered to be the most sensitive data a person may have, and the process of maintaining it is much more difficult. There are still no systems in place to protect the privacy of electronic medical records. The most significant limitation in managing electronic medical records is that the system must be developed only on a permissioned blockchain network, which allows the identities of nodes to be known to other nodes in the network, allowing malicious behaviour to be detected, which would not be possible in a permissionless network. A framework for secure and trustworthy electronic medical record sharing has been proposed by Dubovitskaya et al (Dubovitskaya, 2017). The system was constructed on a permissioned network that allowed the doctor and patient to share a secure network. A membership service is used by the framework to register the various network users. The patient may be able to create a symmetric key (SKAES P) that can be used to encrypt and decrypt data. To share data with the doctor, the patient could exchange the symmetric key with the associated clinician's encryption public key (PKED), making the data sharing trustworthy and secure.

1.7 Objectives

The purpose of this research is to create and implement a block chain-based technology for privacy protection in the health-care industry, using block chain data as an input. The blockchain technology will assure data security, provide control over sensitive data, and make healthcare data supervision easier for patients and other medical players. In their decentralised smart grid energy trading method, blockchain can be utilised to ease secure data management or to improve the security level in a specific application. Following that, we went over the Blockchain architecture and terminology that had previously been utilised in relation to blockchain and medical health data. We've covered the research's broad goal here, and the methods will be covered in detail in the next chapters.

1.7.1 Objective 1: Security and Privacy of Electronic Health Record in a Decentralized Storage

Previously, health records had to be kept in print or on paper. The patient's reports were collected on paper, and the patients were required to keep these paper records in a file or record book. The procedure of storing health records was inconvenient since it was difficult to retain all records pertaining to diagnosis, treatment, and prescription drugs in one location for an extended period of time. Records can be misplaced or torn at any time. Another issue with paper records was that if they were kept in one location, they might not be available in another. As a result, there was a need for a system that could assist in keeping the data safe, in one location for years, and accessible at any time and from anywhere. Electronic Health Records (EHRs) were a way for a patient, a doctor, or a hospital to preserve a computerised record of their medical history. These digital documents can be stored for many years in one location and accessed at any time and from any location. The security and privacy of these digital records are key concerns, as there is a risk of patient data being leaked and misused. Another major issue is the collapse of the centralised system that stores health-care information. As a result, our key goal is to create a method or technology that can store health records in one location for decentralised access while maintaining the security and privacy of Electronic Health

Records. Chapter 2 explains the literature review and applications. In chapter 3, many applications of Blockchain in e-voting and transportation systems are discussed.

1.7.2 Objective 2: Privacy Preservation of Electronic Health Record in a Private Blockchain Using Hyperledger Platform

EHRs, or electronic health records, are a patient's basic health information, such as medical diagnoses, treatments, and medications. These medical records can be stored on a network, so a network where these medical records can be safely maintained with a high level of security and privacy is required. The blockchain technology ensures that the data saved on the blockchain is secure and private to the appropriate level. A blockchain is based on the concept of a decentralised network, which eliminates the possibility of a centralised node failing or data being tampered with A blockchain is a network of connected blocks, each of which is secured by a hash value, providing security and anonymity to the data recorded in the block. A public blockchain and a private blockchain are the two most common types of blockchain. Our plan is to build a private blockchain with three nodes/participants: patients, clinicians, and laboratories. The blockchain's owner creates the IDs for all three participants and has the ability to give and revoke access to the chain's participants. All medical records are saved and accessible from a single location at any time and from anywhere with this type of chain. The goal is to establish a system that uses blockchain technology to integrate EHRs and make them more secure and private on a Permissioned or Private Blockchain. We'll use the Hyperledger Fabric and Composer platforms for this, which aid in the building of a private blockchain. As a result, our primary goal is to ensure the confidentiality and privacy of patient medical data/records by storing them on a private blockchain. In chapters 3 and 4, the entire process is detailed.

1.7.3 Objective 3: Preserving the Privacy of Electronic Medical Records in Blockchain Network Using Tensor Product and a Hybrid Swarm Intelligence

Electronic Medical Records (EMR) were used to store a patient's medical records in one location so that they could be accessed by the user at any time. These digital medical records eliminate the need for patients to transport their records from one doctor to the next or from one facility to another. However, the security and privacy issues associated with the storing and sharing of electronic medical records were the main source of worry. However, while cloud storage is an option, there are still significant security and privacy issues with data saved in the cloud. Concerns were also raised about the sharing of patient medical records with physicians or doctors. Although research has been done on the security and privacy of electronic medical records, there are still some advantages and disadvantages to such techniques. Our goal is to come up with a methodology or procedure that will improve the security and privacy of electronic medical records. To strengthen the confidentiality and privacy of the record, we will begin by acquiring health data as input into a blockchain network, then applying the tensor product method and swam intelligent. For better optimization, the tensor product operation changes the original data into protected data, while the swam intelligence will use dragonfly (DA) and crow search algorithm (CSA). Maximum accuracy and minimal information loss will be used to evaluate the performance. The entire procedure is detailed in Chapter 5. The conclusion and future direction of the thesis are found in Chapter 6.

1.8 Conclusion

In this chapter, the fundamentals of blockchain are introduced. The chapter also discussed about different types of blockchains and how the process of blockchain works with nodes connected in the blockchain network and how the data stored on the blockchain network are secured and protected as discussed in the Merkel Tree. The objectives discussed in the chapter mentions the work to be done for preserving the privacy of the electronic health records.

CHAPTER 2

LITERATURE REVIEW

A blockchain is a technology that is decentralised, immutable, and resistant to tampering. After Satoshi Nakamoto suggested the notion of cryptocurrencies in the year 2008, blockchain technology was born. Blockchain technology was created to support the Bitcoin cryptocurrency. However, as time went on, the IT community realised that technology might be useful in a wide range of other fields. At the moment, the market capitalization of the popular cryptocurrency Bitcoin is estimated to be around $150 billion (Pilkington, 2016; Buterin, 2014). Since then, blockchain technology has advanced in leaps and bounds, and it is now being employed in a wide range of industries due to its numerous benefits. With the introduction of blockchain technology, many firms are benefiting from increased security and privacy. A blockchain technology ensures the data's integrity and redundancy, as well as the fact that once it's saved in the blockchain, it can't be changed or modified from its original state.

The healthcare industry is one area where blockchain technology can be extremely beneficial. Every minute and every day, the healthcare business generates vast amounts of data in the form of patient laboratory tests, X-rays, MRI, CT-scans, financial documents, past prescriptions supplied, previous medical history, and most recent appointments with physicians. All of this information is personal information that is stored as electronic data. As a result, robust security and privacy are required to prevent data loss and exploitation by unauthorised individuals. Electronic medical records are digital copies of a person's medical records that can be saved on any device. Electronic medical records are beneficial to patients because they eliminate the need for the patient to carry different paperwork from one doctor to another and from one hospital to another. Health records can be accessed in real time from any location and remain with the person at all times. However, with the evolution of electronic medical information, there are various risks and liabilities associated with it, particularly in terms of data privacy and inaccurate information (Nakamoto, 2008). As a result, blockchain technology has the capability of maintaining a patient's medical records.

2.1 Search and Selection Process

Since 2000, the search has been a manual search of journal papers and specialised conference proceedings. IEEE, ACM digital library, Springer, Elsevier, ScienceDirect, IGI Global, Taylor & Francis, IOS Press, Hindawi, and MDPI were among the online databases searched. Blockchain, Blockchain with privacy preservation, blockchain on electronic medical health records, and blockchain with swarm intelligence were the topics of various scholars' research. Additional inclusion criteria include research containing terms like "blockchain," "Internet of Things," "privacy preservation," "electronic health record," "heart illnesses," "dragonfly algorithm," "crow-search algorithm," and "swarm intelligence." The literature study did not include any research that used additional descriptors. The poll was conducted between the years 2000 and 2020. Approximately 300 papers were initially chosen. They were then whittled down to 125 by using descriptive keywords. The final 100 publications in this work were chosen from a database of 125 research papers based on full text readability and relevance to our research aims. In fig.2.1, the criteria for selecting research papers are diagrammatically depicted.

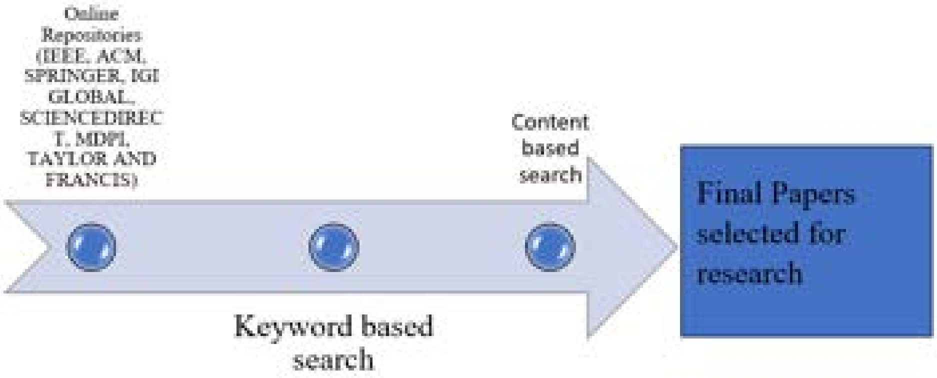

Online Repositories (IEEE, ACM, SPRINGER, IGI GLOBAL, SCIENCEDIRECT, MDPI, TAYLOR AND FRANCIS)
Content based search
Final Papers selected for research
Keyword based search

Figure 2.1 Paper Selection and Review Process

2.2 Related Work on Block Chain

The blockchain is unquestionably a brilliant invention (Nakamoto, 2008). Blockchain technology was created to support the Bitcoin cryptocurrency. However, as time went on, the IT community realised that technology might be useful in a wide range of other fields. To use the blockchain, a person does not need to understand how the internet works. However, only a basic understanding of this new technology is required to determine why it is deemed an innovative technology.

2.2.1 Blockchain Overview

Blockchain is a method of storing and exchanging data in a decentralised, transparent, and tamper-proof manner. The data on a blockchain network is stored in a shared and always-submissive database. The blockchain database is not maintained in a centralised location, which means that the database's entries are public and can be easily verified by millions of computers at the same time. Anyone with access to the internet can view its data. The concept of blockchain technology is based solely on distributed ledger technology, in which each node on the network stores a copy of the ledger (Kessler, 2003). Furthermore, the blockchain network follows a consensus, which means that every 10 minutes, the network checks for itself. A blockchain is made up of multiple nodes connected in a network. Every node in the blockchain has a full copy of the ledger and voluntarily joins the network. In technical terms, blockchain is a data structure for developing chains with a unique ability to resist tampering with a decentralised e-ledger, or in other words, it is a complicated technology that is used to implement forgery-resistant chains with a decentralised e-ledger (Liu, 2018;Amofa, 2018). Blockchain transactions, like those of traditional database systems, cannot be modified, erased, or introduced on the fly (Jothi, 2015). The goal of developing a decentralised chained data structure like this was to create a transaction system with its own currency that could store information about past transactions. The term "blockchain" has become popular in both industry and academics (Zhang, 2017; Yue, 2016). The intrinsic value of cryptographic transactions is derived from their capacity to preserve genuine values internationally and without regard to jurisdiction (Liang, 2017). The security of a blockchain system is managed by security standards, which ensure that users' sensitive data is protected. The whole point of blockchain is to have safe and decentralised transactions.

Block

The blockchain is a series of blocks, as the name suggests, and these blocks form the foundation of the technology.

A Block's Structure

The following specific meta information is included in each block:

Data in Blocks: The information to be saved is in encrypted format in the block, as well as the information about certified and permitted transactions tallied, is referred to as Block Data.

The Block Header itself is made up of the following elements:

Number of Blocks: The index of the block in the chain is easily recognised as the Block Number. It's critical not to mix the block number with the block's unique identity. The size of the blockchain is directly proportional to the block number (Omar, 2017).

Previous Hash is the previous hash.

Current Hash: The generated output of a cryptographic hashing function that encrypts the input values to a certain length is called Current Hash. The block's index, data, previous hash, timestamp, and nonce value are typically provided as input to the hashing process.

Timestamp: A timestamp is a reference to the time when a block was created.

The block's size (optional): The block's size refers to the amount of memory it has for storing prior transactions.

The nonce value is an acronym for "number only used once," and it is sometimes referred to as a measure of difficulty. The nonce is the value that blockchain miners seek. The nonce value is hashed in the block, and when it is rehashed, it becomes the nonce value.

The expected digital signature, i.e. the prior hash, is guaranteed by the authenticity and validity of the block. A block that has not been validated or authenticated will not be added to the chain.

LEDGER is a blockchain-based digital journal that is shared among all users. It keeps track of all transactions on the blockchain network in question.

A blockchain transaction can't be changed after it's been recorded. The public keys of the users participating in the transaction make up the ledger record of the transaction. A user exchanges sensitive information with another user throughout the transaction. The concept and philosophy of distributed ledger ownership are promoted by blockchain technology (Ackerman, 2016; Xia, 2017). Simply said, blockchain technology is nothing more than a reliable and secure application of distributed e-ledger technology.

2.2.2. Consensus Algorithms

A distributed ledger is what a blockchain is. Consider a scenario in which there are five mining nodes. Each node will have a copy of the blockchain, and all of the copies will be identical, meaning that all of the nodes will have exact copies. After completing some transactions, this network now obtains a new block. The blockchain must be updated to include this new block. But which mining node will be responsible for adding this block to the blockchain? (WEI SHE, 2019). The difficulty here is how to decide whether or not to add a new node. As a result, all of the nodes agree on whether or not to add the new block to the blockchain. As a result, the consensus process is defined as the process through which a collection of nodes reaches a choice and all individual nodes agree on and support the decision that provides the best answer (Anwar, 2018). Consensus Algorithms are a collection of algorithms that are used in the consensus process.

2.2.2.1 Types of Consensus Algorithms

There are a variety of consensus algorithms, is divided into following categories: Proof Based and BFT Based.

In the Proof-Based consensus technique, the network's leader is chosen at random from among several other nodes and proposes the final value. Permissionless algorithms are another name for this algorithm (Baliga, 2017). In BFT-based (Byzantine Fault Tolerance), the network's leader is chosen by many rounds of voting among the network's nodes (Wang, 2018). This form of consensus method is also called as Permissioned Consensus Mechanism or Consortium.

2.2.2.2 Proof of Work

The basic concept was first suggested in 1993 to combat spam emails, and it was formally dubbed "proof of work" (Dwork, 2001) in 1997. However, until Satoshi Nakamoto launched Bitcoin in 2009, the technique was generally ignored. He discovered that this process might be used to reach consensus, therefore he utilised it to protect the Bitcoin Blockchain. The proof of work algorithm, on the other hand, requires all nodes to solve a cryptographic challenge (Li, 2017).

A Proof of Work technique is essentially a way for someone to effectively demonstrate to you that they have put in significant computing work. Proof of work protocols are frequently compared to puzzles, and these puzzles can be quite difficult to solve, implying that substantial computational effort is required and there are no shortcuts (Szalachowski, 2019). On the other hand, that effort can be easily confirmed in a fraction of the time it took to carry it out in the first place. POW is used in a variety of applications, with Bitcoin being one among them. The proof of work can be implemented in any timestamp network by incrementing the nonce values (Chepurnoy, 2017). In cryptography, a Nonce is a field in the block that is usually an arbitrary or random number that is intended to guard against reply attacks. The nonce's value should be unique for each block and can only be used once. The nonce value is appended to the end of whatever is being hashed. As a result, if someone tries to repeat the same notes, they will fail because each note must be unique. This means that if the user tries to do something and has already used that note, the session is over. When mining Bitcoin with proof of work, it will prompt you for the answer to a puzzle.

The research's goal is to use Blockchain to create a privacy solution for health-care documents. We covered the detailed application of Blockchain in the fields of e-voting and transportation technology in Chapter 3. However, we have explained health care analytics and the need for Blockchain technology in the health care domain, as well as a literature analysis on privacy control in the health care sector utilising block technology, in this chapter.

2.2.3 Bitcoin or Blockchain

It's easy to get mixed up about what blockchain and bitcoin are and how they're related. When we think of bitcoin, we think of illegal money or a technique to make money without breaking the law. Similar to how a car runs on the technology of moving tyres, bitcoin is a car, and blockchain are the tyres that allow bitcoin to drive (Hulburt, 2014). In order to avoid this, having a central authority between two users that functions as a middleman for transaction typically costs consumers transaction fees. In 2009, bitcoin was launched, which was not real money but rather a virtual or digital currency with some value. Nakamoto et al., 2008. We can consider blockchain to be an operating system, and bitcoin to be an implementation of blockchain technology.

2.2.4 Workflow of Bitcoin

The bitcoin network is currently processing thousands of orders of transactions at the same instant, and all have exposure to the decentralized public record. Every one of the amateurs are engaged on secure authentication and are prepared to insert it into the database, but it's unclear which event will be uploaded immediately. A competition is used to overcome this. Each minor must answer a computationally challenging math problem, and that transaction will be added to the list of transactions that must be completed by any minor or end user as soon as possible (nodes). The incentives people receive for fixing these difficulties and maintaining the blockchain are the reason they are interested in doing so. Minors who get their entries included to the ledger are paid with bitcoins, which keeps them motivated (Macdonald, 2017). With the growth of blockchain technology, new blockchain platforms are being developed, and current ones are being upgraded to include new functionality. Table 2.1 gives the Comparative study of different platforms in Blockchain.

Table 2.1 gives the Comparative study of different platforms in Blockchain.

Platform	Ethereum	Hyperledger	R3 corda	Stellar	Multichain
Features					
Operation mode	Public	Consortium	Private	private	Private
Year of starting	2015	2015	2014	2014	2015
Aim	Become global decentralised supercomputer	Platform for enterprises to create their own permissioned blockchain	Developing an enterprise-grade distributed ledger platform for business across a variety of industries	Develop software for everyone to work on a single network for all financial transaction systems.	designed to make sure about transfer and custody of digital assets.
Governance	Ethereum Developers	Linux Foundation	R3	Steller development foundation	Open Source
Currency	Ether (ETH) Cryptocurrency	No native Cryptocurrency but can be made	No native cryptocurrency	Lumens (XLM)	Native currency

		using chain code			
Consensus	Proof of work, proof of state (Ethash)	PBFT (Practical Byzantine Fault tolerance)	Notary nodes can run several consensus algorithm	FBA (Federated byzantine agreement)	Proof of Work
Project	https://ethereum.org/	https://www.hyperledger.org	https://www.corda.net	http://stellar.org	https://www.multichain.com
Smart contracts	yes	yes	yes	No, but combine transactions with various constraints	Smart filter
Development language	Golang + Python	Golang + Java	Kotlin + Java	Metron	C++/JavaScript
Hash function	Keccak256	SHA3 SHAKE256	SHA-256	SHA-256	SHA3-256
Stateless/stateful	stateful	stateful	stateful	stateful	stateless
Secondary storage	Level DB, Rocks DB	Rocks DB	H2Database	Rocks DB	Level DB
In memory ds	Trie	Merkle Tree	Merkle Tree	Stellar tree	Merkle Tree
Transactions per second	7-12	20000+	15-1678	3000+	500-1000

Purpose	B2C (Business to Customer)	B2B (Business to Business)	B2B	B2B	B2B
Availability of Api access	Yes	No	Yes	Yes	Yes
Availability of sdk	Yes	Yes	Yes	Yes	Yes
Smart contracts implementation	Solidity	Chain code	Kotlin	Multiple SDK available	JavaScript
Scalability	No	No	Yes	Yes	No
Privacy feature	No	Yes	Yes	Yes	Yes
Trust model	Untrusted	Semi trusted	Trusted	semi trusted	Trusted

With so many various technologies and functionalities, it's important to pick the right platform for a certain application. These platforms give any company the freedom to experiment with various technologies to meet their own needs.

First, we went over the health-care data, previous work, and numerous problems in extracting and analysing electronic health data. We've also provided a brief explanation of these terms. Following that, we went into privacy protection strategies in the health-care industry.

2.3 Healthcare Industry

Healthcare is becoming increasingly complicated. The data generated by healthcare is so complicated that maintaining and processing it would be impossible. Hospitals and other medical institutions generate a tremendous volume of data, making it difficult to identify what is needed. The healthcare analysis is beneficial not only to patients, but also to hospitals that care for them prior to and after their hospitalisation. Electronic medical records (EMR), pathology labs, immunisation programmes, and other surveys in medical camps are all places where a lot of healthcare data can be collected. The healthcare sector is expanding every day and proving to be a thriving sector in any country's economy (Yang, 2015). A clinical data warehouse compiles all of a patient's data into a single, well-organized location that may be utilised for analysis and reporting. This is done through a procedure called extraction convert and load, which gets data from several clinical systems and synchronises the formats (see Figure 2.2). The data is cleaned up and then entered into the clinical data warehouse's database through a process known as transformation. The adaptation procedure is extremely noteworthy since information might be maintained in a number of forms throughout platforms. For patient identity male/female or unidentified, a science lab network might use the characters M, F, or you, while a diagnostic management system sometimes use zero, two, or nine alternatively. They must, however, match the clinical data warehouse's designations, and the process of transforming them to match is known as transformation (Zheng, 2017). Another crucial step is to guarantee that all of a patient's records from different systems are linked. To integrate a patient's multiple identifiers across systems, a master patient index, also known as a master person index, is often required (Dennis, 2015). A bottom sensor layer, a middle network layer, and a top application layer can be crudely sketched out as the architecture. The process of analytics in the healthcare industry is depicted in Figure 2.2.

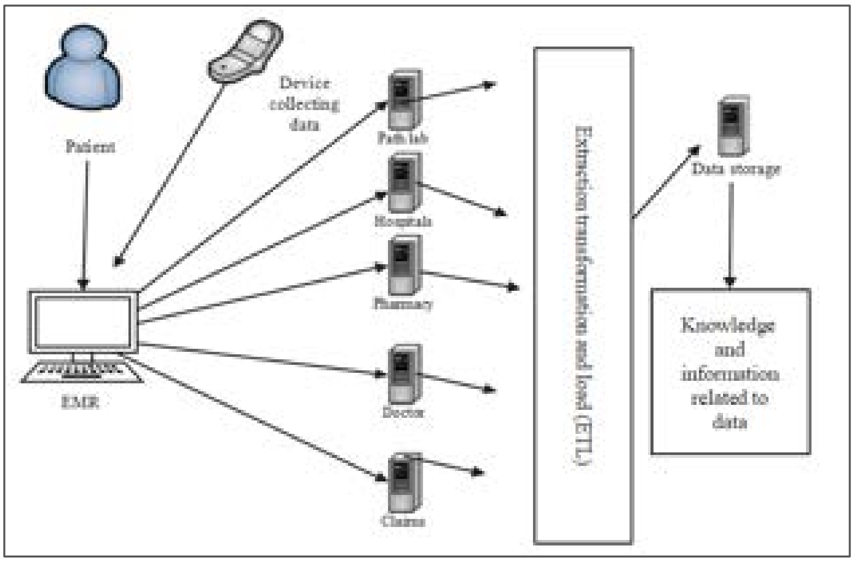

Patient
Device collecting data
Path lab
Hospitals
Pharmacy
Doctor
Claims
EMR
Extraction transformation and load (ETL)
Data storage
Knowledge and information related to data

Figure 2.2 ETL Process in Healthcare Industry

The concept "analytics" is being used in many different situations and with many different interpretations. “Analytics has become a sneak up term for a variety of data analytics (BI) and implementation projects.,” according to Gartner. According to the National Institute of Science and Technology (NIST), analytics is defined as the discovery of meaningful patterns in a given set of data. As one of the next phases, statistical analysis is included. “Analytics can also be utilised in referring to the methods used, their implementation tools, and the outputs of the tools as understood by the practitioner,” according to the NIST. The integration of material into knowledge is the analytics activity. IBM divided analytics into 2 categories in 2013 (Ivanov, 2018):

1.Predictive: In order to address the research, "Whatever might occur?" it employs predictive methods as well as predictions.

2.Prescriptive: It asks, "What should we do?" using optimization and simulation.

A series of steps is involved in data analytics:

- Identify the issue.
- Determine what data is required and where it can be found.
- Create an analysis plan as well as a retrieval plan.
- Take the data and extract it.
- Clean up the data and get it ready for analysis.
- Analyze and understand the information.
- Create a visual representation of the data.
- Disseminate fresh information.
- Incorporate the knowledge into the company.

The first stage would be to characterise the problem to be examined, or to identify the business case in business words. The question now is, why is it vital to study this? What impact will the outcome have on patient care or the institution? As a result, the user must have a clearly articulated problem or inquiry in order for the rest of the procedure to be guided. There must be a method for determining how many records are expected and then retrieving them. Cross-checking with other systems may be necessary. This phase necessitates the participation of the person who regularly retrieves data from the systems in question. An analytical plan should be devised, and a statistician should be engaged, with issues such as what is the population, what sample size is required, and what statistical test should be used.

Mistakes in the data should always be detected as well as repaired when a complete set of records has been extracted from the operational databases, and all chosen data has errors such as inverted symbols and characters, as well as erroneous numbers. It's up to you to decide how to handle empty fields. The next step is to synchronise and convert the data. For example, in one hospital system, patients' gender may be maintained as M, F, or U, whereas in another system, 1, 2, or 9 may be used. To ensure that all records use the same values, one set of values must be modified. After the appropriate transformation stages are finished, the data is imported into the destination system, where it will be analysed and reported on. The data should be confirmed that everything is ready for the analysis and that we have everything we need. This should be compared to the analysis plan that was created and that we have everything we need to solve the problem that was discovered.

We're now ready to do the actual study and carry out the analysis strategy that we devised previously. The system will now be able to communicate the analysis' findings and how they relate to the problem. This communication must be highly clear and quickly understood by the institution's decision-makers. As a result, choosing a suitable representation for your discovery is critical. Choose a representation that is appropriate for the data type; for example, categorical data can be represented using column or bar charts, tables, and pivot tables, whereas quantitative data can be represented using histograms or a range of other graphics such as dispersed plots and Star plots. Tableau and the chart function in Microsoft Excel are two popular tools. A report must be written after the analysis, interpretation, and visualisations have been completed. The initial problem must be stated explicitly in the report. The procedure was utilised to handle the issue, followed by the analysis' outcome and accompanying visualisation. This is new information that has to be shared with the stakeholders that were identified.

Information obtained in the healthcare business includes laboratory test results, imaging tests such as X-rays and CT scans, financial information, prior prescription individual patient, prior health background, and perhaps most recent consultations. When numerous patients are treated at the same hospital or healthcare facility, all of these data add up to a massive amount of information. Big data analytics has resulted in considerable improvements in patient health, as well as a reduction in the cost of medical expenses paid during patient treatment and the development of a strong relationship with the healthcare provider (Wang, 2020; Raghupathi, 2014). Based on the patient's medical history, big data analytics can provide a better solution for hospitals and other healthcare staff (Pramanik, 2018). As a result, healthcare providers could provide better care before the patient's condition deteriorates (Bokas, 2018). As a result, we now understand the importance of data analytics in delivering future insight. Despite the use and display of healthcare data analytics, more than half of healthcare providers are unsure how much and what kind of data is required to create useful insights from their data. In order for healthcare organisations to successfully show and use big data analytics, they will need to look for other metrics and focus on its application; thus, only one organisation will need to win executive backing for a unique programme. Bioinformatics is becoming more significant in healthcare as the use of big data analytics widens the link between consumers and physicians, which is further characterised by the collecting and filtering of statistical data (Wang, 2014). The use of big data in healthcare allows healthcare practitioners to establish trust with their patients, allowing them to change the quality of treatment they provide (Sarkar, 2017). The term "transparency" can be defined by healthcare professionals, which could alter physician culture.

The Internet of Things is changing our way of life, from how we react to how we act. From air conditioners that can be operated with a user's smart phone to smart autos that can provide the shortest routes to smart watches that can track a person's daily activity. The Internet of Things (IoT) is a massive network of interconnected gadgets (Srinivasan, 2019). These gadgets collect and communicate information on how they're utilised and the environment they're in (Atlam, 2020). Sensors, which are incorporated in every physical equipment, be it a mobile phone or any electrical appliance, bar code sensors, traffic lights, and practically anything else that might be encountered in a day's work, are responsible for all of this. These sensors emit data regarding the devices' current state of operation on a continuous basis. The concern may arise as to how the sensors might exchange such a large amount of data and how the data could be used for good. It also allows them to speak with one another using a common language. Data is supplied to the IoT platform security from a variety of sources. The Sap cloud platform collects material out of a variety of sources, evaluates it, and retrieves pertinent information as required (Gubbi, 2013).

In healthcare, IoT is employed with wearable devices that may be connected to the patient and help record the patient's health patterns. The usage of IoT devices makes remote monitoring of the patient considerably easier (Gomez, 2016). This implies that the patient and the doctors are in contact with one another at all times of the day. The patient's hospitalisation has been shortened, and re-admissions have been avoided, thanks to the patient's remote monitoring. As a result, the Internet of Things has made a tremendous impact in lowering costs while increasing patient treatment outcomes. We'll now look at how IoT devices might benefit patients, physicians, hospitals, and insurance companies.

2.4 Cryptography in Blockchain

Blockchain technology is one of the most secure technologies in recent decades, according to Distributed Ledger Technology (Rouse, 2017). Cryptography techniques improve the security of blockchain technology and ensure the privacy of data stored on it. Cryptography has two primary goals: the first is security, which prohibits unwanted access to data, and the second is authenticity and integrity, which protects data from change. Confidentiality, Integrity, Authentication, and Non-Repudiation are the four most important aspects of any network (Wang, 2019). Cryptography can have private and public keys, hashing algorithms, digital signatures, and other tools that could help the blockchain network succeed. Data security is particularly important when the data is either a transaction or electronic medical data. Any patient's electronic medical record is sensitive and confidential information, and a security breach could result in the information being disclosed to any unauthorised person. As a result, this information must be protected from manipulation and unauthorised access. Digital signatures or hashing algorithms are examples of approaches that can be used to secure data in a network. The document, which is digitally signed in the public domain and remains in a documented state, is secured by the digital signature. Hashing techniques, on the other hand, establish a secret value of the data, known as the hash value, for any given data, making it immutable and thereby preserving the data from change while keeping the information's authenticity and integrity. The present systems are built on a centralised architecture that necessitates centralised trust. Furthermore, efficient health data integration and interoperability amongst healthcare systems remain a difficult issue. Another issue is that consumers have very limited control over their personal health information (Liang, 2017). Because the healthcare business is so reliant on data, challenges related to data processing, privacy, and security are increasing at the same time. The term "health data privacy" refers to the secure and private processing of patient data, as well as the requirement for authorization to access the data. Furthermore, security refers to the protection of sensitive information from intruders and even listeners (Omar, 2017). The Blockchain technique will ensure data security, control over sensitive data, and facilitate healthcare data supervision for patients as well as different actors in the medical field by providing the required tool to establish consensus among spread entities without relying on a single reliable party (Hussein, 2018). In their decentralised smart grid energy trading method, blockchain can be utilised to ease secure data management or to improve the security level in a specific application. It can also be used to improve the security of trading data. These approaches, in particular, employ a number of Blockchain-based mechanisms to preserve anonymity in multi-signature, anonymous message encryption, anonymous negotiable energy trade, and other applications. The blockchain is used to manage content distribution (Zhu, 2016).

Confidentiality of patient records, handling and transportation of medical information, health information applications and prediction assessment, and highlighted prospective influences, aims, and potentials related to blockchain technologies in healthcare are all covered in existing blockchain research. A blockchain-based Healthcare Data Gateway was developed. By adopting private multivariate regression computing, the platform not only let individuals to efficiently and securely control, manage, and distribute their information, but it also enabled unauthorized service providers to handle clinical and health data while respecting patient confidentiality (Yue, 2016). Numerous block chain technology techniques and programs have been designed for organizing and retrieving clinical information (Ackerman, 2016). The bitcoin protocol preservation and inherent liberty were leveraged to develop a blockchain-based resource sharing design that addresses the network access effects identified with critical material kept in the internet (Xia, 2017). Employing consortium blockchain architecture and a blockchain-based technique for exchanging health information, a multilateral specific healthcare prognosis model was constructed (Peterson, 2016). The health-care data gateway architecture was created to protect data privacy by encrypting it and storing it. A user can easily download and decrypts encrypted material before deciding whether or not to disclose it. Whenever information is transported, it is re-encrypted, and the destination receives the ciphertext and decryption key (Yue, 2016). Table 2.2 lists various proposed methods with its advantages and disadvantages.

Table 2.2 lists various proposed methods with its advantages and disadvantages.

Authors	Methods	Advantages	Disadvantages
Yue, X *et al.*	Healthcare Data Gateway (HDG) architecture.	Enable patient to own, control and share their own data	Privacy-aware data access policies cannot be easily achieved by traditional access control models and needs complex computations.

		easily and securely without violating privacy.	
Chen, Y *et al.*	Storage scheme and service framework based on the Blockchain.	Make it a potential solution for healthcare data systems that concerns both sharing and patient privacy.	Did not consider a medical Blockchain network to connect several medical and health institutions.
Al Omar *et al.*	Patient centric healthcare data management system	Encrypt patient's data to ensure pseudonymity and helps to attain privacy with less cost.	Unable to handle key-theft/loss mechanisms or key distribution techniques.
Hussein, A.F *et al.*	Blockchain-based data sharing system	System is robust, efficient, immune and scalable offers dependable data privacy.	Processing time may increase.
Daghera, G.G *et al.*	Blockchain-based framework named Ancile	Cost and storage effective.	Did not meet legislative standards for medical data and protection of patient privacy.
Zhang, A. and Lin, X	Blockchain-based secure and privacy-preserving PHI sharing	Time cost increases slowly with the growth of the package length.	Can meet the security goals.

	(BSPP) scheme		
Tian, H *et al.*	Sibling Intractable Function Families (SIFF)	Guarantee the privacy, availability and integrity of medical data.	Communication cost increases linearly.
Zhu, L *et al.*	Controllable Blockchain Data Management (CBDM) model	Allows one to terminate any malicious actions under any type of attack.	Unable to process on real-world environment.

2.5 Related Work on Swarm Intelligence.

Many swarm intelligence-based algorithms have been developed and are now being used to solve a variety of complex computational challenges. Ant Colony optimization, particle swarm optimization, firefly algorithm, cuckoo search algorithm, dragonfly search algorithm, and crow search algorithm are among the different algorithms. The work done with the dragonfly and crow search algorithms has been reviewed.

2.5.1. Dragonfly Algorithm

Hamdy et al. employed the multi-objective version, as well as six evolutionary approaches, to address the design problem of a zero-energy building (Hamdy, 2016). It was proposed to use a hybrid Dragonfly algorithm (Salam, 2016). Another solution to the economic load dispatch problem was proposed by Pathania et al (Pathania, 2016). The location of the unknown wifi nodes, which are randomly put in the given region, was estimated (Daely, 2016). A multi-class SVM classifier was offered as another unique approach (Elhariri, 2016). The firing angle and size of the thyristor-controlled series capacitor were tuned by Hema Sekhar et al (Shekar, 2016). The multilevel segmentation problem was solved using the self-adaptive Dragonfly Algorithm (Sambandam, 2016). DA was also used in the realm of software engineering (Mafarja, 2017). The most important test cases that satisfy all requirements were chosen using DA as an optimization tool (Sugave, 2017). Suresh and Sreejith reduced the cost of production for all units in a solar thermal system (Suresh, 2017). To handle numerical optimization difficulties, a memory-based Hybrid Dragonfly Algorithm was presented (Ks, 2017). With a quasi-triangular cut-out, Jafari and Chaleshtari improved the orthotropic infinite plates (Jafari, 2017). Hariharan and colleagues suggested a method for resolving infant scream classification problems (Hariharan, 2018). Kumar et al. combined the Dragonfly method with cluster cloud models in their research (kumar, 2018).

2.5.2 Crow Search Algorithm

Kim et al. evaluate the effectiveness and efficiency of ‘electronic medical record data cubes. For effective large data analysis, data cubes are used. To ensure data privacy, an electronic medical record data cube privacy-preserving system was designed. The process of anonymization was also discussed in order to protect people's privacy (Kim, 2017). To overcome a few difficulties, Wang et al. presented a privacy-preserving structure. Two protocols were created for the preservation structure. Experiments were carried out on real-world datasets, with the results demonstrating that the created techniques are more usable for huge datasets (Wang, 2015). Adaptable progressing ways might be adopted based on various data priorities to send user health data to servers with reasonable communication costs (Zhang, 2014). The proposed method learns the data distribution more precisely and transfers the acquired healthcare knowledge, protecting the patient's privacy. They've also uncovered important biomarkers (both universal and region-specific) using a built model, as well as biomedical literature has approved the chosen biomarkers (Li, 2016). In digital rights management systems, The validity and confidentiality of the fundamental demands for a person's illness diagnosis were proposed by Huang et al (Huang, 2011). Poulis et al. developed a novel technique for encrypting statistics that guarantees identity disclosure, data redundancy, and information secrecy, and ensures that the data remains anonymous. The effectiveness and competency of the created algorithm were evaluated using a large dataset containing over 200,000 "electronic health records" (Poulis, 2017). A utility-preserving anonymization model has been presented by Lee et al. It is to save the data for as long as it is useful (Lee, 2017). Gao et al. introduced a new reversible data concealment approach, which is especially useful for medical imaging. The test assessed the developed algorithm's predominance of ROI contrast enhancement, as well as visual quality and tamper detection (Gao, 2017).

2.5.3 The Challenges Confronted by Conventional Methodologies are Illustrated Below:

- Health-care systems necessitate an efficient technique for collecting, storing, and determining healthcare data while remaining compliant with privacy regulations. These types of systems do not include some fundamental security precautions, which has led in multiple data breaches, exposing patients to financial risks, social stigma, and mental stress issues.
- Several types of medical data are collected and maintained in a centralised manner in clinical institutions, and they are vulnerable to a variety of risks, including malicious attacks, hacking, and natural catastrophes, all of which can result in the loss of medical data. Blockchain-based data sharing in the system has been presented to secure data privacy by using the immutability and autonomy of the block chain [9]. However, block chain-based systems face some issues, such as access control breaches and immutability.
- The integrity-based medical data is not analysed by systems based on centralised data management. The information about the patients is maintained in a medical repository in these systems, where a hacker can access the database and remove or edit the data.
- Controllable block chain data management (CBDM) model has been developed in order to provide the privacy protection in the clinical-based data by the block chain methods, which is considered a secure platform since all actions are recorded in the chain, which are made by system participants and then expanding the block chains to modify without analysing the blocks makes it computationally effective and challenging.

2.6 Conclusion

The blockchain network is extremely beneficial in all aspects of healthcare. It is adopting blockchain technology to ensure the confidentiality and privacy of patient records. The amount of data generated in the healthcare sector today is enormous, and while we have the technology to store it, the security and privacy requirements for such data are insufficient, particularly when it comes to a patient's Electronic Medical Record (EMR). These types of documents are personal to each patient, and no patient wants his or her personal information exposed or misused by others. Concerns about the privacy of the records have been investigated. This survey on preserving the privacy of the Electronic Medical Data using Blockchain Technology revealed that while some researchers have provided solid techniques to safeguard and preserve a patient's medical record, there are still some issues associated with some of these methods. In the future, we intend to work on a more robust technique to protect the privacy of patient medical records by utilising blockchain technology.

CHAPTER 3

VARIOUS APPLICATIONS OF BLOCKCHAIN BUSINESS MODELS

The evolution of cryptocurrencies Many companies and organisations have discovered how blockchain technology works in practise. It was a period when blockchain technology advanced and was adopted into a wide range of applications in industries including as healthcare, banking and finance, supply chain, insurance, manufacturing, and other critical industries. The absence of third-party engagement is the most significant benefit that blockchain provides to the sector (Ganne, 2018). We covered the fundamentals of Blockchain and its many approaches in the previous two chapters. When blockchain technology is employed for purposes other than bitcoin, it will experience a significant increase in popularity in the near future. Technology is used in a variety of fields, including education, healthcare, and increasing the quality of commercial processes. Many various firms are concerned about the design, execution, monitoring, and improvement of business processes, and many different companies are employing multiple systems to support the process execution. Customers and other business partners rely on a business company's mutual trust. As a result, blockchain creates an environment in which inter-organizational processes may function and execute in a trustworthy manner, as you no longer have to trust anyone but the data on the blockchain. The blockchain network can provide end-to-end product traceability, as well as real-time auditing via timestamps and digital signatures (Litke, Anagnostopoulos, and Varvarigou 2019). We explored the Consortium Blockchain and its applications in several domains such as e-voting and transportation systems in this chapter.

3.1 Introduction

3.1.1 Blockchain: Adding Value to a Business Process

The blockchain network can provide end-to-end product traceability, as well as real-time auditing via timestamps and digital signatures (Litke et. al, 2019). Smart contracts, which are a component of blockchain technology, can be used to conduct transactions that are critical to a business process and are transparent to other blockchain network members. On a blockchain, smart contracts are little pieces of code or programmes. When certain circumstances are met, smart contracts are automatically executed. As a result, smart contracts can be utilised as an agreement between users of the blockchain network for transaction verification without the involvement of a third party, with rules that cannot be changed or amended once made, allowing business parties to collaborate in a transparent manner.

A business can benefit from blockchain by tracing back the items or products that are being traded (Mendling et al. 2018). We understand how frustrating it might be if the item we're working with goes missing or becomes untraceable. Thus, blockchain enters the picture, where the whole information of the item, including the exact date and time of item delivered or received, is recorded on the blockchain, and there is no way to restore the data if it is destroyed. However, every business must exercise caution when deciding whether or not to invest in blockchain technology, as it is not guaranteed that every business will benefit from a blockchain network in terms of design and process improvement, and any unorganised or disorganised structure implemented on blockchain may result in strategic failures (Bertrand Copigneaux 2020). As a result, businesses must first evaluate which aspects of their business or applications should be incorporated into blockchain. As a result, we may conclude that, from a business standpoint, the appropriate technique at the right time can yield the greatest benefit in a business process.

3.1.2 Consortium Blockchain

As a semi-private blockchain, a consortium blockchain can be considered. Members of the blockchain are connected in a permissioned environment in a private blockchain. A single corporation or industry owns a private blockchain, which is more specifically described as a centralised system with powerful cryptography mechanisms connected. A consortium blockchain provides the same benefits as a private blockchain, but the ownership is not controlled by a single corporation or individual; rather, it works under the direction of a group (Li et al. 2018).

3.1.3 Smart Contract

When it comes to transactions between the parties involved in the blockchain network, one of the essential aspects of blockchain is termed a smart contract, a notion introduced by Szabo in 1997. (Szabo 1997). A smart contract is a computer programme that runs automatically and is enforced when a transaction between two parties is completed, acting as an agreement between the parties. Whether the parties agree or not is up to them, but using a smart contract will definitely eliminate the need for a third party. A smart contract is a set of self-executing and self-verifiable codes written in Solidity or Python and embedded in the blockchain network. Because the smart contract is built on the blockchain, it will be immutable, which means that once the code is written on the blockchain, it cannot be changed or amended. In a blockchain network, smart contracts give a high level of security.

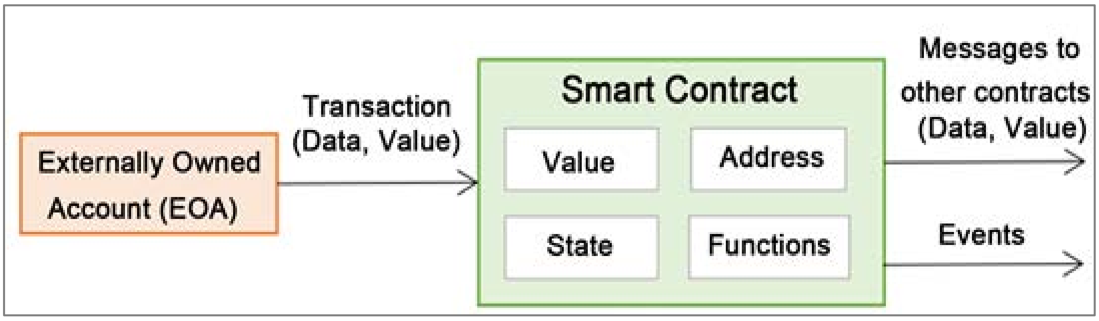

Externally Owned Account (EOA)
Transaction (Data, Value)
Smart Contract
Value
Address
State
Functions
Messages to other contracts (Data, Value)
Events

Figure 3.1 Basic Structure of Smart Contract (Bahga and Madisetti 2016)

A smart contract's structure is shown in Figure 3.1, which includes a value, address, state, and functions. When a smart contract is provided an input, the smart contract's related function is executed, and a preset output is produced. A smart contract can be employed in the bidding process (Chen, Chen, and Lin 2018), with the address field containing the address of the auctioneer and the current winner, the state field containing the current auction time, and the value field containing the current bidding value.

Now that we've seen how a smart contract works, consider the following scenario: three parties are connected in a blockchain network for the purpose of paying rent to the owner. As a result, all parties have agreed to a smart contract-based rent arrangement. This smart contract will now be activated by software or a computer, with some requirements in terms of days, time, and the amount of money that must be triggered, which may be after a month or a year. The smart contract's condition can be activated by a unique address, and once triggered, the money will be sent straight to the house's owner as rent. Similarly, smart contracts can be used to move vital papers from one party to another without the participation of a third party.

3.2 Electronic Voting using Blockchain

Voting is one of the most significant activities in any democratic country because it allows citizens to exercise their power by voting and electing their representatives. The citizen's right to vote can be protected by casting a ballot. Conducting free and fair elections is a fundamental requirement for any government. Every vote counts in whatever form of election, hence the country's electoral commission works hard to ensure a fair election throughout the country. It has also been observed that many adult people do not vote for a variety of reasons. Sometimes citizens enjoy their vacation and stay at home, or they believe the polling station is too far away, or they live outside of their voting city. Some may choose not to attend because they believe their vote will be ignored as a result of the unjust election results. One of the reasons citizens do not vote is because of long lines.

In the current system, it has been observed that traditional paper ballot voting is still employed in various nations. The premise of a paper ballot system is pretty simple: a person signs his or her vote on a piece of paper and places it in the ballot box. After the election, the votes are tabulated, and the winner is whoever receives the most votes. The possibility of fraud in this kind of voting, as someone may mix up the correct and incorrect voting papers, potentially changing the election outcome (every vote counts). As a result, there is a need for a system to replace the traditional voting system that can reduce fraud, making the entire election process as well as the vote counting process more transparent and ensuring that the country gets the deserving candidate.

Furthermore, the technology established must make voting easy and convenient for voters. The approach that bears the smallest cost for conducting elections uses a large quantity of money. A mechanism that allows people to vote while travelling should be devised. We are now in the digital world, and most people choose to live online. Ordering restaurants, booking cabs, shopping for daily supplies, and even meeting life mates online are all things that people like to do online. So, with a few taps or clicks on a screen, a person might cast his votes and select representatives with their profiles visible Voters should be able to vote online while continuing to conduct their daily work at home. Despite the fact that various online voting systems have been presented in the past, none of them have been implemented. There may be a number of obstacles that an online e-voting or remote voting system must overcome (Dahlberg 2018). Let us start with the challenges: there is a need for stringent security measures to be done in order to conduct remote electronic voting for the voting process (Rubin 2002). Because the risk of large-scale manipulation is simply too great in this scenario. There is a chance that the server or machine will be hacked, which will have a direct impact on the voting process and lead to incorrect election results (Bannet et al. 2004). There's a potential that a big number of people will be pushed or influenced to vote (Haynes 2014). There is currently no method to check if your vote was counted in this online voting system. Blockchain technology is the one technology that will undoubtedly be used to create such a system that is essential for the election's demanding process (Shah, Kanchwala, and Mi 2016). Blockchain technology can aid in the development of an electronic voting system that is immutable, transparent, and safe while maintaining the system's privacy. The information recorded about the voting process cannot be hacked into to change the results. In order to conduct fair elections, a blockchain-based voting mechanism could be more effective than existing distant e-voting systems (Curran 2018).

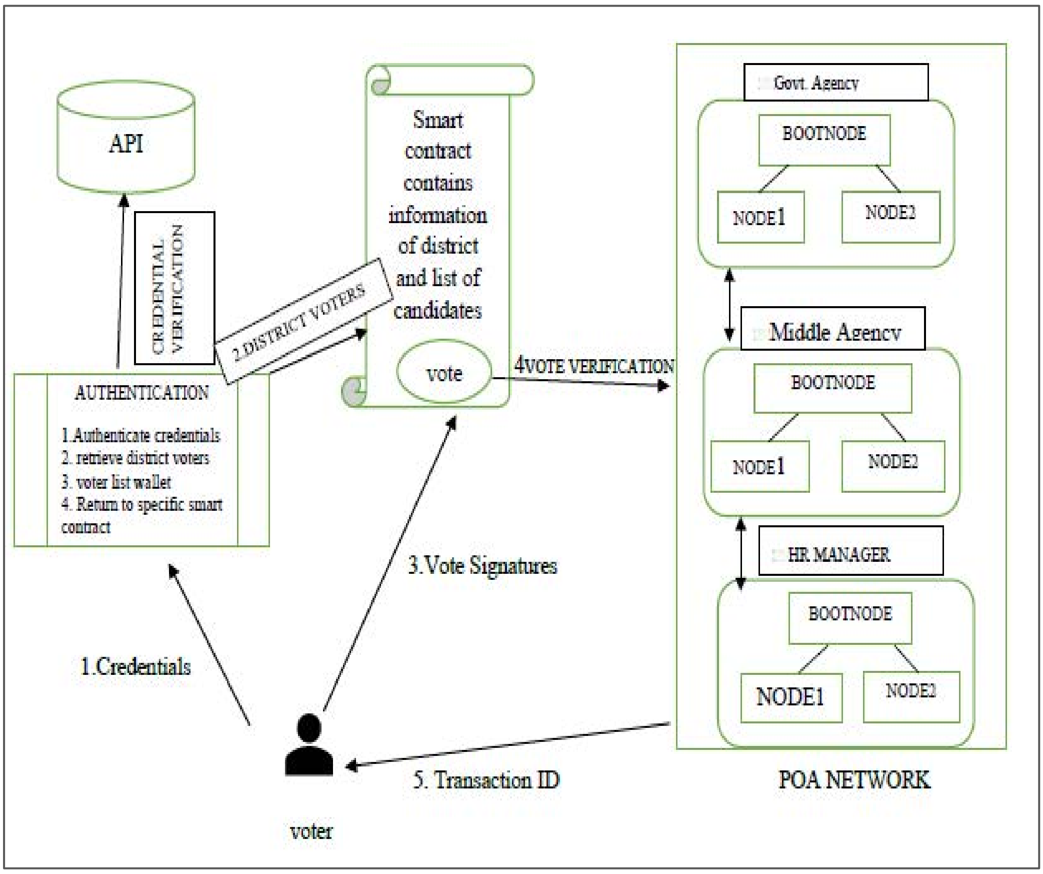


Figure 3.2 Voting authentication and vote casting process (Hjalmarsson et al. 2018) (Bulut et al. 2019)

first phase in this blockchain-based voting system is the authentication procedure, which verifies the voter's identity (Hjalmarsson et al. 2018) (Bulut et al. 2019), as shown in fig. 3.2. This step was taken to ensure that the actual individual was casting the vote and that no bogus users were present, as each vote counts in the voting process and has an impact on the election outcome. To avoid this risk, the user must install a simple application on his or her phone, laptop, or other device. After that, the user must provide documents that will identify him and authenticate the voting process after it has been verified by the organisation or government body that is administering the election. The documents uploaded by the voter prior to the voting process are compared to the list of voters in the organization's database to determine whether or not the person is registered and eligible to vote. Following that, all of the voter's information is securely added to the blockchain. Once the voter's identification has been confirmed, a smart contract in the form of a voting box can be issued to the voter. This smart contract-based ballot box allows voters to vote and submit their ballots.

This type of blockchain-based voting system will ensure that a user votes only once and not multiple times. When a voter votes under a blockchain-based voting system, polling stations will check the voter's blockchain to ensure that the voter has not already cast his vote (Zou et al. 2017). If the user's vote is genuine, the polling station accepts it; however, if the vote is discovered to be invalid, the polling station rejects it. As a result, blockchain will aid in avoiding duplicate votes made by a single voter. After the voting process is completed, all of the votes are combined into a transaction, which is then encrypted and stored in the blockchain. Because of the immutable nature of blockchain, once a vote is cast and a transaction is created, it will be impossible to change or modify the transaction. The voter, on the other hand, will have the option of printing a receipt confirming that he has cast his vote. The voter would be able to check whether his vote was cast and counted in the counting process using blockchain technology. Because blockchain is a distributed technology, this feature of blockchain will assist voters in auditing ballot boxes, confirming the correctness of election results without intruding on other voters' privacy. Furthermore, if we use the usual voting method, there is a potential that there will be some human error in the counting process, which will have an impact on the outcome. However, with blockchain, election results can be announced instantly after voting is completed, eliminating the possibility of human error. Since the ledger is updated with the results, all blockchain voters will receive notification of the election results on their devices. The user will be able to login and vote from anywhere thanks to Blockchain technology (Yu et al. 2018). A phone and an active internet connection would be the only requirements. This would inspire more people to vote and participate in the electoral process from all over the world, because everyone's opinion matters. This technique ensures that important votes are not squandered and that the best candidate wins. When compared to the existing manner of holding elections, the blockchain-based approach would undoubtedly be less expensive. Blockchain technology is slowly but gradually being utilised for secure voting in various nations and jurisdictions. In 2018, West Virginia and Sierra Leone, for example, experimented with blockchain-based mobile voting. This type of blockchain-based voting system could be particularly effective in voting processes in private corporations, organisations, and college elections, in addition to state elections. This type of secure voting system might also be employed in reality shows such as talent hunt shows, where the viewers' votes matter the most. In his report, (Andrew Barnes, n.d.) discusses the three forms of authentication processes in relation to the voting process and the method of voting. The voter's identity number (e.g., Indian citizens have their Aadhaar Number or Voter ID number), the password provided at registration, and their ballot card with a QR code are the different values discussed. Because there are two ways to vote, one through a web portal and the other by physically travelling to a polling location. Though a user's authentication information could be entered in a variety of ways. However, in order to vote for someone, all three pieces of information must be provided. Each polling place will have its own URL that voters will use to access the website where they will be able to cast their vote. This URL will be printed on the ballot card as well. (Bulut et al. 2019) presented a levelled voting method. This system is divided into several layers. Because of the large number of ballot boxes scattered around the country and the distance between voting centres, if the country is designed as a single blockchain, the system's synchronisation will damage its performance. If a single blockchain is developed for the entire country, the distance factor will cause some slowness in the system. In order to reduce the system's latency. From the lowest to the highest level, the system is separated into a chain of levels.

At the most basic level, the chain will be made up of nodes, which can be machines or voting centres where voters will cast their votes. At the second lowest level, there will be a cluster of chains that will store data from one level below. Communication between layers is ensured by the use of communication protocols. This form of communication should be done at regular intervals to avoid a temporal delay in the level synchronisation.

In order to reduce transaction clashes, the level in this system can be increased dependent on the population or voters.

3.3 Smart and Collaborative Transportation

The world is rapidly changing, with cities expanding and urban populations rising. The demand for goods and people transportation is growing, but so are traffic congestion, pollution, road accidents, and climate change. Today, we require increased mobility, but in a more intelligent manner. Electric cars, for example, are charged at the same time as products are loaded. We need dedicated bus lanes where drivers can enter and lead the connected convoy out onto the highway. Connected autonomous cars offer flexible, safe, and modular vehicle convoys that react to changing transportation demands It will be a mobile consolidation centre that can respond to timetables, update the flexible convoy, and switch commodities along the road. A connected vehicle, integrated cloud platform, personnel, logistics partners, and infrastructure all contribute to smart transportation (Wang and Li 2016). Sensors in self-driving vehicles in the smart city can deny truck, perceive movements in the environment, and react promptly and automatically to any odd events, such as accidents, ensuring passenger safety and preventing accidents. In city transportation, bus platooning enhances efficiency and capacity. Public transportation becomes more efficient and brings people closer together with emission-free and silent cars. This opens up new possibilities for smart city planning. In less than a minute, you may charge from the electric grid in a quick and effective manner. Autonomous vehicles, electric vehicles with zero emissions, low noise vehicles, and integration of technology such as blockchain, internet of things, and cloud computing technologies can be used to develop tomorrow's cities and infrastructure in a sustainable manner.

Smart transportation is one of the strategies to create a smart city that can improve people's lives while also increasing sustainability. It entails the following: 1. Information system: This system collects data on traffic, modes of transportation, and automobiles. These technologies aid in making public transportation more efficient and accessible, as well as maximising the use of private automobiles.

2. Smart city technologies: These include new and enhanced modes of transportation, such as mobile apps, connected autos, and more.

The following are the components of smart transportation:

1. Vehicles that are connected.

2. Maas (Mobility as a service).

3. Automatic Teller Machines (Advanced Traffic Management system).

3.3.1 Connected Vehicles

Modern vehicles are now equipped with IoT (Internet of Things) technology that allows them to communicate with other traffic management systems. This is referred to as V2I (vehicle to infrastructure) (Ubiergo and Jin 2016). These vehicles transmit information about their surroundings, such as roads, traffic rerouting, and so forth. They may also communicate with other vehicles, sharing data like as speed, location, and direction.

3.3.2 MaaS

It combines the functionality like payments, planning and booking. It provides single It integrates features such as payments, planning, and booking. It provides a single user interface for many modes of transportation. Passengers can choose from a variety of services that can assist them in getting to their location with ease, quickness, and at a lower cost. It has the potential to improve the quality and accessibility of public transportation.

3.3.3 ATMS

This is a smart city traffic management system that uses data from street lights, smart roadways, toll booths, and traffic lights. This system manages traffic lights, adjusts toll costs, and sends traffic data to other control centres. It aids in the provision of real-time traffic information to drivers, as well as the optimization of traffic flow and congestion reduction. Contactless fare payment, shared car systems, smart parking, autonomous vehicles, and on-demand service are some of the aspects of smart transportation.

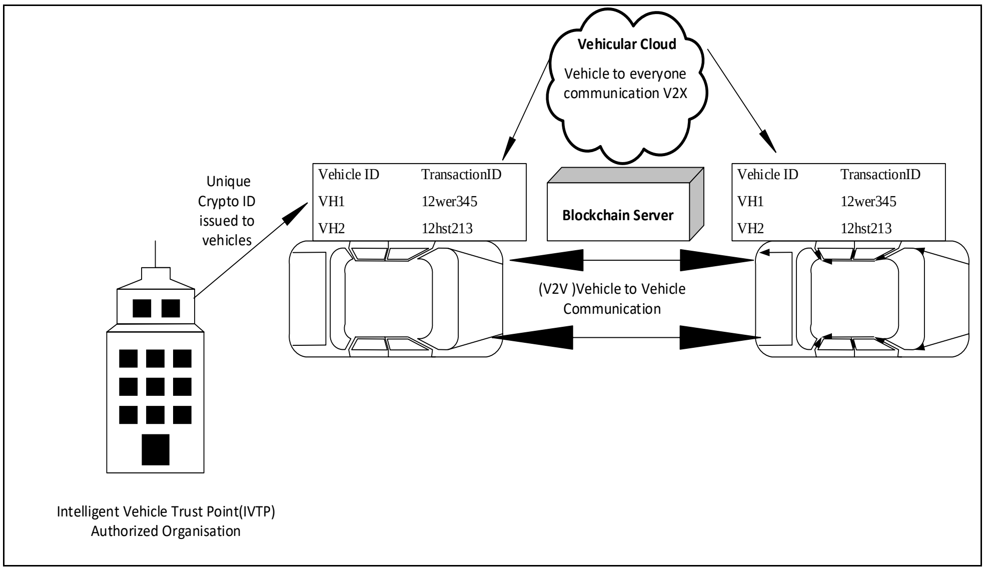
Smart cities' major goal is to provide effective services to their inhabitants while lowering administrative costs (Lima et al. 2020). When all of the vehicles in a smart city are connected to each other via IoT and the internet, issues of security and privacy can be overcome using blockchain. Traffic conditions and accident information can be easily shared between vehicles in a secure manner using this real-time position. With the use of smart, autonomous, and connected cars, CITS (Cooperative Transportation System) and smart transportation are boosting the road traffic sustainability (United Nation 2015). These vehicles have the potential to totally transform traffic networks by enhancing security and safety, as well as lowering energy consumption and emissions. Electric vehicles with no drivers will radically transform the transportation sector, and new business models with mobility as a service as a goal are emerging (Pangbourne et al. 2018). Blockchain technology can help build confidence in vehicular networks by allowing for the deployment and development of mobile autonomous systems with safe and immutable transactions in distributed ledgers. Food waste and food scandals are reduced by the traceability of transportation effectiveness in blockchain. Smart contracts can enhance the market of electric car with reduction in emission which Smart contracts can boost the electric car market by lowering emissions, which is good for the environment. Data sharing among drivers combined with incentive systems can help cities minimise traffic congestion.

Smart Transportation using a decentralised blockchain network that is not owned by any corporation but on which any company can join, collaborate, and create. The DAV open-source platform is built to be readily integrated into any autonomous vehicle platform; it's written in any language that developers are familiar with, and it allows them to link their vehicles to the blockchain without having any prior knowledge of the technology. This is a sample application created with the DAV open-source platform. It's a drone delivery, and you have a user asking bids for drones in the area. It's purely peer-to-peer, with no corporate involved. Drones submit bids and pricing in DAV tokens. The user accepts that the smart contracts have been signed, that the mission is underway, and that the tokens will be sent once the task is completed. The DAV Alliance is a group of commercial entities that have integrated the DAV protocol and platform into their vehicles.

Capacity is one of the most pressing issues confronting shippers in today's market. Because short order lead times and tiny order sizes aren't changing, there are only so many consolidation chances inside a company's outgoing and incoming flows. The logical next step is to focus on collaborative logistics. Now, in order to take advantage of collaboration, you must know your network inside and out. You must also be able to see both your outbound and inbound flows. Collaborative logistics does not always have to involve other shippers; it can also occur within your own organisation or between departments. Understanding where you have consistent, freight understanding, and order sizes that are conducive to outgoing and inward complementary flows, whether within your network or across a network of shippers, is critical to your transportation strategy. And building a mobility strategy to take advantage of a collaborative network requires intentional effort; it's all about first and foremost understanding and recognising what's going on within your own network. Collaborative logistics are a bit of a stretch if you don't have visibility, if you don't understand, if you can't see what's going on between your outbound and inbound operations, or across different divisions, even within your own company, but once you get there, there's still a lot of shipping going on. There are a lot of 80% full trucks that might be 100% full through collaborative opportunities both within your network, such as with other divisions, suppliers, and carrier partners, as well as across networks. Now, in order to do it with other shippers, you must first understand what's going on in your own network, including where you have steady flows and freight that lends itself to cross-loading and transportation consolidation options. Being able to view not only the planning and execution taking place within your own supply chain, but also what's going on in other networks, in real time. Not only that, but having strong computational and optimization capabilities that will aid in the identification of collaborative logistics prospects is the only way to go. Optimisation and transparency are achieved through collaborative logistics.

Blockchain has a lot of potential in terms of improving transportation and making businesses more profitable and efficient (Yuan and Wang 2016). Major difficulties confronting the transportation business include payment conflicts, excessive administration costs owing to paper transactions, and the industry's struggle to match shipper demand with carriers (demand and supply). Blockchain facilitates document coordination through the use of a distributed shared ledger, resulting in significantly less paper work. Smart Contract allows for quick processing by expediting approvals and clearing. Blockchain trust provides firms with secure, up-to-date, and certified data to help them make informed decisions. With the use of the blockchain, order authentication and tracking are done instantly, making the system scalable. BiTA is a blockchain-based collaborative transportation firm established in the United States (Oriold 2011). Blockchain addresses the issue of transportation by settling payment disputes, lowering administrative costs, and tracking temperature-controlled commodities such as vaccines. It is nearly hard to alter any data in the blockchain, making it more trustworthy.

Because the blockchain enables data authentication and validation, freight tracking is much more efficient (Irannezhad 2019). The capacity is monitored via Blockchain, IoT, and Artificial Intelligence. Sensors in cars can detect how much space is taken up in a package, calculate the cost, and send all of the data to blockchain. a single vehicle The performance of a car may be tracked with the use of blockchain, which can also be used to buy and trade vehicles. V2V (vehicle to vehicle communication) uses blockchain and the internet of things to allow vehicles to interact with one another, improving safety and fuel efficiency (Dey et al. 2016). Figure 3.3 depicts Smart Transportation Technology, in which cars are given a unique id as well as a transaction ID. Through an authorised organisation, the Intelligent Vehicle Trust Point (IVTP). Blockchain Server achieves vehicle-to-vehicle (V2V) communication via the vehicular cloud. By providing authorised data and preventing duplications, technology has completely eliminated the middleman. Smart Contract eliminates all administrative effort, reduces costs, and eliminates the possibility of errors. Payments to the shipper are made automatically when the parcel arrives at its destination, thanks to smart contracts.


Vehicular Cloud
Vehicle to everyone communication V2X
Unique Crypto ID issued to vehicles
Blockchain Server
(V2V)Vehicle to Vehicle Communication
Intelligent Vehicle Trust Point(IVTP) Authorized Organisation

Vehicle ID	TransactionID
VH1	12wer345
VH2	12hst213

Vehicle ID	TransactionID
VH1	12wer345
VH2	12hst213

Figure 3.3 Smart transportation (Dey et al. 2016)

Toyota is utilising distributed ledger and blockchain technologies to accelerate the development of autonomous driving technology (ETAuto 2017). They work in industries such as data and transaction sharing, as well as insurance. Blockchain allows individuals and businesses to safely share driving data in the marketplace. Vehicle sensors are fully aware of their surroundings and, because they are also connected to the cloud, they generate a large amount of data. By protecting data privacy and ownership, blockchain creates an atmosphere conducive to sharing. The usage of blockchain-based tools has the potential to allow vehicle owners to profit from their asset by selling cargo space or rides. All information regarding drivers, passengers, and owners can be stored in these tools. Smart contracts can be used to validate payments between parties without the need for a mediator. Insurance blockchain can be used to store and preserve transparency between owners, drivers, and insurance firms to reduce the trouble and fraud.

Porsche has also used the blockchain to improve its self-driving technology. They've proven that using an app, we can lock and unlock a vehicle, as well as use it for permission. They claim that blockchain-based services are both quick and secure. Distributing access and authorisation may be done quickly, securely, and remotely. All communication between cars and other participants is kept under strict confidence. They've created a blockchain-based network that's safe for electric vehicle charging and payments. Self-driving cars can update road conditions on the network, offer traffic alerts, accident alerts, weather alerts, and traffic congestion alerts on the V2V network, thanks to this technology combined with the internet of things.

IBM is also utilising distributed ledger and blockchain technology to enable secure payments such as e-battery charging, toll tolls, and parking fees for vehicles. This allows a vehicle to respond to its environment without the need for human involvement.

Blockchain improves confidence between players in smart cities and smart transportation, as well as the secure exchange of money and data. It lowers harmful attacks on automobiles by improving security and key management, and it can also provide legal guidance in the event of an accident. It may also offer rewards to drivers who submit accident and traffic information. Supply of Energy for electric vehicles recharging can be managed well by blockchain. Blockchain can effectively regulate the supply of energy for electric vehicle recharging. Smart transportation ushers in a new mobile environment that is more efficient, uniform, and linked. Consumers, systems, and service-oriented business models are central to this system. The primary foundations of a decentralised mobile platform are the convergence of IoT, blockchain, and cloud.

3.4 Industrial Trading Business Model using Blockchain

Blockchain is simply a decentralised digital database with no central authority. The blockchain technology is based on a peer-to-peer network that is distributed, allowing all network participants to access the database's records. Blockchain is a rapidly evolving world, and knowing what's going on and understanding the technology is critical for regulators. (2018, Ganne) Build a connection between the blockchain community and the trade community in the book, and try to explain what blockchain technology is all about in simple terms to trade officials? What does it have the ability to do? What it can't do, and what it can't do. Without a policy framework that allows blockchain to grow, it has the potential to improve supply chain transparency and traceability. We may be squandering a chance to improve the efficiency and inclusiveness of international trade. According to Gartner, the advantages from block chains might yield three trillion dollars in value worldwide by 2030, according to recent research. While technology creates exciting possibilities, it also poses legal, regulatory, and policy challenges that need to be addressed. Because transactions are connected and time recorded, blockchain has opened up a plethora of new possibilities for international trade. Because multiple players have real-time access to the same information, technology allows for the facilitation of a variety of processes, such as border procedures. These players don't communicate with one another, work in silos, don't share data, and don't necessarily trust one another. As a result, having technology that allows these many players to collaborate and trust one another is extremely valuable. Except that the technology is the source of trust, and it is critical for regulators to keep this in mind as they consider what their role should be and what they can do to allow technology to realise its full potential and make a difference.

International trade will be transformed by blockchain technology. SAP is exhibiting how digitally expedited procedures may save time and money for several stakeholders. It is not simply the seller and the buyer that are involved in international trade. Banks, insurers, carriers, freight forwarders, agents, brokers, and government agencies are all engaged. Parties today exchange data and documents in a peer-to-peer environment. There is no unified perspective of the process or revisions of documents. The expense of individual interactions between partner systems is high. Paper-based document management is inefficient, and transporting paper documents via express courier services adds a substantial cost factor. Blockchain for ocean transportation addresses these difficulties and provides mutual benefits to all stakeholders involved in the supply chain. SAP Cloud Platform Blockchain Service can run a blockchain for maritime transportation (SAP 2018). The various parties can link any system via web services or utilise a cloud application to access the blockchain. The transaction is documented, and all parties involved are invited and enrolled. Important papers, such as letters of credit, are transferred and signed online. The shipping process is overseen by both parties. The shipper submits all necessary documentation for export customs clearance. The ocean carrier posts the bill of lading after the customs clearance status is obtained. Electronic papers can be digitally signed using a smartphone app. A bill of lading's ownership is securely transferred. Banks, insurers, and purchasers are always in the know about what's going on. It's all about clearing import customs and getting the container released from the port of discharge in the destination country. Mobile QR code scans, two-factor authentication, and a verification against block chain-based entitlements are all part of SAP's highly secure container release procedure Ocean shipping blockchain promises to generate a new level of security, transparency, and trust. It transforms ocean shipping procedures by allowing digital document sharing, signing, and approval. In a nutshell, this revolutionary method reduces costs, improves productivity, and eliminates fraud and stolen freight. For this new solution, SAP is collaborating closely with clients in a co-innovation paradigm.

3.5 Conclusion

Many firms have been attracted to blockchain because of its security and privacy features. Technology has been employed in a variety of industries and organisations to facilitate various types of transactions as well as the development of numerous business models. Many nations are working on elections based on blockchain technology, employing online voting, which will make voting easier for voters and ensure the anonymity of electronic voting, boosting the economy of any country. Because the data is extremely safe and there may be a vast amount of data, blockchain-based cloud storage could be extremely beneficial. Using blockchain technology, smart and collaborative transportation, such as smart vehicles and smart transit, may be conceivable. International trading, which involves many different entities in the network, can now be connected in a secure blockchain network, which will allow users of the network to not only track items for trading, but also to make payments and transactions among themselves using the blockchain's smart contracts.

CHAPTER 4

PRESERVING THE PRIVACY OF ELECTRONIC HEALTH RECORDS USING BLOCKCHAIN

4.1 Introduction

Several aspects of human life have been impacted by technological advancements in recent decades. It provides a number of advantages, particularly in the healthcare sector. Electronic data and statistics are kept, which aid clinicians in better diagnosing patients. It has also increased communication between doctors, and doctors are now quickly available to patients in an emergency. The medical records of patients are preserved electronically in the form of digital statistics known as Electronic Health Records (EHRs), which are kept by the hospital or a clinician throughout time (Gunter, 2005). The electronic medical statistics include MRI reports, previous medical examinations, vaccines, laboratory data, and any type of allergies that the patient may have (Hufnagel, 2009). These statistics are real-time information that can be accessed by a sick person or a doctor, and they are only available to legitimate users. It can be shared with other health-care experts from many institutions for improved research and study in the field. There are a number of advantages to using electronic health records, including:

It improves on traditional ways of storing patient medical data on paper, which were vulnerable to numerous unforeseen events such as natural disasters, robbery, and conflict.

• EHRs are highly useful in the continuous advancement of healthcare because they reduce the incidence of data mistakes.

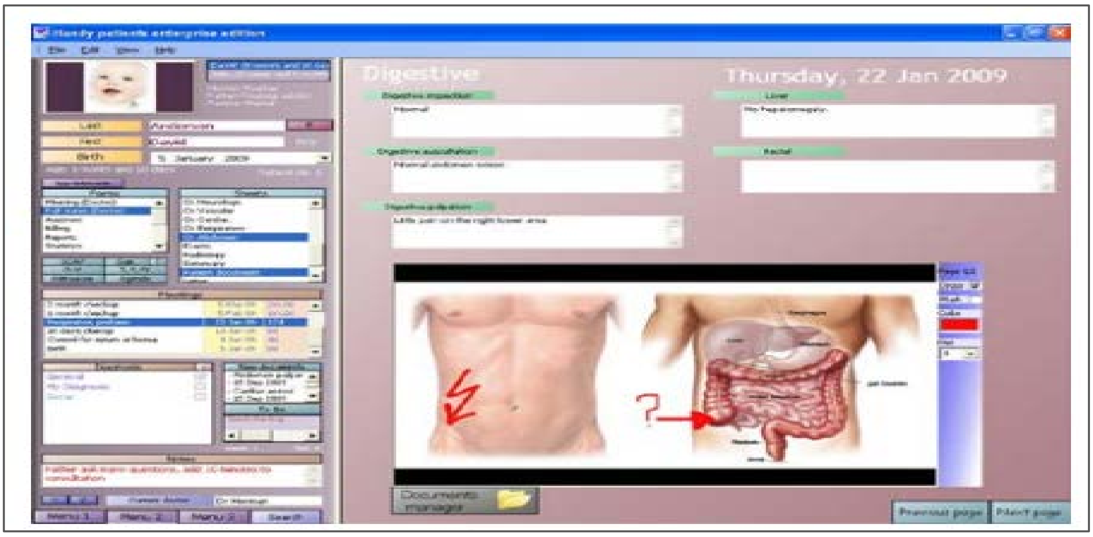
• The accuracy and clarity of health information is improved by minimising the occurrence of data errors.

- It can also be effective in disseminating health information at any time and place, reducing the likelihood of repeat testing, treatment delays, and empowering patients to make better decisions (Evans, 2016).
- Patients' participation has grown, allowing care practitioners to make better, faster judgments and give better care to sick people as quickly as possible..

Apart from the advantages of technology growth, electronic statistics have a number of disadvantages. The following are some of the disadvantages: • The data has become more vulnerable to unauthorised access.

- The records are stored using a cloud-based approach, which is secured using passwords that can be easily compromised using various hacking techniques or social engineering.
- The records are stored using a cloud-based approach, which is secured using passwords that can be easily compromised using various hacking techniques or social engineering (Fernandez-alman, 2013). Various hacking techniques or social engineering (Fernandez-alman, 2013).

As a result, there is a pressing need to protect patients' personal information and health data by storing it securely and preventing intruders from accessing it (Bertino, 2015). Following a blockchain-based method for EHRs is an effective way of securely storing statistics via a network. To address these issues, a safe framework based on blockchain is proposed for securing patient medical records and maintaining the privacy of sick people. Figure 4.1 shows an example of an electronic health record (Oguntoye patients electronic medical record (free open-source version)).



Digestive

Thursday, 22 Jan 2009

Last: Anderson

First: David

Birth: 5 January 2009

Liver: No hepatomegaly

Rectal

Figure. 4.1 A sample glimpse of an electronic health record

Figure 4.2 depicts the procedural flow for storing electronic health records electronically.

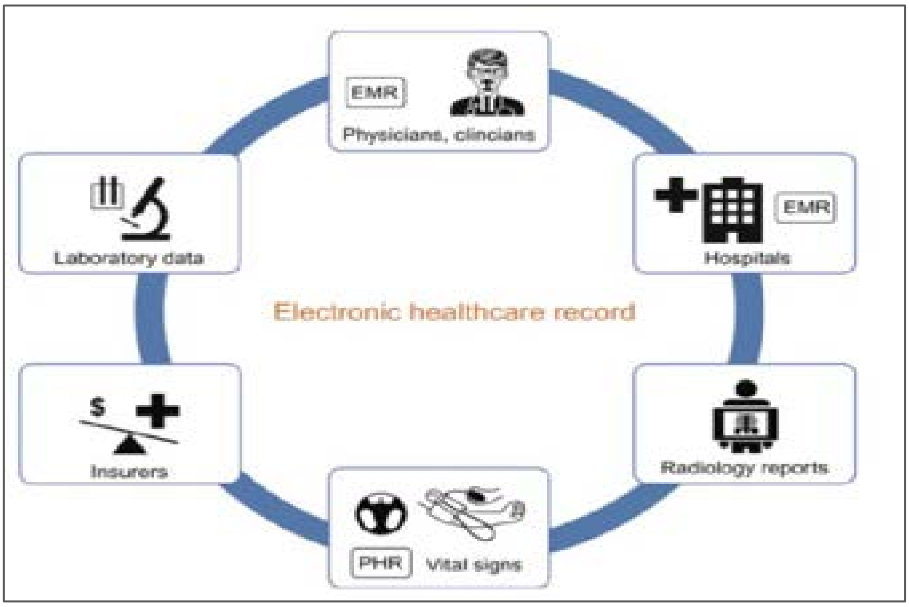


Figure 4.2 Electronic healthcare record process diagram

4.2 Blockchain in Preserving EHR

There is minimal assurance of the forthrightness and validity of ill person data on neither side of the current biological statistics management system driven by medical organisations. The threat of biological statistics being harmed is unavoidable, and these numbers are constantly exposed to security threats, personal privacy breaches, and other difficulties. Most biological statistics are stored in biological institutions in a centralised way, which makes them vulnerable to various threats such as deliberate tampering, hacking, and natural disasters, all of which can result in biological data loss and destruction.

4.2.1 Structure Design and Architecture

Participants, Assets, and Transactions are the three primary components of the blockchain network. An electronic health record structure employing blockchain is described in this implementation. Figure 4.3 (a) shows the structure of blockchain (b). There are four key participants in the electronic health record:

i. Clinicians/Doctors
ii. Patients
iii. Labs
iv. Administration

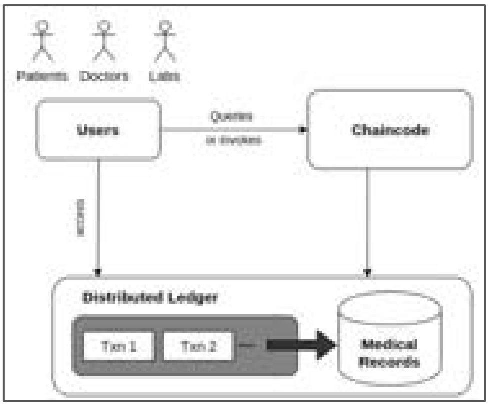
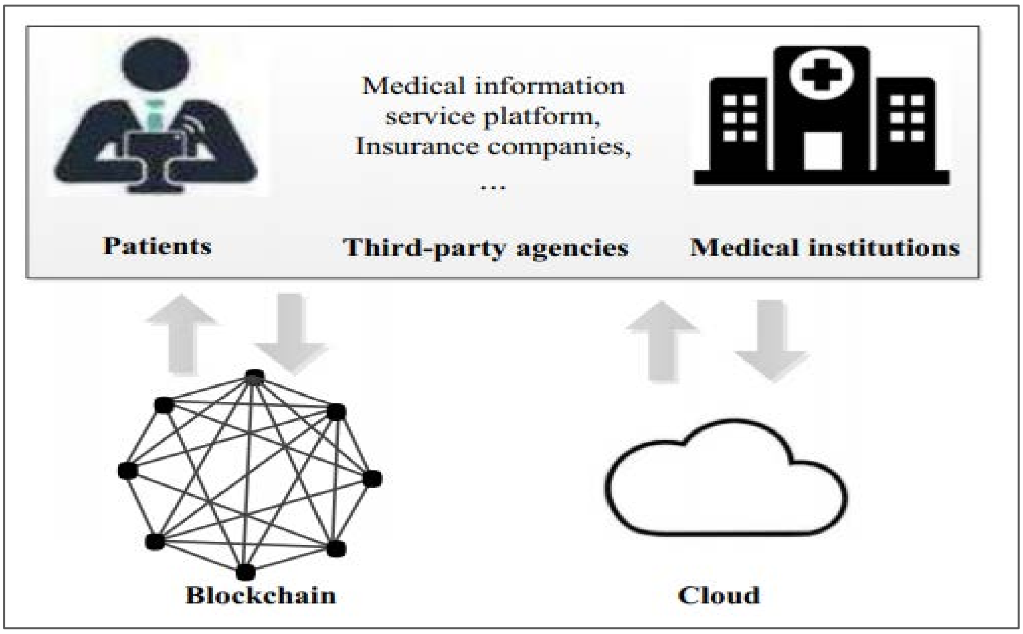


Figure. 4.3 (a) The Architecture of the Structure



(b)

Figure. 4.3 (b) The Architecture of the Biological Blockchain

As a participant in the EHR structure, patients play a significant role. They own the health data that is collected and stored on the blockchain. They have the ability to update their personal information. As a result, they have the authority to control who has access to their information. Patients prevent any unauthorised medical provider or third party from accessing their information. Clinicians are health-care professionals who use diagnosis to collect biological data on patients. They are accountable for updating health-related information in the records of only those patients who have confirmed that they are authorised physicians and have given them permission to write into their records. They have the ability to modify their personal information or profile. Labs are in charge of conducting tests, generating test findings, and updating this information in the statistics of those patients who have given them permission to write into their records. They have the ability to edit their profile information. The administrator is in charge of deploying the blockchain network, implementing various contracts in the network, generating the key, and encrypting and decrypting transaction data.

Biological statistics are the network's asset in this structure. Each biological record belongs to a sick person who has signed up for the network. When a transaction is completed, the asset's value changes. Changes include things like statistical updates if the sick individual is diagnosed with a new ailment, prescription changes, test findings, and so on.

Transactions are acts taken on the network's assets, such as adding a participant, generating a biological record, retrieving specific material from the network, updating the participant's information, and granting or robbing access to a clinician or lab. A relationship between the two participating nodes is required for the execution of some of these transactions. A physician, for example, may be granted access to a patient's biological material if the patent's ID appears on the list of that clinician's patients. In basic terms, the person whose biological data is to be accessed must be a patient of a doctor, and only then will access be granted. This structure also defines the permission rules. These rules determine what kind of access and resources are available to the participant. This aids in limiting access to all of the structure's resources. Only authorised users have access to manipulate or read certain information. The system performs the following transactions:

• CreateMedicalRecord - This transaction creates records in the network. There are fields such as recordID, owner, and a list of permitted patients and labs in it. It has fields for storing patient medical information such as medical history, last consultation with which doctor, consultation date, allergies, any dangerous habits, and so on. The record's ID is unique to the record and is used to identify it in the collection.

- GrantAccess - In order to change the record, the clinician/doctor would require access to it; only the approved doctor would be able to read or write it. Using this transaction, access is granted.
- GrantAccessToLab - If labs want to change a record, they must have access to it as well.

- .RevokeAccess - Once the need to access a certain record is fulfilled, the access to that record from the clinician. The clinician no longer remains authorized to read or alter that record.

• RevokeAccessFromLab - Once the job is completed, access to the labs is likewise removed.

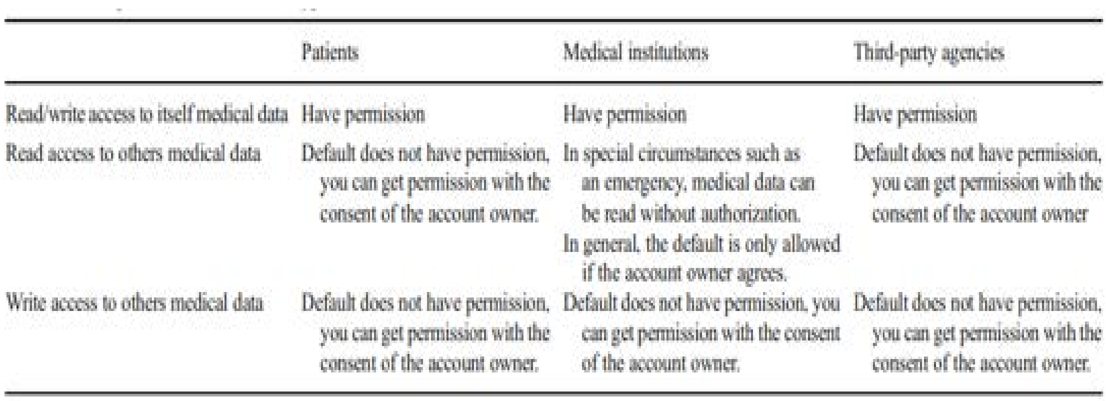
• AddParticipant - This transaction is run whenever a new node is added to the system.

• UpdateParticipant - This occurs when the data inside the participant's node is changed.

• UpdateAsset - This occurs when we make changes to the medical records' details.

To accomplish safe storage and sharing of biological facts, the storage scheme employs blockchain and cloud storage technologies. Figure 4.3 depicts the biological blockchain's architecture (b). The biological blockchain has three primary categories of transaction bodies: biological institutions, patients, and third-party agencies (such as biological material service platforms, biological insurance organisations, and so on). Biological institutions are in charge of diagnosing and treating patients, as well as collecting their biological data. Patients can see doctors at various biological institutions and retain ownership and management of their personal biological data Some services, such as recommending biological institutions and registering for appointments, can be provided by third-party agencies. Permissions vary depending on the transaction body type. Table 4.1 displays the permissions for the three different types of transaction bodies. The biological blockchain's core transactions are storage of statistics and access to control. Although it would be ideal to store all biological statistics on the blockchain, practical restrictions such as cost and storage space have limited this to only index material of biological statistics and transaction statistics. Large amounts of biological data should be encrypted and saved outside of the blockchain. These biological statistics were averaged in cloud storage under the chain in our scheme.

Table 4.1 Permissions for the three types of transaction bodies



	Patients	Medical institutions	Third-party agencies
Read/write access to itself medical data	Have permission	Have permission	Have permission
Read access to others medical data	Default does not have permission, you can get permission with the consent of the account owner.	In special circumstances such as an emergency, medical data can be read without authorization. In general, the default is only allowed if the account owner agrees.	Default does not have permission, you can get permission with the consent of the account owner
Write access to others medical data	Default does not have permission, you can get permission with the consent of the account owner.	Default does not have permission, you can get permission with the consent of the account owner.	Default does not have permission, you can get permission with the consent of the account owner.

Permission determines control access, and different transaction entities have varying control permissions. The right to utilise personal biological statistics is totally controlled by the patient in the biological blockchain; the ill person may authorise a subject access to the required data. The sick individual can also revoke their consent at any moment. The freshly created blocks are confirmed before being added to the main chain, forming a permanent record of the transaction data. The timestamp is used to ensure that the blocks in the biological blockchain follow the timing connection. The blockchain's statistics have been tampered with using the hash function, and identity identification can be done using public-key encryption. The combination of these technologies ensures the biological blockchain's safety and security. The biological blockchain's block structure is based on a Merkle Tree and is constructed as depicted in Fig. 4.4 The fundamental functions of the biological blockchain are the release, preservation, and sharing of biological data. A doctor creates biological data or examination reports for a sick person who attends a biological institution. The physician prepares the digest and hash of the biological statistics and posts them to the blockchain after signing in with the issuer's private key when the biological statistics are generated. Simultaneously, the biological statistics are encrypted with a symmetric key and the biological statistics' encryption key is encrypted with the patient's public key. Both are supplied to the sick person in large quantities, along with a biological statistics storage area for data storage. Following receipt of the statistics from the biological institution, the sick person verifies the institution's signature, then uses its own private key to decrypt the biological statistics encryption key, the original biological data, and the signature, and then generates a new encryption key to store the biological statistics and its signature in the cloud storage extensively with Biological sharing. The user has complete control over the biological data usage rights, and the ill person can authorise a third-party agency to access some of his or her biological data via the access to control mechanism, and can revoke his or her consent at any moment. The access to control policy will be determined by the location, usage rights, and expiration date of the shared statistics in cloud storage, as well as the decryption key of the third-party agency written into the biological blockchain, and cloud storage management.

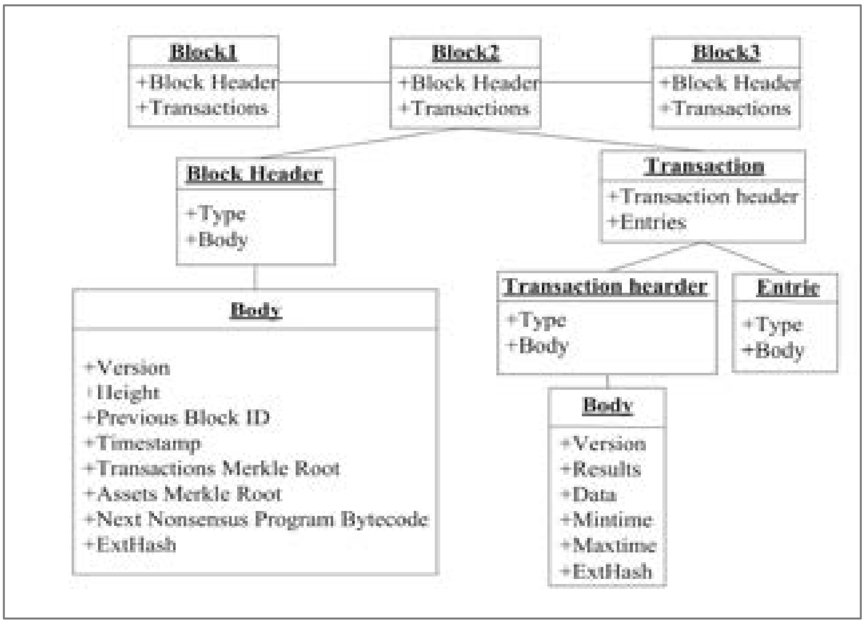


Figure. 4.4 The Block Structure of the Biological Blockchain

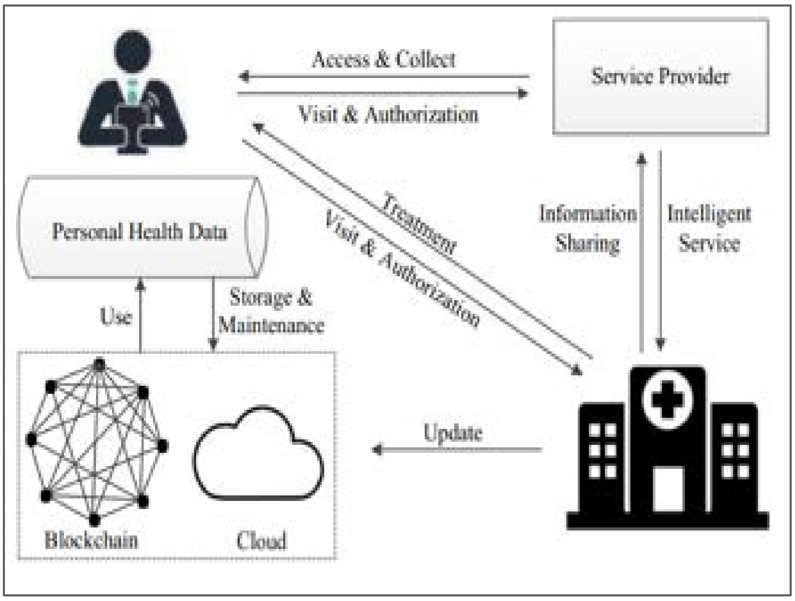


Figure. 4.5 A Biological Service Framework Based on Blockchain Technology

4.3 Structure Implementation

To put this structure in place, we used the Hyperledger Fabric blockchain-based platform and the Composer tool.

4.3.1 Hyperledger Fabric

It is a Hyperledger project and a blockchain framework developed by the Linux Foundation. This framework is useful because it allows components to be plug-and-play, such as consensus and membership services. It enables container technology to host smart contracts, often known as "chain code," which make up the structure's logic (Sabarivelan, 2020).

4.3.2 Hyperledger Composer

- It is a free and open-source tool for constructing a blockchain-based business network. The tool aids business owners and developers in the creation of many smart contracts and blockchain applications to address a variety of business issues. Various procedures are followed to construct this blockchain-based EHR network, as indicated in fig 4.5.
- Data collection: The doctor collects the patient's personal information as well as biological statistics such as vital signs, allergies, dangerous behaviours, biological history, test results, prescriptions, and statistics created through clinical diagnosis.
- Wallet allocation: This is a designated area for the blockchain network to be deployed. It's where track of all of the transactions is kept.
- Using Hyperledger Fabric and Composer to deploy a blockchain network: We implement our business network and start our blockchain network on composer playground following wallet allocation.
- Creating various nodes in the system: We created a model of our structure that included the template design of several pamphlets.
- Biological data creation: We also provide a framework for storing patient-owned biological statistics.
- • Transaction creation: We construct the transactions that must be carried out according on the requirements, such as granting or robbing access to and from doctors or labs, or listing the permitted clinicians or labs for a biological record.

- • Adding a node to the structure: Using sample statistics, an instance of the Sick person, Clinician, Lab, and biological record owned by some patients was created. Before being added to the network, the nodes are confirmed by other registered nodes in the network and a public identifier is generated.
- • Definition of various permissions granted to the user: This is where we define which structure resources (biological data) that participant has access to. Only participants with specific permissions (such as Read-only, Write, All, Transfer, and so on) have access to specific biological statistics.
- • Transaction execution: Various transactions are done based on the user's requirements, and statistics can be retrieved from the saved collection if necessary. Following the execution, a new biological record is created.

  Figure 4.6 shows a node formed for a sick patient, whereas Figure 4.7 shows a record of all network transactions.

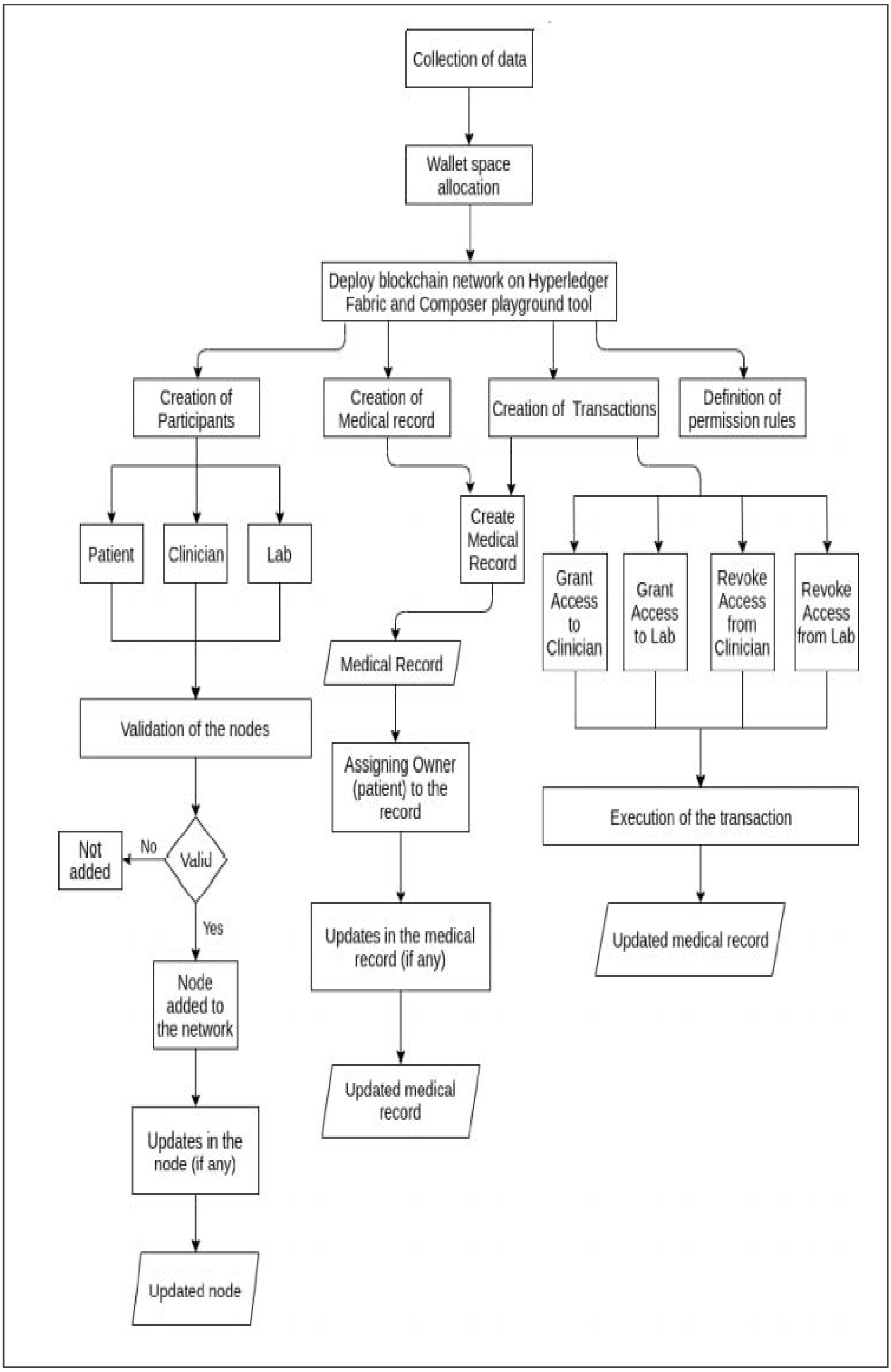
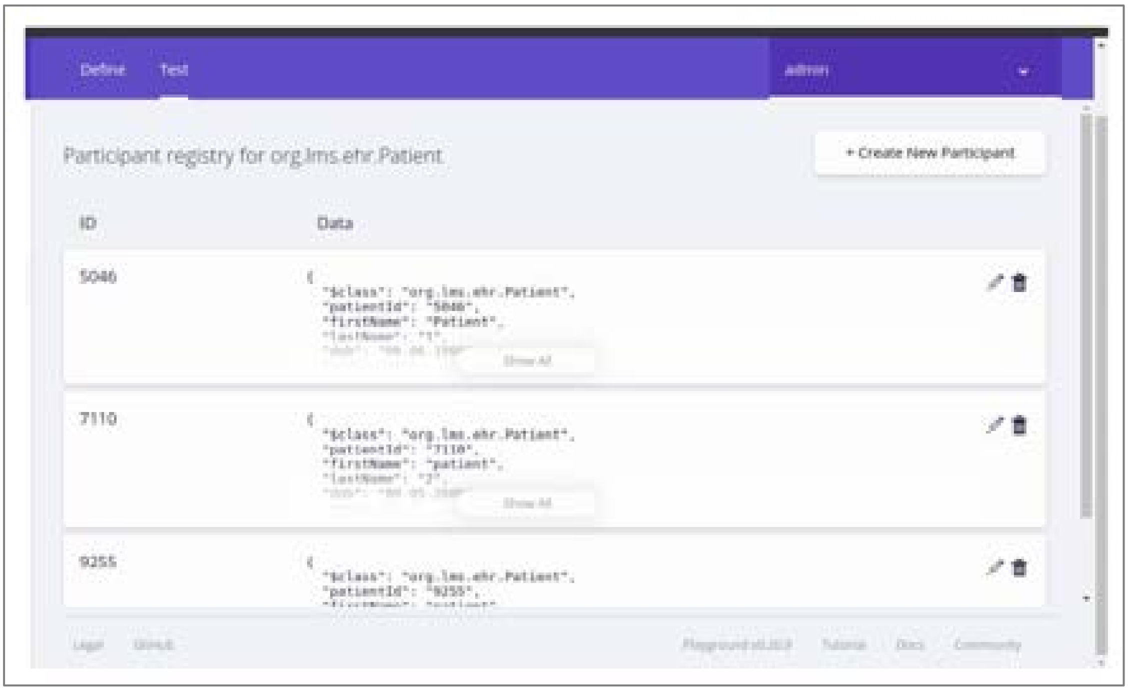

Collection of data
Wallet space allocation
Deploy blockchain network on Hyperledger Fabric and Composer playground tool
Creation of Participants
Creation of Medical record
Creation of Transactions
Definition of permission rules
Patient
Clinician
Lab
Create Medical Record
Grant Access to Clinician
Grant Access to Lab
Revoke Access from Clinician
Revoke Access from Lab
Medical Record
Validation of the nodes
Assigning Owner (patient) to the record
Execution of the transaction
Not added
No
Valid
Yes
Updates in the medical record (if any)
Updated medical record
Node added to the network
Updated medical record
Updates in the node (if any)
Updated node

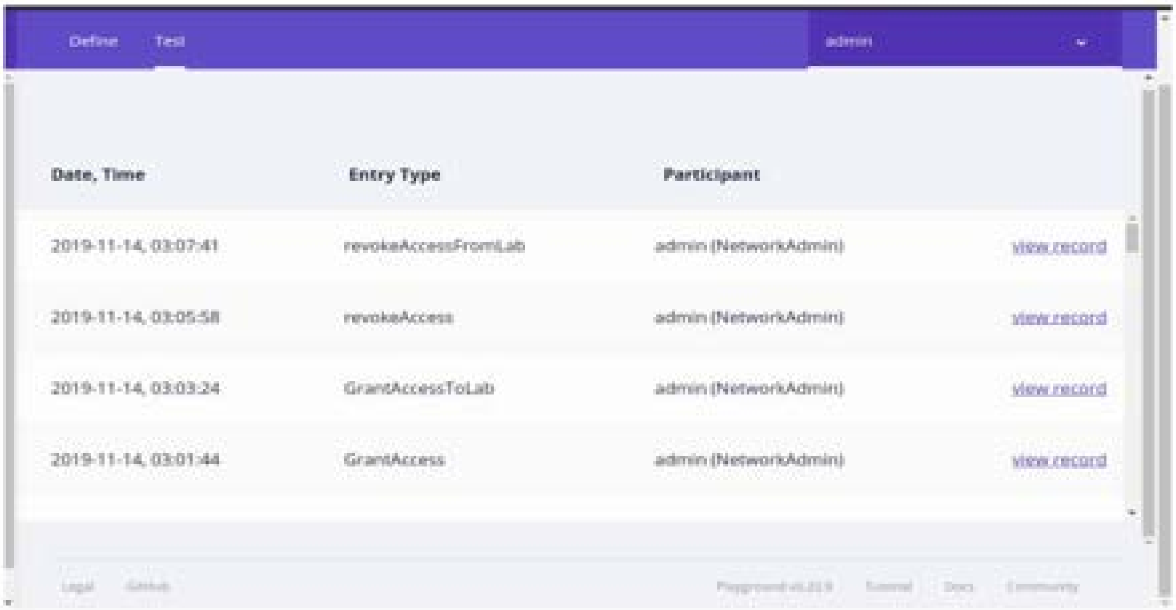
Figure 4.6. Flowchart of the whole process



Participant registry for org.lms.ehr.Patient

ID	Data
5046	{ "$class": "org.lms.ehr.Patient", "patientId": "5046", "firstName": "Patient", "lastName": "1", "dob": [illegible]
7110	{ "$class": "org.lms.ehr.Patient", "patientId": "7110", "firstName": "patient", "lastName": "2", "dob": [illegible]
9255	{ "$class": "org.lms.ehr.Patient", "patientId": "9255", "firstName": [illegible]

Figure 4.7 Sick person node created and added to the network



Date, Time	Entry Type	Participant	
2019-11-14, 03:07:41	revokeAccessFromLab	admin (NetworkAdmin)	view record
2019-11-14, 03:05:58	revokeAccess	admin (NetworkAdmin)	view record
2019-11-14, 03:03:24	GrantAccessToLab	admin (NetworkAdmin)	view record
2019-11-14, 03:01:44	GrantAccess	admin (NetworkAdmin)	view record

Figure 4.8 A record of all transactions that executed in the network

4.4 Conclusion

EHRs (electronic health records) are patient health records that are saved digitally in a network. EHRs provide a variety of options to improve patient care, clinical practise performance measurements, and future clinical research contributions. In the modern era of smart cities and homes, the techniques utilised to store EHRs have been quite vulnerable. Hackers and unauthorised third parties can readily access the data. Patients and healthcare providers also have no access to the information. These solutions fail to strike a satisfactory balance between data security and data accessibility. However, blockchain has the potential to solve these problems. Blockchain creates an immutable ledger system that allows transactions to take place in a decentralised fashion. The three major characteristics of blockchain technology - security, decentralisation, and transparency - ensure that any application created with it is secure and inaccessible to unauthorised parties. Manipulation of data on a blockchain network is nearly impossible. In this project, we propose a way to use blockchain technology to create EHRs and make them safer and more private. Using cryptographic techniques and decentralisation, blockchain technology will maintain control over information access. It will also strike a balance between data security and data accessibility. The conceptualization of data privacy and security issues in electronic healthcare is the fundamental goal of this project.

CHAPTER 5
PREVENTING THE THEFT USING BLOCKCHAIN TECHNOLOGY

Blockchain technology is a new technology that was created for the purpose of cryptocurrencies, but as it spreads to other industries, it is providing many benefits to blockchain users. Blockchain technology is resistant to tampering and is one of the most secure technologies available today. These characteristics of the technology have led to its usage in a variety of industries where information security and privacy are paramount.

The healthcare industry is one such sector where blockchain technology has played a critical role in safeguarding patient information and offering privacy to any patient's health-related problem. One example is the protection of human organs and uncommon blood kinds from theft. There have been several incidences of organs and rare blood groups being taken from organ donation camps and blood banks in most nations, particularly in India. This might be due to a variety of factors, including insufficient security measures or transaction failures such as dual transactions. Using such transactional and security concerns, the theft might be regulated to a large extent. As a result, the main goal is to provide a new way for leveraging Blockchain technology to prevent the theft of human organs and rare blood groups.

5.1 Introduction

The blockchain is unquestionably a brilliant invention (Politou, 2019). It was created by a person or group of persons under the pseudonym Satoshi Nakamoto, but it has now grown into something bigger. Blockchain technology was created to support the Bitcoin cryptocurrency. The goal of developing a decentralised chained data structure like this was to create a transaction system with its own currency that could store information about past transactions. The term "blockchain" has become popular in both industry and academics (Pilkington, 2016; Maltseva, 2019). The intrinsic value of cryptographic transactions is derived from their capacity to preserve genuine values internationally and without regard to jurisdiction (Zhou, 2019). The security of a blockchain system is managed by security standards, which ensure that users' sensitive data is protected.

5.2 Preventing the Theft of Human Organ and Rare Blood Group

The whole point of blockchain is to have safe and decentralised transactions. There have been several incidences of organs and rare blood groups being taken from organ donation camps and blood banks in most nations, particularly in India. The causes range from ineffective security measures to transaction failures such as dual transactions. Such transactional and security concerns might be managed with this solution, preventing theft to a large extent.

Healthcare is becoming increasingly complicated. The data generated by healthcare is so complicated that maintaining the data's quality will become harder in the future. Hospitals and other medical institutions generate a tremendous volume of data, making it challenging to identify exactly what is needed. The healthcare analysis is beneficial not only to patients, but also to hospitals that care for them prior to and after their hospitalisation. Managing healthcare data also encourages patients to participate in predictive modelling and analysis based on the data. Electronic medical records (EMR), pathology labs, immunisation programmes, and other surveys in medical camps are all places where a lot of healthcare data can be collected. Each of these systems is built and intended for clinical usage, such as in hospitals where we have electronic healthcare systems as well as specific departmental systems for laboratory diagnostic imaging, pharmacy, nutrition services, billing, anatomic pathology, and so on. In other words, they collect precise data on the patient for patient care. However, none of the systems contain a complete set of data for each patient or group of patients, thus all patients hospitalised in January with a specific disease can be analysed and reported Getting a detailed understanding of what's going on with individual patients as well as with groups of patients necessitates combining data from several systems and performing statistical analysis on it. In contrast to the many clinical systems discussed above, a clinical data warehouse compiles all of a patient's data into a single, well-organized location that can be utilised for analysis and reporting. Laboratory test reports, imaging tests such as X-rays and CT scans, financial records, past medication supplied to the patient, previous medical history, and latest appointments are all examples of data generated in the healthcare industry. When numerous patients are treated at the same hospital or healthcare facility, all of these data add up to a massive amount of information. The amount of data used in the healthcare industry is rapidly increasing. However, there are certain issues with a large volume of healthcare data, such as security of patient data, privacy of patient data, data access, and how this data can be accessible outside of the healthcare delivery facility where the data is held. Furthermore, when compared to traditional storage methods, the storage capacity of big data and the type of solution provided by big data would be more efficient.

5.2.1 IoT Device

The internet of things (IoT) is a network of "things" that are integrated with sensors, software, and other technologies and are connected via any network (usually the internet) to exchange data and control from anywhere. IoT devices must have a unique identifier, and they must be able to communicate any data over a network without the need for human or node involvement. The IoT platform integrates data from numerous sources, does further analyses on the data, and extracts relevant information as needed (Gonzalez, 2020).

These wearable devices can be attached to the patient, allowing for the recording of the patient's health habits. The usage of IoT devices makes remote monitoring of the patient considerably easier (Litke, 2019). This implies that the patient and the doctors are in contact with one another at all times of the day. The patient's hospitalisation has been shortened, and re-admissions have been avoided, thanks to the patient's remote monitoring. As a result, the Internet of Things has made a tremendous impact in lowering costs while increasing patient treatment outcomes. We'll now look at how IoT devices might benefit patients, physicians, hospitals, and insurance companies.

The ESP32 chip, which is integrated with the sensors, actuators, and/or embedded system, pushes the data to the internet/Bluetooth. As part of the programme that will run, Esp32 includes a TCP Server. Esp32's job is to monitor incoming connections at a certain port on the device's IP address. When a distant computer, or client, connects to the TCP Server, it creates a channel for communication between the ESP32 and the client at the remote site. A WiFiServer object is used in an Arduino application for the ESP32 to generate a server. When a new connection is established, the server sends a WiFiClient object to serve as the communication channel.

5.2.2. IoT for Patients

Wearable IoT devices come in a variety of shapes and sizes. The gadget could be a fitness band that the patient wears on his or her wrist, or any other wireless device that measures the patient's blood pressure, heart rate, or even blood sugar level. These gadgets may be quite beneficial to patients since they can warn them to any changes in their calorie count, blood pressure variances, or any upcoming appointments. As a result, IoT gadgets have aided many patients, particularly those who are elderly and live alone. The IoT gadget may notify family members of any changes in the patient's values, prompting them to contact the appropriate medical agency.

5.2.3 IoT for Physicians

The patient's wearable devices not only assist the patient in preserving his or her regular health, but they can also be extremely beneficial to clinicians. Clinicians or doctors can monitor the patient's health on a daily basis as well as in the event of an instant medical emergency. These wearable devices allow doctors to keep a closer eye on their patients and communicate with them more frequently. The information gathered from the patient's wearable gadgets may aid the doctor in determining the optimal treatment option for the patient. Clinicians could also make decisions based on the data collected on whether the patient requires hospital admission or not.

5..2.4 IoT for Hospitals

Not only for patients, but also for hospitals, IoT devices might be quite beneficial. IoT devices are gadgets that have sensors that can collect data and produce an output. As a result, the gadgets can be used to track not just the patient's health, but also real-time information on the hospital's medical equipment, such as monitoring equipment, oxygen pumps, and cylinders (Lucas, 2015). Deploying medical personnel to multiple areas, and if medical personnel are going for any testing, such as corona virus testing, at several sites, they may be tracked and any assistance needed can be provided without wasting time locating the locations. Similarly, being close to a corona patient can be avoided with IoT devices by monitoring the patient from afar, preventing infections in the medical personnel. IoT devices could be extremely valuable in tracking drugs or pharmaceuticals that come from a trusted source, as well as monitoring temperature and humidity conditions.

5.2.5 IoT for Insurance Companies

For countersigning and claims processes, insurance firms can regulate data collected through health monitoring devices. This information could aid insurance companies in resolving claims and identifying forecasts for underwriting. IoT devices can help maintain transparency between the insurance business and the insured person by rapidly handling claims, with accurate pricing, and in different risk assessment processes (Maltese, 2015). The Internet of Things devices assist insurance firms in collecting data directly from insured clients, keeping track of their day-to-day activities, and keeping them on the proper treatment plan while implementing preventative health steps to maintain their health. With the use of IoT devices, claims settlement might be done in a simple and speedy manner.

A NodeMCU (ESP32 chip) is coupled to a keypad and a servo motor in the current scenario, transforming it into a node that is connected to the internet via a secure network. When a user inputs their phone number, it is uploaded to the cloud and loaded to the server, which generates a unique password for each user and sends it to their phone through text message. Once the number has been confirmed, a signal is delivered from the commonly utilised in circumstances where irreversible hash statements are required. A hashed value cannot be used to regenerate the original content from which it was formed, however an encrypted value may be decoded back to its original value if the relevant values such as salt and secretKey are known.

5.3 Proposed Methodology

Blockchain is a method of storing and exchanging data in a decentralised, transparent, and tamper-proof manner. Blockchain technology has the potential to revolutionise healthcare delivery. Laboratory test reports, imaging tests such as X-rays and CT scans, financial records, past medication supplied to the patient, previous medical history, and latest appointments are all examples of data generated in the healthcare industry. When numerous patients are treated at the same hospital or healthcare facility, all of these data add up to a massive amount of information. The amount of data used in the healthcare industry is rapidly increasing**.** However, a large volume of healthcare data has problems such as patient data security and privacy (Oriold, 2011, Pangbourne, 2018), data access, and how this data can be accessible outside of the healthcare delivery facilities where the data is held. Blockchain technology has the potential to help with this problem. One of the most important aspects of healthcare today is the need to handle a significant quantity of data, which is referred to as big data (Park, 2017), and this data may have an impact on the cost, quality, and value of the care provided.

The use of blockchain technology is critical. The technique protects the data's integrity or redundancy, ensuring that it has not been changed or tampered with from its original condition, or that it has not been damaged due to a database error. Blockchain technology can also be used to distribute healthcare data around multiple nodes in a network that makes advantage of the data's capabilities. Such characteristics, on the other hand, have an impact on the cost, quality, and value of the data that is employed. Only the nodes connected in the blockchain network have the right to access the healthcare data, and only after gaining permission from the person's own data, therefore blockchain technology can help with security and privacy of healthcare data. As a result, blockchain is employed to prevent the theft of human organs and uncommon blood groups gathered from various Big Data sources. First, we'll go through some of the key terms in blockchain.

5.3.1 Block

The blockchain, as the name implies, is a chain of blocks, and these blocks form the foundation of the technology. The following specific meta information is included in each block:

Data in Blocks: The data to be stored in encrypted format in the block, as well as the information about certified and permitted transactions tallied, is referred to as Block Data. The block header itself is made up of the following elements:

Number of Blocks: The index of the block in the chain is easily recognised as the Block Number. It's critical not to mix the block number with the block's unique identity. The size of the blockchain is directly proportional to the block number (Atzori, 2015).

Previous Hash: The previous block's hash value is referred to in the current block to form a link. Tampering is prevented by the prior hash value. 0 is the previous hash for the genesis block: The genesis block, also known as the basic block, is the first block on the blockchain.

Hash of the Day: The created output of the cryptographic hashing algorithm, which encrypts the input values to a certain length, is known as Current Hash. The block's index, data, previous hash, timestamp, and nonce value are typically provided as input to the hashing process.

Timestamp: A timestamp is a reference to the time when a block was created.

The block's size (optional): The block's size refers to the amount of memory it has for storing prior transactions.

The nonce value is an acronym for "number only used once," and it is sometimes referred to as a measure of difficulty. The nonce is the value that blockchain miners seek. The nonce value is hashed in the block, which limits the mining complexity when rehashed.

The expected digital signature, i.e. the prior hash, is guaranteed by the authenticity and validity of the block. A block that has not been validated or authenticated will not be added to the chain.

LEDGER is a blockchain-based digital journal that is shared among all users. It keeps track of all transactions on the blockchain network in question. A blockchain transaction can't be changed after it's been recorded. The public keys of the users participating in the transaction make up the ledger record of the transaction. A user exchanges sensitive information with another user throughout the transaction. The concept and philosophy of distributed ledger ownership are promoted by blockchain technology (Bryanov, 2018; Ge, 2019). Simply said, blockchain technology is nothing more than a reliable and secure application of distributed e-ledger technology.

5.3.2 Types of Blockchain

Public, Private, and Hybrid blockchains are the three most common types of blockchains. The permission standard is used to separate the many blockchains.

5.3.2.1 Public or Permissionless

Blockchains are decentralised, distributed, and public, which means that anyone can publish a block like the one illustrated in fig. 1. Permissionless blockchain networks are accessible to anyone, regardless of their physical location (Zhang, 2019). All that is required is access to the internet and the necessary software to run the blockchain network. Furthermore, all connected users have the authority to write data onto the blockchain, and their consent is required before any data is stored in the database (ledger). Bitcoin is a popular example of a public blockchain (Sharma, 2018). This e-currency allows users to conduct transactions directly between themselves without the need for a middleman such as a bank. Permissionless Blockchain has a few pros and disadvantages.

Advantages:

- Global accessibility

; • True decentralisation and transparency.

Why Because the rules of blockchain intended for security persistence are public, hostile assaults are substantially more common in open blockchain networks, necessitating even greater computational power to assure security and authenticity.

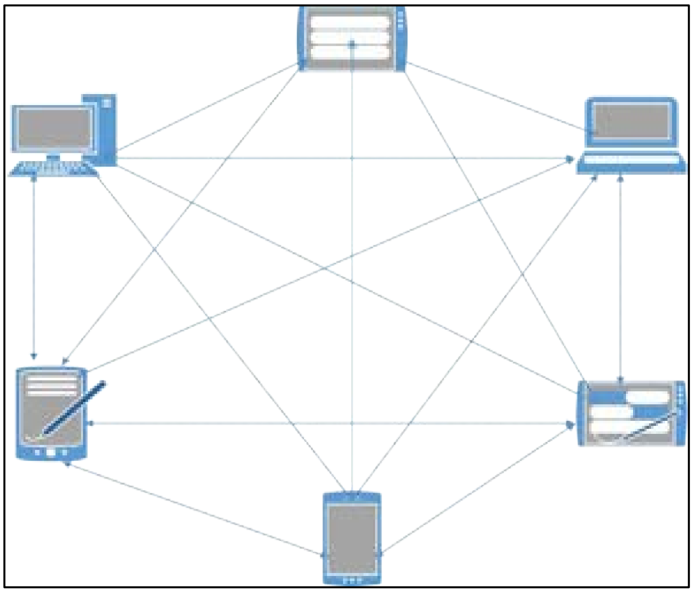


Figure 5.1 A Public Blockchain

5.3.2.2 Private or Permissioned

Blockchains are distributed networks with centralised or decentralised governance that allows for the adding of blocks to the chain and ledger access. Ledger records are used to track transactions. Because the number of malicious attacks is extremely low, the mining model used in private chains does not necessitate the deployment of high computational power to ensure authenticity and security. Furthermore, all users' identities are directly or indirectly known to the members of this exclusive network. Instead of a single organisation acting as the authorised entity to oversee the chain's complete processing and functionality, select specific nodes, or users, are given this power, which can be renewed on a regular basis. Consortium blockchains, despite of their popular use, are partially centralised and more efficient than public chains. Organizations that want a more rigorous and strong mechanism to secure their (exclusively) shared information, for example, employ permissioned blockchain systems. Permissioned blockchain networks can also be employed in organisations that choose, wish, or are compelled to operate together but do not completely trust each other with sensitive data if an individual regulates the publishing of blocks.

Permissionless Blockchain has a few pros and disadvantages.

- Less computing power;
- Fewer malicious assaults;
- Faster than public blockchains.
- The Private or Permissioned form of blockchain is partially transparent because only a few members of the organisation or a single user have unlimited access to the chain, which could lead to the possibility of infiltration.

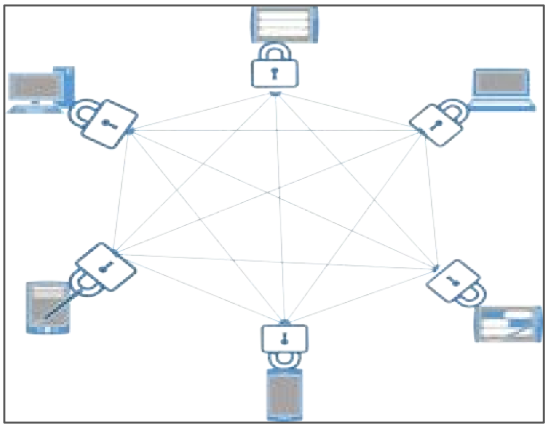


Figure 5.2 A Private Blockchain

5.2.3 Hybrid

Blockchains combine the security and transparency benefits of a public blockchain with the privacy benefits of a private blockchain. The ability for health-related companies, for example, to preserve data segregated as public and private information, thanks to the combination of public and private blockchain. Hybrid chains connect to other private and public blockchains, allowing hybrid blockchains to be used in more places (Sagirlar, 2018). 'Dragon Chain' is the name of a well-known hybrid blockchain.

5.3 RSA

Rivest–Shamir–Adleman is referred to as RSA. It's a widely used asymmetric cryptographic technique for message encryption and decryption (Minni, 2013). A public key and a private key are returned. The RSA algorithm is predicated on the notion that factoring a big integral value can be challenging (Siahaan, 2016; Islam, 2018). The public key is made up of two numbers, one of which is the result of multiplying two rather large prime numbers (Islam, 2018). The private key is made up of the same two prime numbers (Mustafa, 2018). The public key is made up of two numbers, one of which is the result of multiplying two reasonably large prime numbers (Islam, 2018), and the private key is made up of the same two prime numbers (Mustafa, 2018). As a result, factorising a large prime integer is required to compromise the private key. As a result, encryption durability is determined by the key size, or length of the key, and as the key size is doubled or tripled, the strength of encryption increases exponentially, making the strength and size directly proportional. In the blockchain, there are two sorts of keys: The public key, as the name implies, can be published publicly, and the blockchain ledger records its entries against the user's public key, but the private key is designed to be kept private. The public key is used to encrypt the message or data that has to be exchanged, and the private key is used to decrypt it. Both the public and private keys are produced using RSA methods. A private key is typically 256 bits long, while a public key is typically 2048 bits long. Private keys are faster than public keys due to their reduced size.

5.4 SYSTEM ARCHITECTURE

In the next section we have shown the basic architecture used in the proposed approach for the theft prevention.

5.4.1 Architecture Block Diagram 1: Authentication

The user will authenticate with an email address and a password; these will be encrypted and saved in the database, along with a produced set of keys (public key and private key) that will be given to the user along with the token. Fig. 5.3 depicts the architecture.

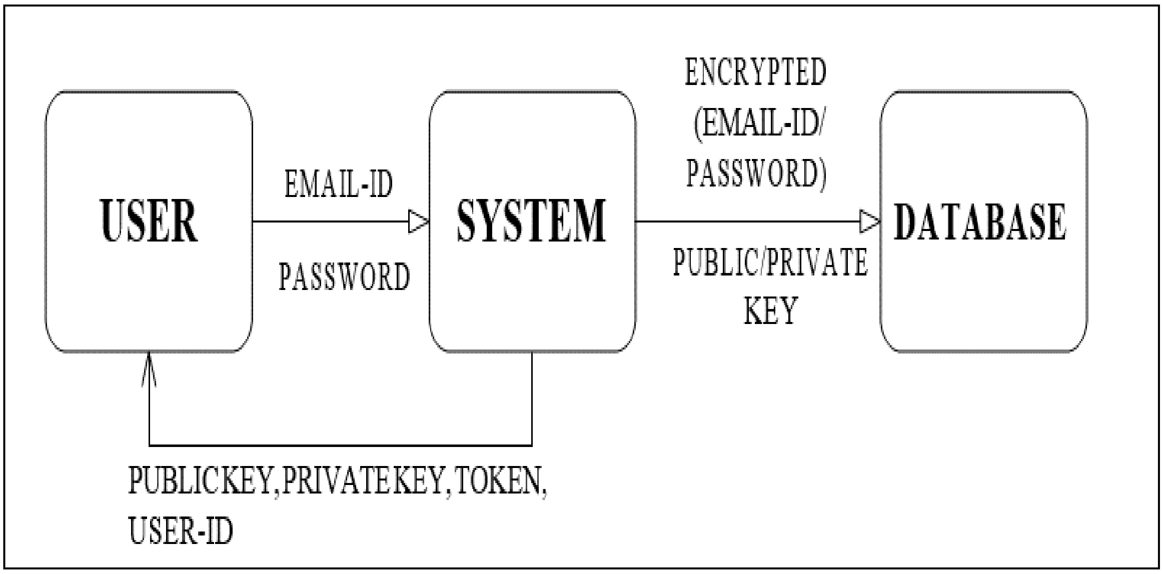


Figure 5.3 Authentication Process

5.4.2 Architecture Block Diagram 2: Creating Block

The user will supply transaction data, such as the organ(s)/unit(s) of blood group requirements, as well as a private key. The application will submit a private key and an authentication token to the backend server, which will compare the private key to the private key of the token's associated user. The system will generate a block with ID, index, previous hash, current hash, data, and nonce if they match. (Note: For the Genesis block, the prior hash is zero, and the hash obtained by mining acts as the previous hash for subsequent blocks.). A block will be added to the chain after it has been successfully created, i.e. after mining. Following that, the password will be generated and stored in encrypted format in the block's database, along with data encryptions and the creator's email address. At the moment of creation, the password, as well as other block-related information, will be displayed to the user in decrypted format. Figure 5.4 depicts the architecture.

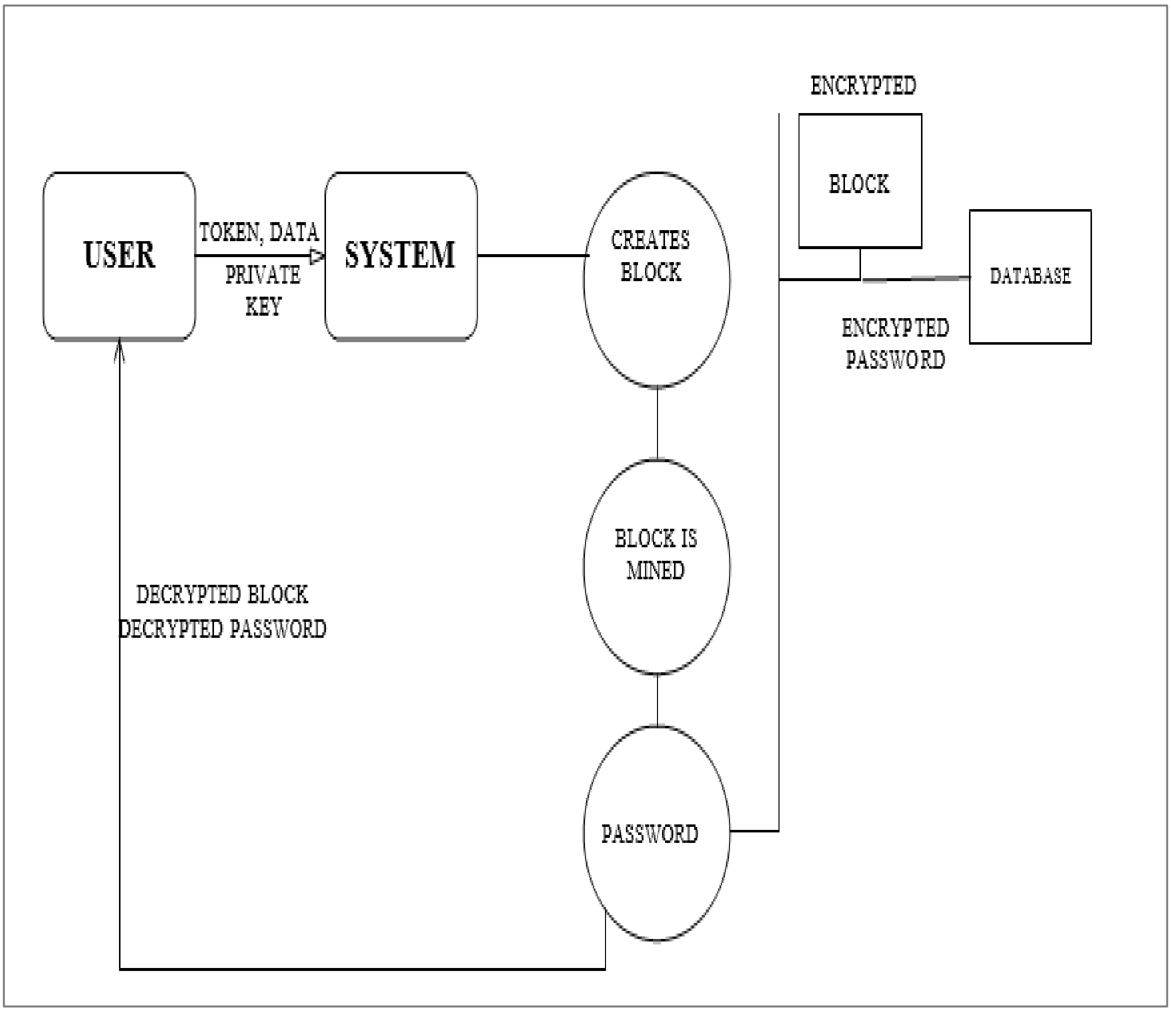


Figure.5.4 Creation of Block for Blockchain

5.4.3 Architecture Block Diagram 3: Public Ledger

The user will supply a private key, which the application will send to the backend system along with an authentication token. The ledger's information will be displayed to the user after successful key verification. Meanwhile, an asynchronous procedure will run to cross-check all of the blocks to see if their creator and accessing user are the same, in which case the decrypted password belonging to those specific blocks will be displayed; otherwise, all information will remain encrypted. Figure 5.5 depicts the architecture.

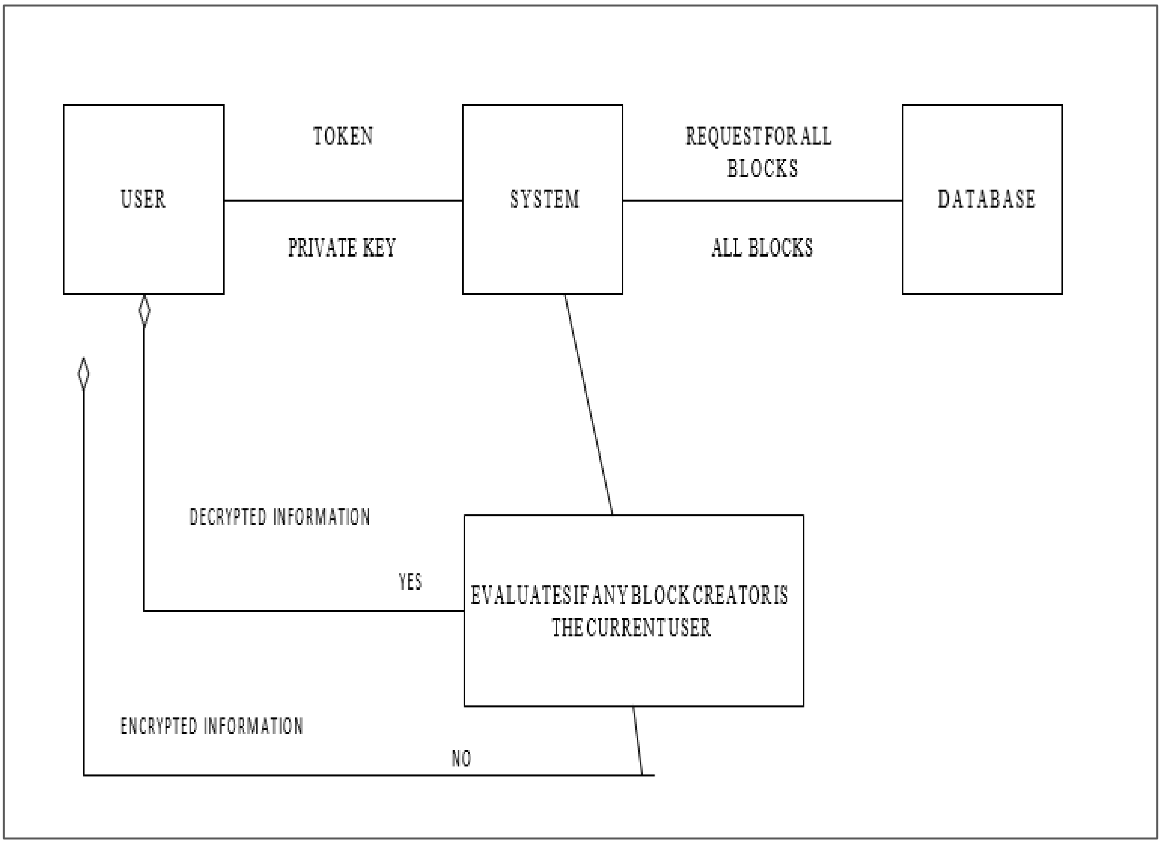


Figure 5.5 Request to Public Ledger

5.4.4 Architecture Block Diagram 4: Request Access of Safe

The user will enter his authentication credentials and block ID into an IOT Device connected to the backend server, which will issue a post request for the credentials entered to the appropriate API endpoint.

The system will verify credentials and grant access to blockchain only to authorised users, after which the block ID entered will be checked against all blocks created by the current user, if a match is found, the user will be asked to input the password corresponding to that particular block, if this password and the one generated at the time of block creation (stored in encrypted form) match, the user will be asked to input the password corresponding to that particular block. The block's credentials are kept in an encrypted manner in a database.

2. Only three unsuccessful transactions per block ID are valid; otherwise, the block would be permanently flagged for unauthorised access and a security breach would occur.

Block is a constructor/class function with three parameters.

The block's index is called the index.

Data: The information that will be stored within the block.

PrevHash: The hash of the chain's prior block.

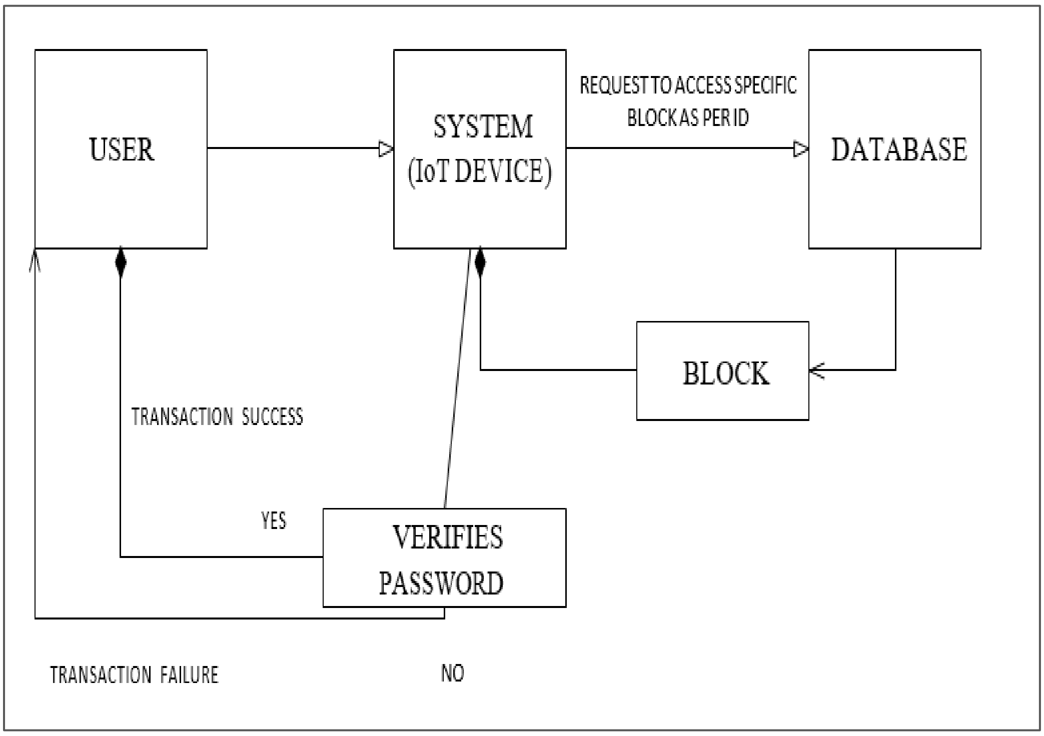


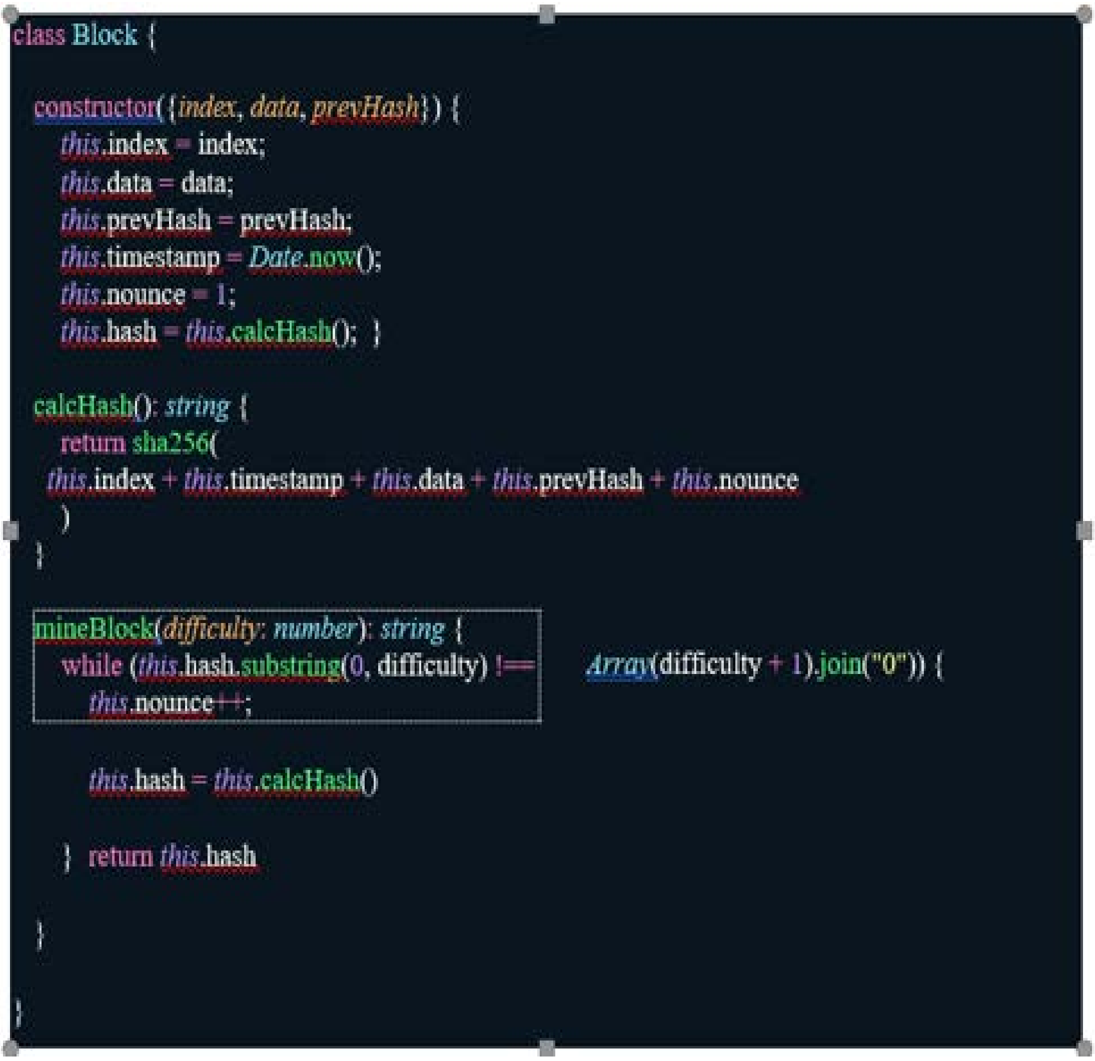
Figure.5.6 Request to access safe

We have implemented the function using JavaScript, and for ease of working, nonce value is hardcoded to 1.

Hash function uses:

- index
- timestamp
- data
- prevHash
- nonce

To create the hash value for the current block using the SHA256 algorithm. For ease of workflow, custom mining action is attached to the block which carries out the mining action as shown in the script.



```
class Block {

  constructor({index, data, prevHash}) {
    this.index = index;
    this.data = data;
    this.prevHash = prevHash;
    this.timestamp = Date.now();
    this.nounce = 1;
    this.hash = this.calcHash();  }

  calcHash(): string {
    return sha256(
   this.index + this.timestamp + this.data + this.prevHash + this.nounce
    )
  }

  mineBlock(difficulty: number): string {
    while (this.hash.substring(0, difficulty) !==      Array(difficulty + 1).join("0")) {
      this.nounce++;

      this.hash = this.calcHash()

    }  return this.hash

  }

}
```

Figure 5.7 (a) Creating the Hash functions

The created block function takes in the following parameters

index

data

prevHash

On passing the following information to the Block class, a custom block is returned, and it is stored in a variable: toAddBlock. if prevHash i.e. previous hash, is 0 then the block is returned as the genesis block, else the mining action takes place to ensure the validity of the information passed in the block, if the information is valid, then the block is returned else **false** is return, which means that the block is invalid.

```
type TCreateBlock = {
  index: string;
  data: string;
  prewash: string
```

```
}
const createBlock = (blockInfo: TCreateBlock) => {
  const toAddBlock = new Block(blockInfo)
  if (blockInfo.prevHash === "0") {
     // genesis block
     return toAddBlock
  } else {
          // mineBlockTakes in difficulty value

     const returnedHash = toAddBlock.mineBlock(2);

     return returnedHash === toAddBlock.hash ? toAddBlock : false

  }

};
```

Figure 5.7 (b) Creating the Hash functions

So, using proposed method we have secure the network for theft of blood rare group and human organs.

5.4 Conclusion

Diverse work is being done around the world to broaden the scope of blockchain. Though it has been applied in a variety of fields other than finance, including healthcare and security, as well as a number of others that have yet to be discovered. The current concept of using blockchain as a second layer of security for creating passwords and assuring secure transactions of extremely valuable commodities such as human organs and blood groups. Theft could be reduced to a manageable level by implementing such a technique.

CHAPTER 6

PRIVACY PRESERVATION IN BLOCKCHAIN NETWORK USING TENSOR PRODUCT AND A HYBRID SWARM INTELLIGENCE

6.1 Introduction

Electronic medical records (EMR) have grown in popularity as a means of improving diagnosis accuracy, however privacy and security are still concerns in this EMR. Block chain has been established as a major technique to access personal health information (PHI) in the past, supported by privacy protection and security preservation due to the immutability features. Sharing health-care data has a number of advantages, including maximising knowledge of trends and patterns in public health care as well as diseases to determine effective medical quality care (Bordea, 2015), providing doctors with useful information to provide better treatment recommendations, and making the best use of national health-based service budgets for a variety of reasons (Bordea, 2015). (Zhang, 2016). Medical data is dispersed among various medical institutions, with data standards that differ from one another, resulting in limited intractability of medical records. The existing database system of a medical institution does not ensure the reliability and integrity of patients' medical records. As a result, data loss was unavoidable, resulting in data theft and personal privacy breaches. Furthermore, medical records are kept in a centralised location, making them exposed to risks such as malicious assaults, hacking, and natural catastrophes, which can result in the loss of medical data.

A secure data sharing infrastructure is required to safely share medical records among companies. Privacy, security, and interoperability are just a few of the issues that must be addressed. To begin, highly sensitive electronic medical records are stored in a centralised framework and maintained on public clouds. This exposes it to a high level of danger, necessitating the use of authenticated access. Furthermore, efficient medical record integration and interoperability among medical organisations is a difficult undertaking. The fact that patients/users do not have access to their own medical records added to the challenge. (Liang, 2017) Due to the healthcare industry's numerous constraints and challenges, a secure and confidential authorised system to store, process, and access patients' medical records is required. As a result, security refers to the protection of sensitive medical data from intruders and various listeners (Omar, 2017). A blockchain-based solution is proposed to maintain control and security over sensitive medical data. Blockchain has been used in various approaches to achieve privacy and security, such as multi-signature, message encryption, energy trading, and others, to securely manage medical records and to enhance the security and safety of trading data in a decentralised environment of smart grid energy trading. medical records for multiple users (Hussein, 2018). (2019, Zhu). In, the literature, several applications in the healthcare industry have been focused using blockchain (Omar, 2017; Yue, 2016; Shrier, 2017; Xia, 2017; Peterson, 2016). Existing approaches confront a few issues in the literature, such as:

- Health-care systems necessitate an efficient technique for collecting, storing, and determining healthcare data while remaining compliant with privacy regulations. These types of platforms lack some basic security safeguards, resulting in a number of data breaches, exposing users to economic dangers, social stigma, and mental stress difficulties (Yue, 2016).
- Several types of medical data are collected and maintained in a centralised manner in clinical institutions, and they are vulnerable to a variety of risks, including malicious attacks, hacking, and natural catastrophes, all of which can result in the loss of medical data (Chen, 2019).
- Block chain-based data sharing has been included in the system to guarantee data privacy through the immutability and autonomy of the block chain's features (Yue, 2016). The use of block chain-based techniques has some drawbacks, such as access control leaks and immutability. The mechanisms based on the key-theft/loss and the techniques based on the key distribution were unable to handle (Omar, A et al., 2019).
- • The processing time was longer in this case (Hussein et al.).
- • Medical data privacy and legislative criteria are not being met (Dagher, et al., 2018).

- • In (Tian, et al., 2019), the communication cost is linearly increased. In a real-world setting, (Zhu et al) does not process.
- • Systems based on centralised data management do not analyse medical data with integrity. The information about the patients is stored in a medical repository in these systems, where a hacker can remove or edit the data once the database is accessed (Tian, 2019).
- • The controllable block chain data management (CBDM) model was developed to provide privacy protection in clinical-based data using block chain methods (Zhu, 2019). It is considered a secure platform because all system participants' actions are recorded in the chain, and then expanding the block chains to modify without analysing the blocks makes it computation.

  Personal data loss, particularly medical data loss or privacy leaks, can lead to a variety of hazards, including hostile acts, hacking, and natural calamities. Clinical data is centralised in clinical institutions, making it more vulnerable to a variety of challenges such as attacks, natural disasters, and hacking, all of which can result in the loss of medical data. Patients can download data records, which have been encrypted and decrypted before, and then preparations for sharing the downloaded data can be made. During data sharing, the data is encrypted several times, with the decryption keys and ciphertext being given to the receiver each time. As a result, the chapter's goal is as follows:

  1. What is the most efficient way to obtain blockchain input data?
  2. How are tensor vectors calculated and used in a way that does not degrade utility?
  3. Where can I find an objective assessment of the optimization criteria?
  4. How is performance reviewed in order to achieve better results?

However, in today's modern scientific period, there is a need to tackle complex problems with high accuracy and efficiency, which has led to the development of artificial intelligence. Only machines were previously educated for various applications such as robotics, text to speech converters, and others. Nature's biological features have been used to derive intelligence in recent years. These characteristics have evolved from numerous groups of birds, insects, and mammals known as swarms, and the behaviour is referred to as swarm intelligence (Beni, 1989; Millonas, 1994; Bela, 2006). It has a variety of real-world uses. Beni and Wang proposed it for the first time in 1989. (Beni, 1989). Swarms have two highly intriguing properties: navigation and foraging, through which they combine numerous local optimization rules to attain global optimum solutions.

As a result, a block chain-based technique based on tensor product and a hybrid swarm intelligence-based (DragonFly algorithm and Crow search algorithm) generation is developed for privacy protection. The raw data matrix and the solitary and utility (SU) coefficient were multiplied using the tensor product, and the blockchain data with mixed qualities was initially exposed to the privacy preservation method As a result, the SU coefficient's derivation, which takes into account both sensitive information and utility, was stated as a searching problem. After that, the proposed algorithm for calculating the SU coefficient was presented.

The following are the contributions of this research to the preservation of privacy:

• Creating a DragonFly-Crow Search (D-CS) model with a novel objective function for determining the best SU coefficient. The Dragonfly Algorithm (DA) and the Crow-Search Algorithm (CSA) were combined to create the D-CS (CSA). As a result, the SU coefficient's derivation handles both utility and sensitive information.

Where the input data matrix and SU coefficient for tensor operation are given, generating the tensor product for transforming the original data into protected data without breaching the utility.

6.2Swarm Intelligence

Swarms are a large group of homogeneous insects which exchanges information locally to attain global optimum solution. Common examples of swarm include swarm of ants, bees, dragon flies and flock of birds such as crows. They have some common behavioural patterns such as Navigation and Foraging.

The best examples of navigation are birds which migrate easily and intelligently. Birds saves high amount of strength due to V-shaped flight configuration (Zhang, 2016). Foraging is another important behaviour. Foraging necessitates group activity, which ants and bees excel at since they imprint the quickest path from food source to hive/nest (Liang, 2017). They use pheromone deposits to identify the route they take in quest of food. The more pheromone deposits there are, the better the path to go in quest of food.

They used the pheromone deposits to inform and guide other members of their community.

Such outstanding and effective behaviours have evolved over ages, and as a result, they have become the most popular solution for completing our daily duties.

6.2.1. Working Principle

Craig Reynolds first developed and recreated swarm behaviour and movement in 1986, using three simple rules that they move in the same direction and stay close together to avoid colliding with their neighbours.

Swarms obey some basic operating principles in addition to these guidelines, such as:

The Proximity Principle states that swarms should be able to compute the proximity of their objective. principle of diverse response states that swarms should appropriately spread their resources so that they are not vulnerable to specific environmental conditions Principle of stability and adaptability – Swarms adapt to their surroundings in order to stay stable.

Swarms interact locally with one another through self–organization and emergence, resulting in a fully coordinated system as a whole

.6.2.2. Swarm Intelligence Based Algorithms

6.2.2.1. Dragonfly Algorithm

Odonata is another name for dragonflies. Each dragonfly's life cycle is divided into two stages: nymph and adult. They spend the majority of their lives as nymphs, undergoing metamorphosis before becoming adults (Thorp, 2014). They have two primary functions: static swarms are used for hunting, while dynamic swarms are used for migration. Static swarms are small groups of insects that fly back and forth over a short region in search of other flying prey like butterflies and mosquitoes (Wikelski, 2006). Static swarms are distinguished by their limited movements and sudden changes in flight route. Migrating swarms, on the other hand, migrate in one direction over great distances.

6.2.2.2. Crow Search Algorithm

Crows, often known as corvids, are the smartest birds on the planet. They displayed various examples of their dexterity. Self-awareness is first seen in mirror testing. Second, they have the ability to create tools. Finally, they recall faces and issue warnings when a hostile individual approaches (Rincon; Prior, 2008). Other intriguing facts about crows include the fact that they observe other birds' behaviour and where they hide food in order to grab it when the owner of the food leaves. Clayton (Clayton, 2005).

6.3 Structure of Blockchain

Blockchains are a type of data structure that has a chain shape and is linked together by a hash value-based address pointer. Block chains are a decentralised, distributed, shared state machine in which each node maintains its own copy of the chain, with transaction processing determining the current state. The hash blocks from earlier block chains, the current hash block, the nonce ("number used once"), the hash of numerous transactions (Merkle root), the data transaction, and the timestamp are all included in every block in the block chain. A block chain is a distributed database or public ledger where transactions are validated and digital-based events are safeguarded and chronologically connected in data blocks. The newly created records plus the data given by the transaction initiator make up the so-called data block. Furthermore, each block is identified by timestamps and preceding hash blocks, indicating that the data in the block chain is absolute and visible. After obtaining consensus with 51 percent of the users in the distributed network, block chains are added to the legitimate blocks Furthermore, a distributed P2P network with nodes that keep a similar copy of transaction records provides robustness and resistance to attacks and single-point-of-failure. As a result, block chains have become popular in a variety of fields.

6.3.1. Blockchain Network Bridge: The block chain network bridge with a single node is made up of block chain services, block chain wallets, bridge-based sensors, and bridge-based machines, which are characterised as follows:

6.3.2 Blockchain Service*:* The data grid's distinguishing feature is that it provides exceptional quality-based services. The most important industrial areas considered in the block chain, in terms of industrial growth, are software-based services and information technology. Services based on information technology and software goods, such as the integration-based system, were used by block chain providers.

6.3.3 Blockchain Wallet: The private keys for each account are assigned to the block chain wallet, which consists of private keys. The master key, also known as the random key, and the standard-based advanced encryption are used to encrypt this type of private key. For peer-to-peer transactions, a combination of private and public keys is utilised to create a digital-based signature. For example, the elliptic curve digital signature technique (ECDSA) is used by Bitcoin for privacy sharing, encryption, and cryptography based on threshold measurements.

6.3.4 Sensor Bridge: Actuators and sensors are required for sensing-based services. The electrical-based and optical-based signals are detected and responded to using a sensor device. This gadget is capable of transforming physical characteristics such as temperature, humidity, speed, and blood pressure into electrically measurable signals. Controlling or moving the system requires the use of an actuator. After the sensing process, the block chain data are generated from the bridge-based machine.

6.4Research Methodology

6.4.1 Proposed Privacy Preservation

The block chain structure's system model is depicted in Fig. 6.1. Consider how many hospitals in the city have come to an agreement to join a league in order to share patient health records. The data security of the system can be improved by constructing two types of block chains: consortium-based block chains for hospitals and privacy-based block chains for each hospital. The PHI of the patients visited is collected and saved in privacy-based block chains, whereas in consortium-based block chains, the PHI keywords are stored in the alliance by all the institutions.

The services of the blockchain, the wallet of the blockchain, the bridge-based sensor, and the bridge-based machine process the blockchain-based networks. As a result, the data in the blockchain are the results of the bridge-based block chain network, which are subject to privacy preservation. Privacy maintenance is achieved via D-CS, which is a CS/DA integration (Chandrasekar, 2020). DA is better in solving single-objective optimization problems, but CSA is better at finding optimal solutions to a variety of optimization issues. They are easy to implement, have a small number of parameters, and are adaptable. The proposed D-CS algorithm is given for blockchain-based privacy maintenance. By merging DA (Mirjalili,2016) and CSA, a new algorithm named D-CS was developed (Askarzadeh, 2016). The privacy and utility factors are considered in the objective evaluation of the optimization criteria.

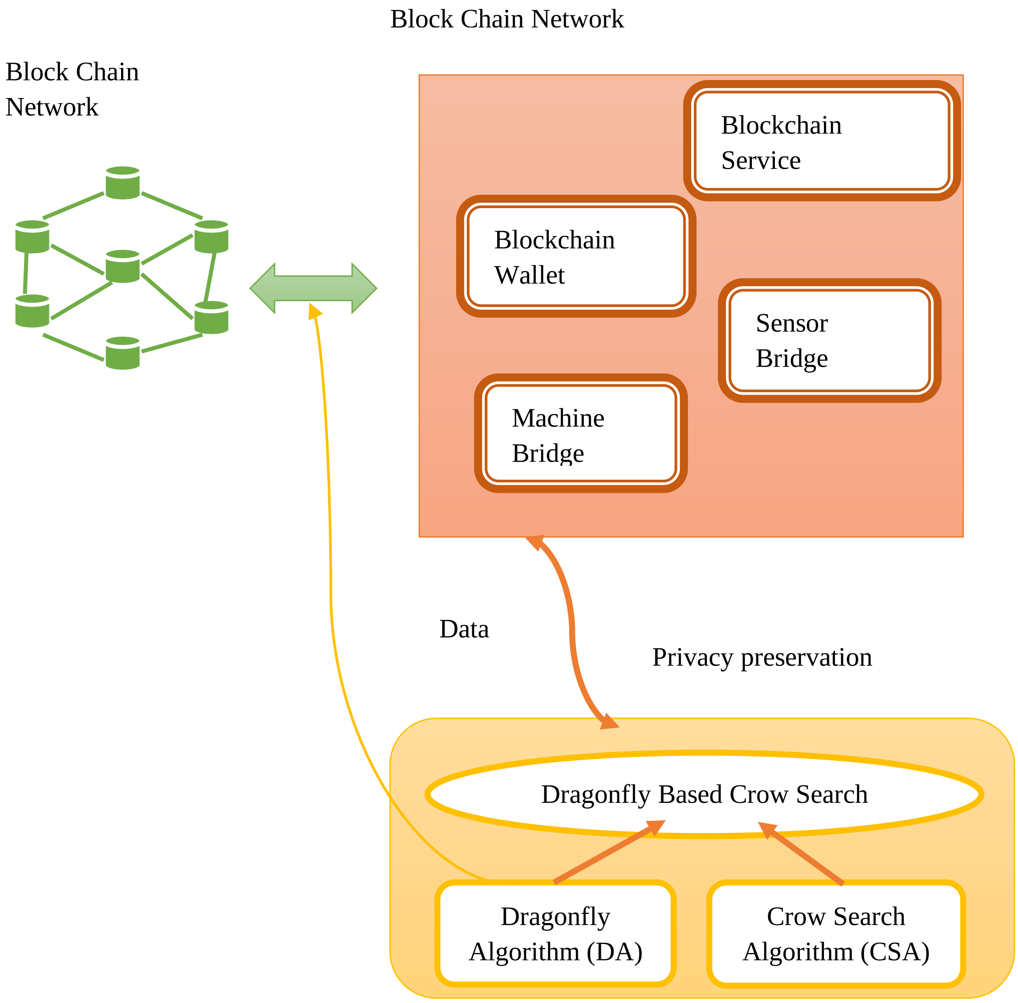


Figure. 6.1. A System model of blockchain with privacy

Overall, the established privacy protection strategy consists of two key components. The SU coefficient is optimally found using the D-CS method with the new goal function in the first phase. The input data matrix and SU coefficient are multiplied by a tensor product operation in the second phase to turn the original data into protected data without breaking the utility. The block diagram of the privacy preservation strategy is shown in Figure 6.2.

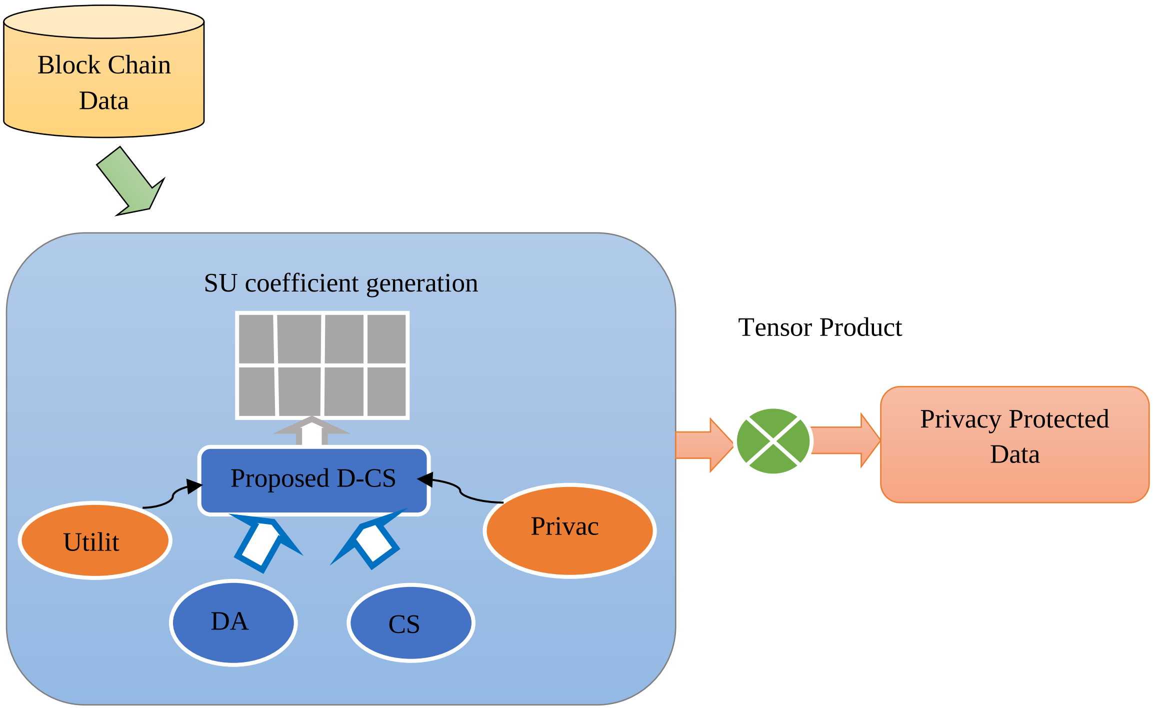


Figure. 6.2. Block diagram of blockchain-based privacy preservation using proposed D-CS technique

6.4.2 Privacy Preservation

Assume that the blockchain data input is denoted as B along with the several attributes represented as:

$$Data_{p\times q} B = \{b_{xy}\}; (1 \leq x \leq m); (1 \leq y \leq v) \qquad (1)$$

where b_{xy} represents the x^{th} data record in the y^{th} attribute; m is the overall data points; and v denotes the total attributes for every data point. Then, blockchain data key matrix is given by:

$$_{p\times q} D = B + k \qquad (2)$$

where k denotes the key; and symbol $+$ represents the element-wise multiplication. The key k is expressed as $k = \sum_{x=1}^{m} b_{xy} * l ; 1 \leq l \leq z$ (3)

After generation of the key, the data square matrix (DSM) is computed using the following expression: ${}_{m\times m}R = D.D^{T}$ (4)

The data matrix and solitude and utility (SU) coefficient are then multiplied through the tensor product via the tensor vector, which is expressed as

$$\backslash_{r\times 1} H = SU_{m\times 1} \otimes S_{x(m\times 1)} \quad (5)$$

where $\otimes$ denotes the tensor product; and SU represents the SU coefficient, which is generated using the proposed D-CS model. After that, the privacy-protected data are obtained, and the privacy-protected data column is given by:

$$J_{y} = H \bullet D_{y} \quad (6)$$

where the matrix multiplication is denoted as $\bullet$; and m elements are taken for the tensor vector H. Consequently, the secret key is generated by concatenating the tensor vector and the key using the formula:

$$_{(r+1)\times 1}R_{i} = H \| k \quad (7)$$

Finally, the data are retrieved using the expression:

$$D_{y}^{*} = \frac{J_{y}^{*}}{R_{i_{r\times 1}}^{*}} \quad (8)$$

where $R_{i_{r\times 1}}^{*}$ is the secret key from which $r \times 1$ is considered because the concatenated value is not chosen and finally, the original data can be retrieved using:

$$D^{*} = D_{y}^{*} - R_{i_{r\times 1}} \quad (9)$$

6.4.3 Proposed Dragonfly-Crow Search Algorithm for The Generation Of SU Coefficient

The proposed D-CS for obtaining the SU coefficient is briefly discussed in this section. D-CS was created by merging DA (Mirjalili, 2016) and CS (Askarzadeh, 2016) to discover the optimum solution based on the heuristic qualities of a dragonfly, as previously indicated. According to DA (Mirjalili,2016), a dragonfly moves from one area to another at different speeds depending on five factors: separation, alignment, cohesion, attraction in the direction of a food source, and opponent distraction. The survival of dragonflies is influenced by several factors. The DA uses weight parameters ranging from 0 to 1 for each factor, hence improving convergence The DA, on the other hand, is inspired by the dragonfly's natural behaviour and movement, which varies during the iteration. In order to search and identify their prey with respect to their memory, the typical CS, a population-dependent optimization, relies on the clever crow behaviour. Crows' intelligence is demonstrated by their mirroring the behaviour of other crows to allocate food by following their neighbours. They can also recall the prior food location. As a result, CSA is based on the behaviour of crows and their search mechanism, with customizable parameters like awareness likelihood and flight length. The decision variables, objective functions, restrictions, and intensification and diversification control of CSA are used to tune these parameters. Furthermore, the method effectively exposes a superior trade-off between the phases of diversification and intensification with a high convergence rate, implying a short computing time. The following are the steps involved in the D-CS algorithm:

Step 1: Initialization

The dragonfly population is first initialized to choose the best position and is expressed as:

$$Y = \{Y_1, Y_2, \ldots, Y_j, \ldots, Y_u\} \tag{10}$$

where Y_j signifies the location of the j^{th} dragonfly in the solution.

Step 2: Calculate the objective function

The fitness function must then be calculated in order to find the best-based result. The best location is generated by evaluating the optimal solution in the final iteration. The fitness function's expression is as follows:

$$Fitness(f) = \frac{1}{2}[(1 - I_{loss}) + A] \tag{11}$$

where I_{loss} denotes information loss, and A is accuracy.

Step 3: Position update using dragonfly crow search algorithm

The DA algorithm is used to solve binary and multi-objective problems and is inspired by the dynamic swarming behaviour of dragonflies. The algorithm outperforms previous algorithms by handling challenges based on unknown search areas and overcoming optimization issues. As a result, the researchers chose this technique to overcome the challenges produced by open-source optimization tools. For the randomly initialised generalisation level and cluster size, the position of the records is changed and updated using:

$$Y^{j}_{\tau+1} = Y^{j}_{\tau} + \Delta Y^{j}_{\tau+1} \tag{12}$$

where $\Delta Y^{j}_{\tau+1}$ denotes the change in the position of the records. The expression for the record change is represented as:

$$Y^{j}_{\tau+1} = Y^{j}_{\tau} + \left(eN_j + fO_j + dM_j + hQ_j + gP_j\right) + \varpi \Delta Y^{j}_{\tau} \tag{13}$$

where N_j refers to the separation of records; O_j signifies the alignment; M_j is the cohesion of records; Q_j represents the attraction towards food source; and P_j indicates the location of enemy records. The position of the record and neighboring record gets changed for each factor, separation, alignment, cohesion, attraction, and enemies' location, and the expression is given as:

$$N_j = -\sum_{n=1}^{L} \left(Y_j - Y_n\right) \tag{14}$$

Where Y is the current individual location; Y_n represents the n^{th} neighbouring individual location, and L represents the total amount of individuals and T_n indicates the n^{th} neighbouring individual velocity. The alignments O_j and cohesion M_j is calculated as in equations (15) and (16),

$$O_j = \frac{\sum_{n=1}^{K} T_n}{K} \tag{15}$$

Attraction towards the food source Q_j and outward distraction from enemy P_j is calculated by equations (17) and (18),

$$M_j = \frac{\sum_{n=1}^{K} G_n}{K} - G_n \tag{16}$$

Where, G_n is the current position of the individual, K denotes the number of neighbourhoods, G^{α} denotes the location of the food source, and the location of the enemy is represented as G^{β}. The updated equation is expressed as:

$$Q_j = \left(G^{\alpha} - G_j\right) \tag{17}$$

$$P_j = \left(G^{\beta} - G_j\right) \tag{18}$$

Where G^{α} denotes the location of the food source; and the location of enemy is represented as G^{β}. The updated equation is expressed as:

$$Y_{\tau+1}^{j} = Y_{\tau}^{j} + s_j \times E_{\tau}^{j} \times \left(v_{\tau}^{a} - Y_{\tau}^{j}\right) \tag{19}$$

$$Y_{\tau+1}^{j} = Y_{\tau}^{j} + s_j \times E_{\tau}^{j} v_{\tau}^{a} - s_j \times E_{\tau}^{j} Y_{\tau}^{j} \tag{20}$$

$$Y_{\tau+1}^{j} = Y_{\tau}^{j}\left(1 - s_j \times E_{\tau}^{j}\right) + s_j \times E_{\tau}^{j} v_{\tau}^{a} \tag{21}$$

$$Y_{\tau}^{j} = \frac{Y_{\tau+1}^{j} - s_j \times E_{\tau}^{j} v_{\tau}^{a}}{1 - s_j \times E_{\tau}^{j}} \tag{22}$$

where $Y_{\tau+1}^{j}$ represents the updated location of the j^{th} crow in the next iteration; Y_{τ}^{j} indicates the updated location of the j^{th} crow in the above iteration; the flight length of the j^{th} crow is represented as E_{τ}^{j}; s_j represents the random number of the j^{th} crow, ranging from 0 to 1; and the memory of the a^{th} crow is indicated as v_{τ}^{a}.

Equation (22) is then substituted into equation (13) to integrate CSA and DA:

$$Y_{\tau+1}^{j} = \frac{Y_{\tau+1}^{j} - s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} + \left(eN_j + fO_j + dM_j + hQ_j + gP_j\right) + \varpi \Delta Y_\tau^j \tag{23}$$

$$Y_{\tau+1}^{j} = \frac{Y_{\tau+1}^{j}}{1 - s_j \times E_\tau^j} - \frac{s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} + \left(eN_j + fO_j + dM_j + hQ_j + gP_j\right) + \varpi \Delta Y_\tau^j \tag{24}$$

$$Y_{\tau+1}^{j} - \frac{Y_{\tau+1}^{j}}{1 - s_j \times E_\tau^j} = eN_j + fO_j + dM_j + hQ_j + gP_j + \varpi \Delta Y_\tau^j - \frac{s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} \tag{25}$$

$$Y_{\tau+1}^{j}\left(1 - \frac{1}{1 - s_j \times E_\tau^j}\right) = eN_j + fO_j + dM_j + hQ_j + gP_j + \varpi \Delta Y_\tau^j - \frac{s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} \tag{26}$$

$$Y_{\tau+1}^{j}\left(\frac{1 - s_j \times E_\tau^j - 1}{1 - s_j \times E_\tau^j}\right) = eN_j + fO_j + dM_j + hQ_j + gP_j + \varpi \Delta Y_\tau^j - \frac{s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} \tag{27}$$

$$-Y_{\tau+1}^{j}\left(\frac{s_j \times E_\tau^j}{1 - s_j \times E_\tau^j}\right) = -\frac{s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} - \left(eN_j + fO_j + dM_j + hQ_j + gP_j\right) - \varpi \Delta Y_\tau^j \tag{28}$$

The final updated equation obtained after integrating DA and CS is given by:

$$Y_{\tau+1}^{j} = \frac{1 - s_j \times E_\tau^j}{s_j \times E_\tau^j}\left[\frac{s_j \times E_\tau^j v_\tau^a}{1 - s_j \times E_\tau^j} - \left(eN_j + fO_j + dM_j + hQ_j + gP_j\right) - \varpi \Delta Y_\tau^j\right] \tag{29}$$

Where e denotes the separation-based weight; f is the weight-based on alignment; d represents the weight-based on cohesion; h represents the food factor; g represents the enemy factor; and ϖ represents the weight of inertia.

Step 4: Location update based on levy flight

In addition to the factors mentioned above, the dragonfly also moves from one place to another based on the Levy flight movement, which is expressed as

$$Y_{\tau+1}^{j} = Y_\tau^j + Levy(r) \times Y_\tau^j \tag{30}$$

where $\mathrm{Levy(r)}$ indicates the levy flight with dimension r .

Step 5: Checking the feasibility of the obtained solution

Once the location of the dragonfly is updated, the solution undergoes fitness evaluation, in which the best solution is determined by finding the location with minimum fitness. After that, the optimal solution is replaced by an older solution.

Step 6: Termination

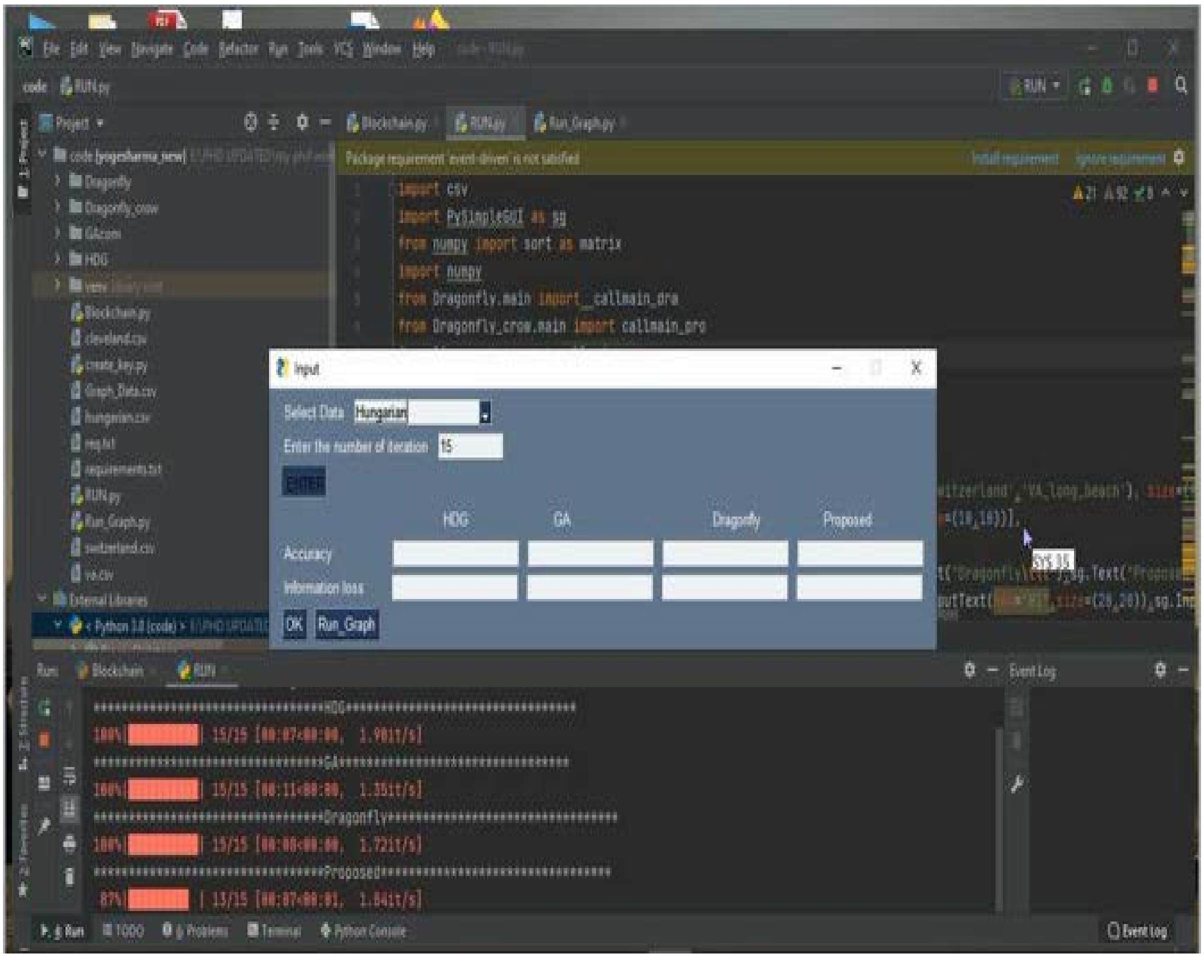
All the previous steps are repeated till the best solution is obtained or it satisfies the condition criteria. Algorithm 1 illustrates the pseudo-code of the proposed D-CS.

Algorithm 1. Pseudo-code of the proposed D-CS approach

```
Input: Dragonfly population $Y = \{Y_1, Y_2, \ldots, Y_j, \ldots, Y_u\}$
Output: Best solution
Procedure:
Begin
Population initiation: $Y = \{Y_1, Y_2, \ldots, Y_j, \ldots, Y_u\}$
Initialize the step vectors of $Y$
While $\tau < \max gen$
Compute the fitness function for all the dragonflies
Update food source as well as enemy
Update the weights
Compute separation, Alignment, cohesion, Attraction, and Distraction
If (solution $j$ has neighbor)
Update the velocity by equation (7)
Update the position by equation (6)
Else
Update the position of the solution by the (29)
End if
End for
End if
End while
 Check the feasibility of obtained solutions
Return the best solution
$\tau = \tau + 1$
  End while
End if
End for
Optimal solution is obtained
End
```

6.5. Implementation

On the PyCharm software, the proposed methodology has been implemented. For the blockchain implementation we have used Ganache environment in order to deploy and use the blockchain for 10 dummy users with their account address and private key for testing of our application. The various implementation processes are depicted in Figure 6.3. (a)-(g). Hungary, Cleveland, Switzerland, and VA long beach are the four datasets where the technique is used. The outcome has been computed after 15 iterations of the operation.



```
import csv
import PySimpleGUI as sg
from numpy import sort as matrix
import numpy
from Dragonfly.main import _callmain_dra
from Dragonfly_crow.main import callmain_pro
```

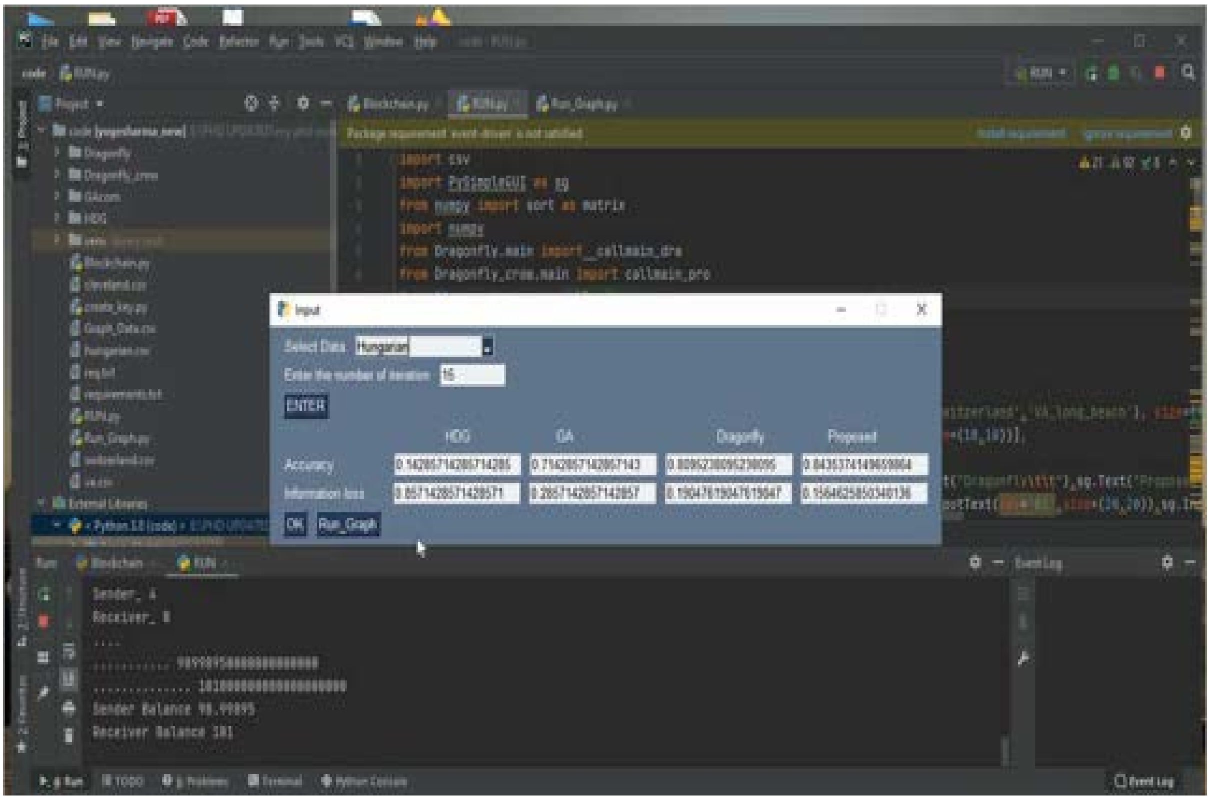
Select Data: Hungarian

Enter the number of iteration: 15

	HOG	GA	Dragonfly	Proposed
Accuracy				
Information loss				

```
*********************************HOG*********************************
100%|██████████| 15/15 [00:07<00:00,  1.98it/s]
*********************************GA*********************************
100%|██████████| 15/15 [00:11<00:00,  1.35it/s]
*********************************Dragonfly*********************************
100%|██████████| 15/15 [00:08<00:00,  1.72it/s]
*********************************Proposed*********************************
 87%|████████  | 13/15 [00:07<00:01,  1.84it/s]
```

(a)



```
import csv
import PySimpleGUI as sg
from numpy import sort as matrix
import numpy
from Dragonfly.main import _callmain_dra
from Dragonfly_crow.main import callmain_pro
```

Input

Select Data: Hungarian

Enter the number of iteration: 15

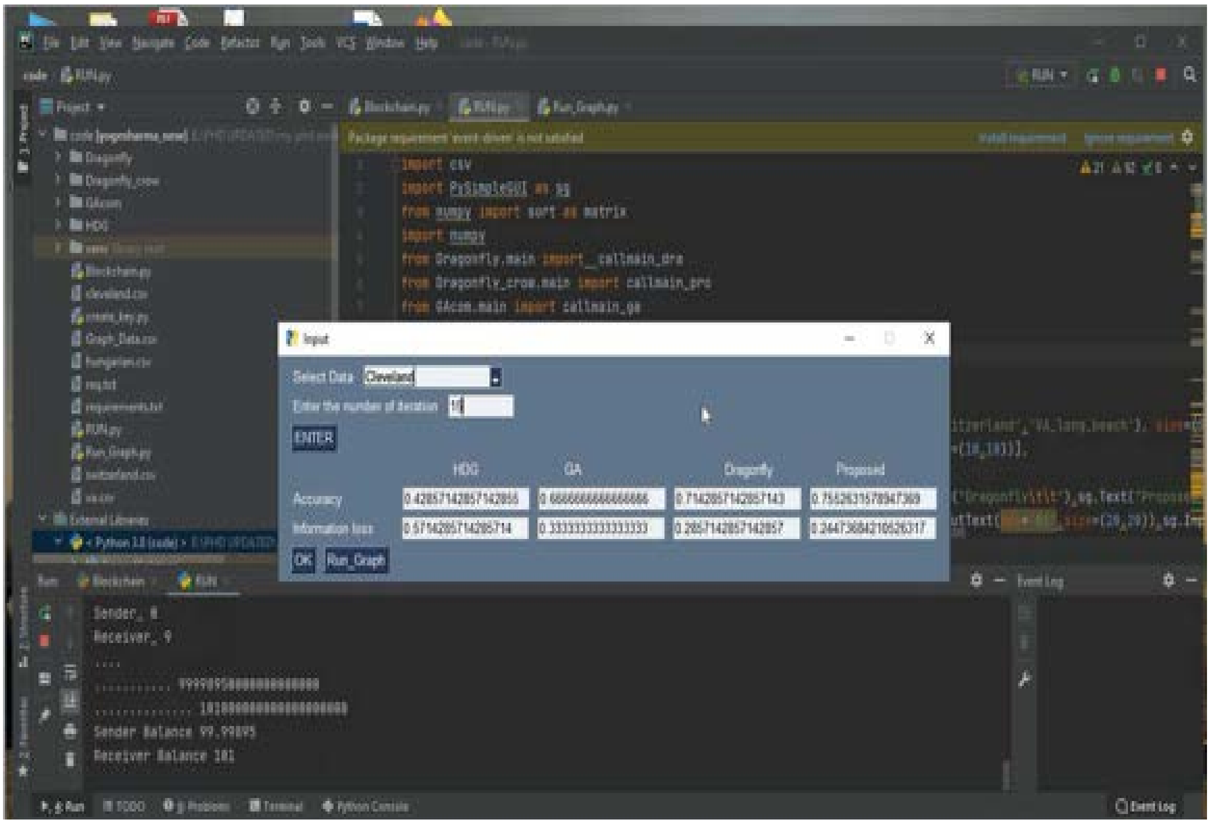
ENTER

	HDG	GA	Dragonfly	Proposed
Accuracy	0.14285714285714285	0.7142857142857143	0.8095238095238095	0.8435374149659864
Information loss	0.8571428571428571	0.2857142857142857	0.19047619047619047	0.1564625850340136

OK Run_Graph

```
Sender_ 4
Receiver_ 8
....
........... 9999895000000000000
............. 101000000000000000000
Sender Balance 99.99895
Receiver Balance 101
```

(b)



```
import csv
import PySimpleGUI as sg
from numpy import sort as matrix
import numpy
from Dragonfly.main import _callmain_dra
from Dragonfly_crow.main import callmain_pro
from GAcom.main import callmain_ga
```

Input

Select Data: Cleveland

Enter the number of iteration: 10

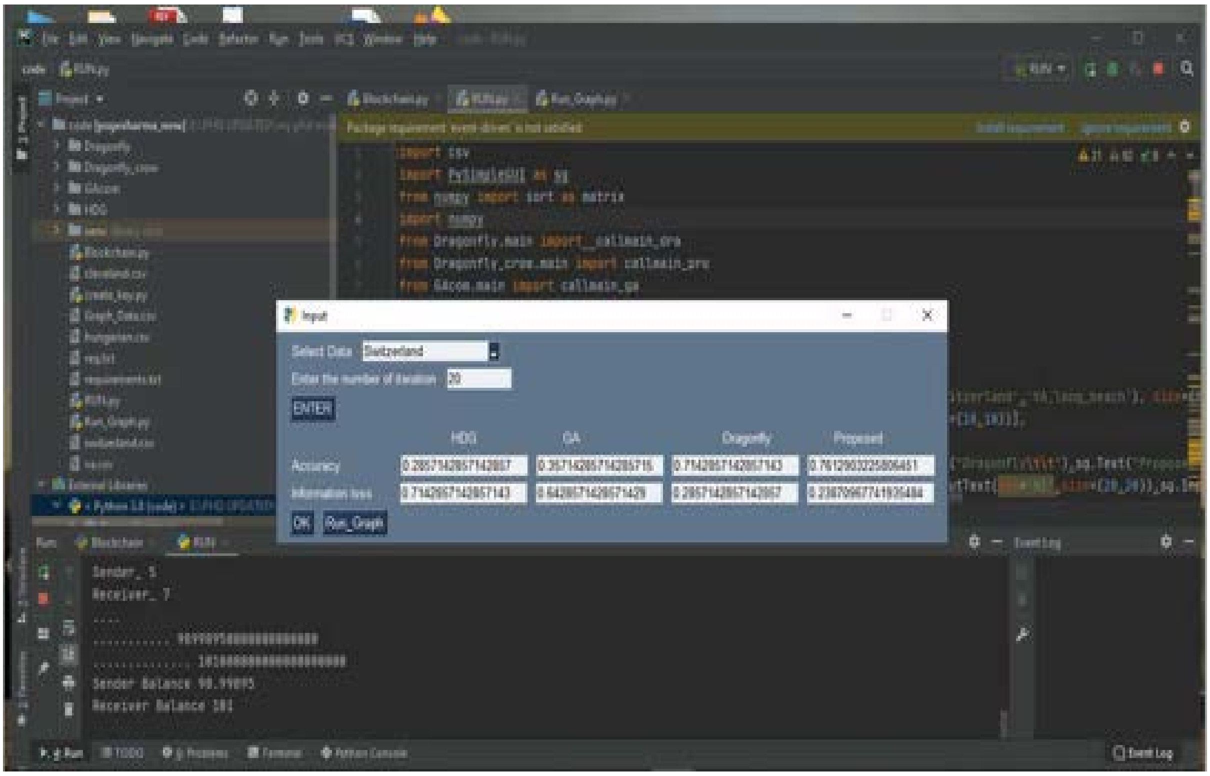
ENTER

	HDG	GA	Dragonfly	Proposed
Accuracy	0.42857142857142855	0.6666666666666666	0.7142857142857143	0.7552631578947369
Information loss	0.5714285714285714	0.3333333333333333	0.2857142857142857	0.24473684210526317

OK Run_Graph

```
Sender_ 8
Receiver_ 9
....
........... 9999895000000000000
............. 101000000000000000000
Sender Balance 99.99895
Receiver Balance 101
```

(c)



Package requirement 'event-driven' is not satisfied

```
import csv
import PySimpleGUI as sg
from numpy import sort as matrix
import numpy
from Dragonfly.main import _callmain_dra
from Dragonfly_crow.main import callmain_pro
from GAcom.main import callmain_ga
```

Input

Select Data: Switzerland

Enter the number of iteration: 20

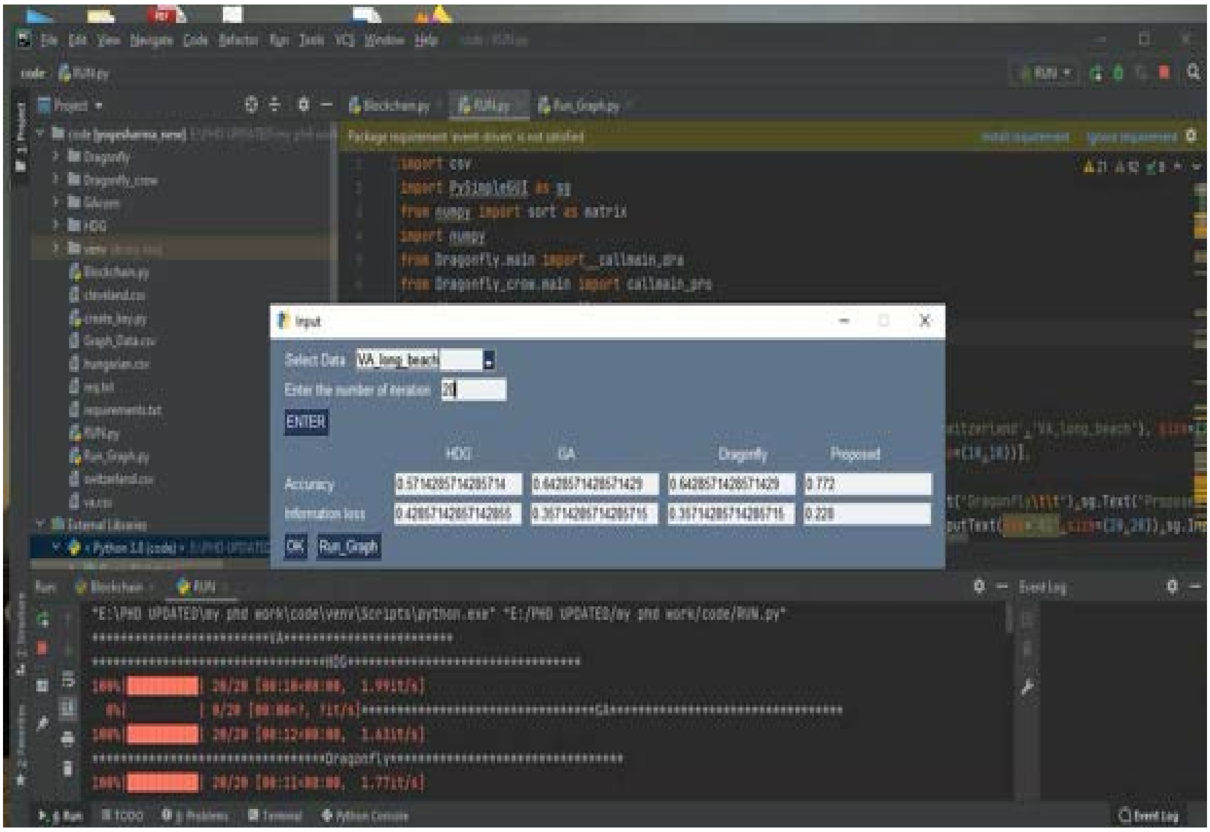
ENTER

	HDG	GA	Dragonfly	Proposed
Accuracy	0.2857142857142857	0.35714285714285715	0.7142857142857143	0.7612903225806451
Information loss	0.7142857142857143	0.6428571428571429	0.2857142857142857	0.23870967741935484

OK Run_Graph

```
Sender_ 5
Receiver_ 7
....
........... 9899958000000000000
.............. 1010000000000000000000
Sender Balance 98.99895
Receiver Balance 101
```

(d)



Package requirement 'event-driven' is not satisfied

```
import csv
import PySimpleGUI as sg
from numpy import sort as matrix
import numpy
from Dragonfly.main import _callmain_dra
from Dragonfly_crow.main import callmain_pro
```

Input

Select Data: VA_long_beach

Enter the number of iteration: 20

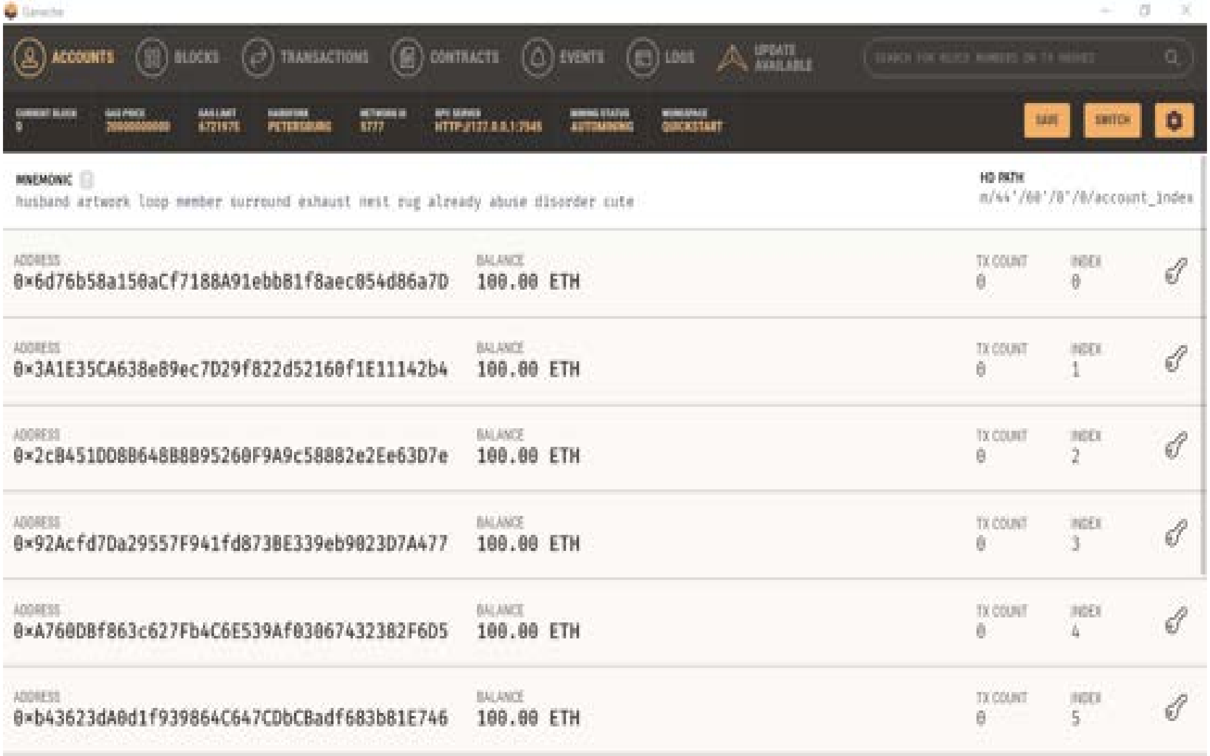
ENTER

	HDG	GA	Dragonfly	Proposed
Accuracy	0.5714285714285714	0.6428571428571429	0.6428571428571429	0.772
Information loss	0.42857142857142855	0.35714285714285715	0.35714285714285715	0.228

OK Run_Graph

```
"E:\PHD UPDATED\my phd work\code\venv\Scripts\python.exe" "E:/PHD UPDATED/my phd work/code/RUN.py"
**************************GA**************************
***********************************HDG***********************************
100%|██████████| 20/20 [00:10<00:00,  1.99it/s]
  0%|          | 0/20 [00:00<?, ?it/s]***********************************GA***********************************
100%|██████████| 20/20 [00:12<00:00,  1.63it/s]
***********************************Dragonfly***********************************
100%|██████████| 20/20 [00:11<00:00,  1.77it/s]
```

(e)



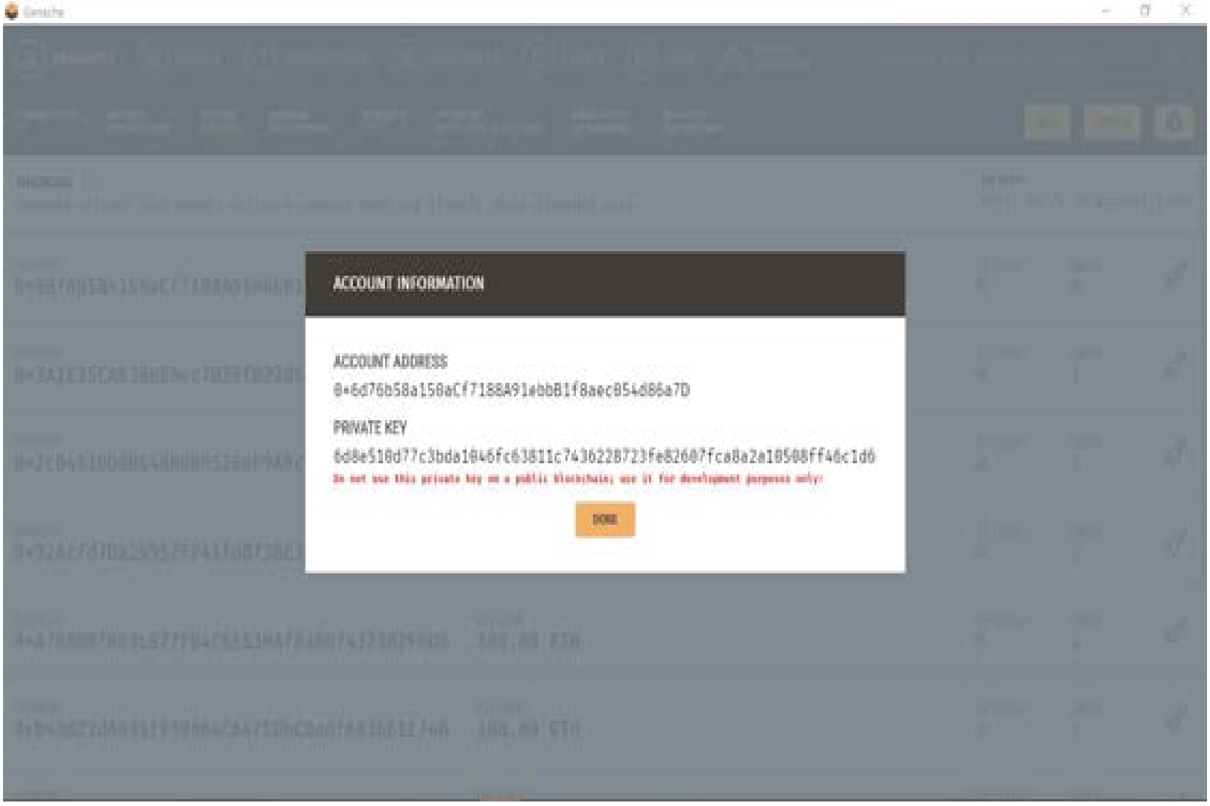
CURRENT BLOCK 0 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK PETERSBURG | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE QUICKSTART

MNEMONIC
husband artwork loop member surround exhaust nest rug already abuse disorder cute

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×6d76b58a150aCf7188A91ebbB1f8aec054d86a7D	100.00 ETH	0	0
0×3A1E35CA638e89ec7D29f822d52160f1E11142b4	100.00 ETH	0	1
0×2cB451DD8B648B8895260F9A9c58882e2Ee63D7e	100.00 ETH	0	2
0×92Acfd7Da29557F941fd873BE339eb9023D7A477	100.00 ETH	0	3
0×A760DBf863c627Fb4C6E539Af03067432382F6D5	100.00 ETH	0	4
0×b43623dA0d1f939864C647CDbCBadf683bB1E746	100.00 ETH	0	5

(f)



ACCOUNT INFORMATION

ACCOUNT ADDRESS
0×6d76b58a150aCf7188A91ebbB1f8aec054d86a7D

PRIVATE KEY
6d8e510d77c3bda1046fc63811c7436228723fe82607fca8a2a10508ff46c1d6
Do not use this private key on a public blockchain; use it for development purposes only!

(g)

Fig. 6.3(a)-(g) Various steps of implementation on four datasets

6.6. Results and Discussion

This section compares the developed technique with the conventional-based methods using a heart disease dataset in terms of accuracy and information loss. The analysis was conducted with various iterations to demonstrate the effectiveness of the proposed D-CS.

6.6.1 Experimental Set-up

The blockchain network was simulated, and the proposed solution was implemented in the network using the Python programming language. The execution was carried out using a PC with a Windows 10 operating system, 2GB of RAM, and an Intel i3 core processor. PySimpleGUI, numpy, matplotlib, sklearn, web3, and tqdm are among the packages used.

6.6.2. Dataset Description

The D-CS approach was tested utilising four different datasets from a cardiac disease dataset, including Cleveland, Hungarian, Switzerland, and VA Long Beach. The Cleveland dataset, which was collected from the Cleveland Clinical Foundation and developed by David W. Aha, was utilised as dataset-1. The Hungarian dataset was received from the Hungarian Institute of Cardiology, and the Switzerland dataset was obtained from the University Hospital in Basel, Switzerland. The dataset-4 was created by Robert Detrano and was based on the VA Long Beach dataset. The dataset consists of 303 instances with 75 features, and the integer and real attributes make the dataset multivariate. Age, sex, chest pain type, resting blood pressure, serum cholesterol, fasting blood sugar, resting electrocardiographic results, maximum heart rate achieved, exercise induced angina, ST depression induced by exercise relative to rest, the slope of the peak exercise ST segment, number of major vessels, and the predicted variable are the fourteen attributes used for experimentation (diagnosis of heart disease).

6.6.3 Evaluation Metrics

Based on the accuracy and information loss outcomes, the D-CS approach was used to analyse the procedure.

6.6.3.1 Accuracy

In the context of privacy preservation, accuracy is defined as the degree of similarity of a calculated value to the original value, and is expressed as:

$$Accuracy = \frac{T_p + T_n}{T_p + T_n + F_p + F_n} \qquad (31)$$

Where T_p indicates the true positive rate; F_p represents the false positive rate; T_n denotes true negative; and F_n denotes false negative rate.

6.6.3.2. Information Loss:

In the context of privacy preservation, information loss is defined as the degree of determined erroneous values in comparison to the original value, and is expressed as:

$$Information\,loss = \frac{F_p + F_n}{T_p + T_n + F_p + F_n} \qquad (32)$$

6.6.4 Competing Methods

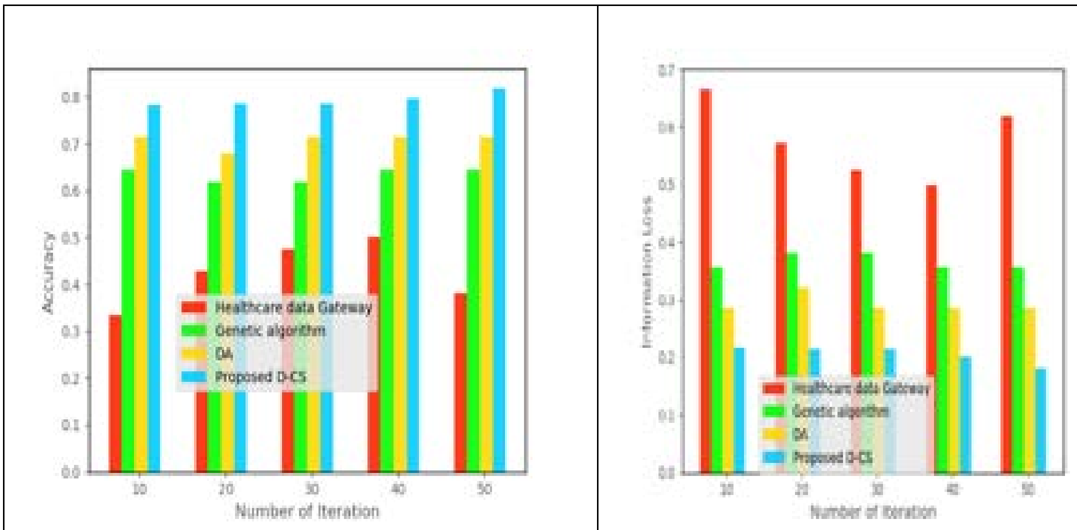
The suggested method's performance was compared to current approaches such as the healthcare data gateway, dragonfly algorithm (DA), and genetic algorithm (GA).

6.6.5. Comparative Analysis

The accuracy and information loss parameters of the D-CS methodology were compared to those of traditional methods in a comparative analysis. The analysis went through several revisions.

6.6.5.1. Analysis by Dataset-1

By altering the iterationsindataset-1, Fig. 6.3 depicts the study of approaches in terms of accuracy and information loss. When the number of iterations was 10, the accuracies measured by the healthcare data gateway, GA, DA, and suggested D-CS were 0.333, 0.642, 0.714, and 0.782, respectively, as shown in Fig. 6.4 (a). These algorithms' respective accuracies for the 50th iteration was 0.380, 0.642, 0.714, and 0.818. Figure 6.4 depicts the method analysis in terms of the information loss parameter values (b). The healthcare data gateway, GA, DA, and D-CS computed information loss values of 0.666, 0.357, 0.285, and 0.217 for the 20th iteration, respectively. When the number of iterations increased to50, the information loss values were0.619, 0.357, 0.285, and 0.181, respectively.

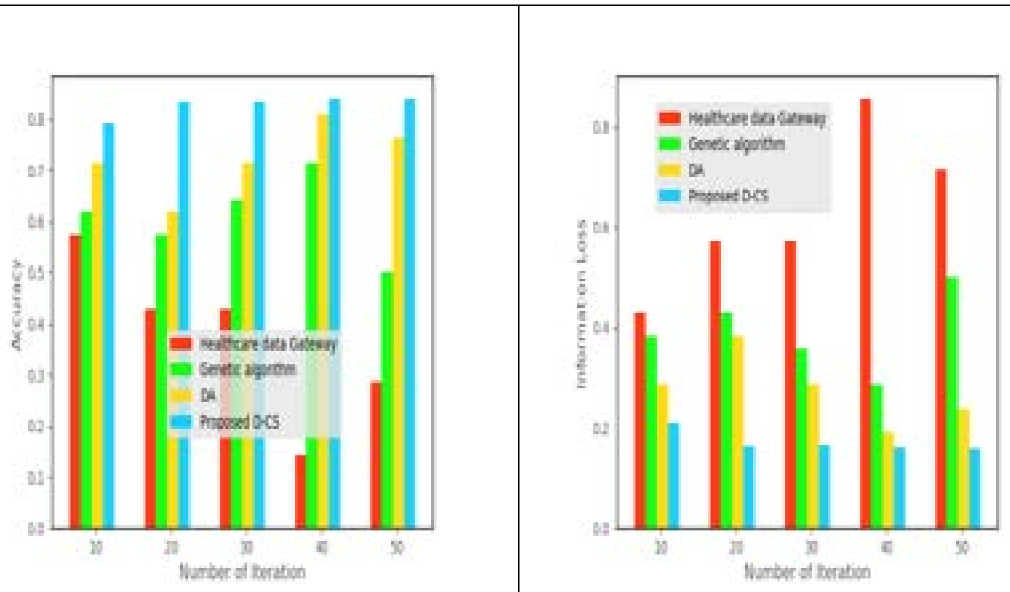


a) b)

Figure 6.4. Method analysis-based on iterations by the dataset-1 with respect to a) Accuracy and b) Information Loss

6.6.5.2. Analysis by Dataset-2

In Fig. 6.5, the accuracy and information loss of the approaches are examined by changing the iterations by the dataset-2. The accuracies measured by the healthcare data gateway, GA, DA, and D-CS were 0.571, 0.619, 0.714, and 0.790, respectively, when the number of rounds was 10. Existing Healthcare data gateway, GA, DA, and planned D-CS accuracy scores for the 50th iteration was 0.285, 0.5, 0.761, and 0.840, respectively. The approach analysis based on information loss is shown in Figure 6.5 (b). The healthcare data gateway, GA, DA, and D-CS computed information loss values of 0.571, 0.428, 0.380, and 0.164, respectively, for the 20th iteration. The information loss values were 0.714, 0.5, 0.238, and 0.159 as the number of iterations climbed to 50.

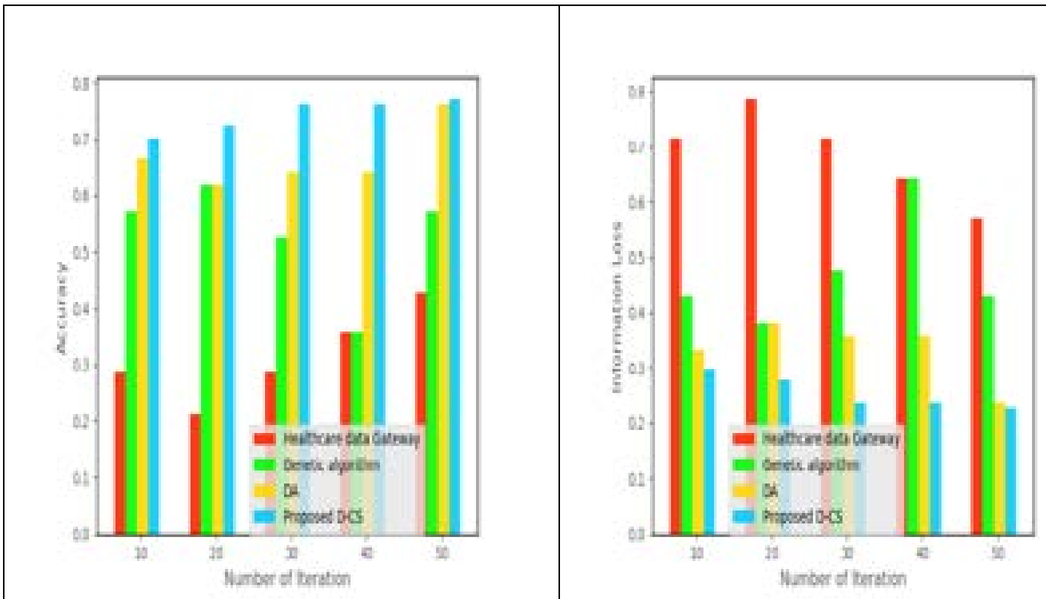


a)	b)

Figure 6.5. Method analysis with iterations by the dataset-2 with respect to the a) Accuracy and b) Information Loss

6.6.5.3. Analysis by Dataset-3

The accuracy and information loss analysis of the approaches in dataset-3 is depicted in Fig. 6.6. The accuracy values evaluated by the existing healthcare data gateway, GA, DA, and D-CS for the 10th iteration were 0.285, 0.571, 0.666, and 0.701, respectively, as shown in Fig 6.6 (a). The accuracy values for the 50th iteration was estimated as 0.428, 0.571, 0.761, and 0.770. Fig. 6.6 (b) depicts the analysis of the methods in terms of information loss parameter. In 20th iteration, the information loss values computed by existing healthcare data gateway, GA, DA, and D-CS were 0.785, 0.380, 0.380, and 0.277, respectively. When the number of iterations increased to 50, the obtained values were0.571, 0.428, 0.238, and 0.229, respectively.

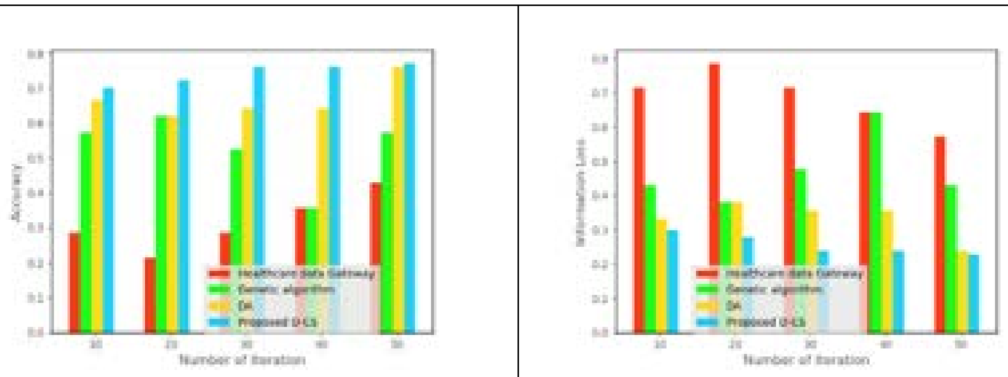


a) **b)**

Figure 6.6. Method analysis with iterations by dataset-3 with respect to the a) Accuracy and b) Information Loss

6.6.5.4. Analysis by Dataset-4

By adjusting the iterations, Fig. 6.7 displays the method analysis in dataset-4 in terms of accuracy and information loss. The accuracy values obtained by the present healthcare data gateway, GA, DA, and the proposed D-CS were 0.428, 0.5, 0.607, and 0.708, respectively, when the number of iterations was 10. The obtained accuracies for the 50th iteration was 0.428, 0.571, 0.571, and 0.748, respectively. Figure 6.7 (b) shows the method analysis in terms of the information loss parameter. The information loss values computed by the existing healthcare data gateways, GA, DA, and D-CS, were 0.666, 0.428, 0.292, and 0.285, respectively, for the 20th iteration. When the number of iterations was increased to 50, the information loss values were 0.571, 0.428, 0.428, and 0.252, respectively.



a)

b)

Figure. 6.7. Method analysis with iterations by dataset-3 with respect to the a) Accuracy and b) Information Loss

6.5.5. Analysis for Average and Standard Deviation

The average and standard deviation of the comparison approaches are presented in this section. The analysis is carried out by setting the iteration to ten and repeating the experimentation 20 times. In Table 6.1, the average and standard deviation of comparison approaches for various datasets are listed. For the Cleveland, Hungarian, Switzerland, and VA datasets, the average and standard deviation values obtained by the proposed D-CS are better than those obtained by other approaches such as HDG, GA, and DA (see Table). **Table 6.1 Analysis based on Average and Standard Deviation**

Dataset s	statistics	HDG	GA	DA	D-CS
Cleveland	Average	0.49458	0.63952	0.71796	0.80653
	Standard deviation	0.05956	0.05937	0.05151	0.02433
Hungarian	Average	0.41239	0.63540	0.71370	0.80949
	Standard deviation	0.11972	0.06893	0.05223	0.04018
Switzerland	Average	0.44158	0.59554	0.71728	0.76045
	Standard deviation	0.09668	0.08409	0.03914	0.03509
VA	Average	0.40504	0.57196	0.64366	0.73276
	Standard deviation	0.04793	0.06880	0.04901	0.03018

6.6.6. Comparative Discussion

In terms of accuracy and information loss, Table 6.2 shows the approach analysis in datasets-1, dataset-2, dataset-3, and dataset-4. In dataset-2, the proposed D achieved a maximum accuracy of 0.840, compared to 0.285, 0.5, and 0.761 produced by the existing healthcare data gateway, genetic algorithm, and DA, respectively. In dataset-2, D-CS had the lowest information loss of 0.159, compared to 0.714, 0.5, and 0.238 for the healthcare data gateway, GA, and DA, respectively.

Table 6.2. Comparative Analysis

Datasets	Metrics	Healthcare Data Gateway	Genetic Algorithm	DA	**Proposed D-CS**
Dataset-1	**Accuracy**	0.380	0.642	0.714	**0.818**
	Information Loss	0.619	0.357	0.285	**0.181**
Dataset-2	**Accuracy**	0.285	0.5	0.761	**0.840**
	Information Loss	0.714	0.5	0.238	**0.159**
Dataset-3	**Accuracy**	0.428	0.571	0.761	**0.770**
	Information Loss	0.571	0.428	0.238	**0.229**
Dataset-4	**Accuracy**	0.428	0.571	0.571	**0.748**
	Information Loss	0.571	0.428	0.428	**0.252**

6.7. Conclusion

The D-CS model is used to suggest a better privacy preservation approach. The blockchain input data are received from the blockchain network using four processes: the block chain facility, the bridge-based sensor, the machine bridge, and the block chain wallet. The data matrix and SU coefficient are then multiplied by the tensor product to compute the tensor vector from the block chain input data. The tensor product is used to turn raw data into protected data while maintaining utility. The D-CS approach, which is a combination of the DA and CSA, is used to calculate the SU coefficient in this example. The objective assessment of these optimization criteria is done in terms of issues such as privacy and utility. The proposed technique was tested against the Hungarian, Cleveland, VA Long Beach, and Switzerland datasets, all of which were derived from a heart disease dataset. In comparison, using dataset 2, the generated model beat the previous datasets, obtaining a maximum accuracy of 0.840 and a minimum information loss of 0.159, demonstrating its superiority.

CHAPTER 7

CONCLUSION AND FUTURE SCOPE

The feature of blockchain like security and privacy has given many organizations attracted towards the technology. The technology has been used in many different industries and organization form various kind of transactions and also in creation of many business models. Many countries are working on the elections based on blockchain technology by using the online voting which will be easier for the voters and more secure and preserve the privacy of electronic voting which will boost the economy of any country. Since the data is very secure and there could be large amount of data so the blockchain based- cloud storage could be very useful. The smart and collaborative transportation which include smart vehicle and smart transportation, could also be possible using the blockchain technology. The international trading which includes many different entities in the network can now be connected in a secure blockchain network which will not only enable the users of the network to track the item for trading but also enable the payment and transaction among the users of the node through the smart contract of the blockchain. Blockchain network is very useful in every field of cryptocurrency. Healthcare is one of those sectors which is moving on to blockchain technology in order to provide security and privacy to the patients record. The amount of data generations today in the healthcare sector is humongous, although we have the technology to store this huge amount of data but the security and privacy need for such data is not appropriate specially when we talk about the Electronic Medical Record (EMR) for any patient. These kinds of records are private to any patient and any patient does not want his private record to get leaked or get misuse by any other person. Researches have been conducted regarding the privacy of the records. This survey conducted on preserving the privacy of the Electronic Medical Record using Blockchain Technology has shown that how researches has been done till now, some of the researchers has provided strong methods to protect and preserve the medical record of a patient but there are still few challenges associated with some methods. Also, the data is not accessible to patients and care providers. These schemes are unable to create a balance between data security and data accessibility. But blockchain can resolve these issues. Blockchain creates a ledger system that is immutable and allows the transactions to take place in a decentralized manner. The three main features of blockchain technology - Security, Decentralization, and Transparency make any application built using it secure and not accessible by unauthorized parties. The manipulation of data is almost impossible to do in a blockchain network. In this project, we propose a system to implement EHRs using blockchain technology. The blockchain technology will keep control over access to information using its cryptographic techniques and decentralization. There is diverse work being done around the globe for expanding the horizon of blockchain. Though it has been used more than just as a financial tool, also in healthcare and security besides numerous others which haven't yet come into the picture. The current idea of using blockchain as another security measure for generating passwords and ensuring secured transactions of extreme essential commodities specifically like human organs and blood groups. By using such a mechanism, the theft could be brought down to a relatively lesser number.

An improved privacy preservation method is proposed using D-CS model. In this approach, the blockchain input data are obtained from the blockchain network based on four processes, including block chain facility, bridge-based sensor, machine bridge and block chain wallet. Then, block chain input data are subjected to the privacy preservation step, from which the data matrix and SU coefficient are multiplied through the tensor product to compute the tensor vector. Here, the tensor product is utilized for converting the raw data into protected data without affecting the utility. In this case, the coefficient of SU is obtained using the D-CS method, which is an integration of the DA and CSA. The objective evaluation for these optimization criteria is carried out in terms of the factors-based on the privacy and utility. The performance of the proposed method was evaluated against the Hungarian, Cleveland, VA Long Beach, and Switzerland datasets taken from a heart disease dataset. Comparatively, the developed model outperformed the other datasets by achieving a maximal accuracy value of 0.840 and minimal information loss of 0.159 using dataset 2, indicating its superiority.

Such researches and developing new techniques, methods are really important not only in the healthcare industry but there are lot many organizations and industries where the privacy and security of information, documents is really needed. Many industries and organization slowly and steadily adapting the blockchain technology. But there are still many countries where the technology is only in books and curriculum. Although the future is very unpredictable, but the lot many things are considered to be predictable.

REFERENCES`

[1]. A. Al Omar, M. S. Rahman, Basu, A. and Kiyomoto, S. (2017), "Medibchain: A blockchain based privacy preserving platform for healthcare data," In proceedings of International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage, pp. 534-543.

[2]. Abd Zaid, D. S. (2018), “Lightweight Rsa Algorithm Using Three Prime Numbers”, International Journal of Engineering and Technology, pp. 293-295.

[3]. Ackerman, A., Chang, A., Diakun-Thibault, N., Forni, L., Landa, F., Mayo, J., and van Riezen, R. (2016), “Blockchain and Health IT: Algorithms, Privacy and Data”, Project PharmOrchard of MIT’s Experimental Learning “MIT FinTech: Future Commerce.”, White Paper August.

[4]. Amofa, S., Sifah, E. B., Kwame, O. B., Abla, S., Xia, Q., Gee, J. C., and Gao, J. (2018), “A blockchain-based architecture framework for secure sharing of personal health data”, In 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), pp. 1-6, IEEE.

[5]. Anwar, H. (2018), “Consensus Algorithms: The Root of The Blockchain Technology”, Recuperado de: https://101blockchains. com/consensus-algorithms-blockchain, 5.

[6]. Askarzadeh, A., (2016), "A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm," Computers & Structures, vol.169, pp.1-12.

[7]. Atlam, H. F., and Wills, G. B. (2020), “IoT security, privacy, safety and ethics”, In Digital twin technologies and smart cities, springer, pp. 123-149.

[8]. Atzori, M. (2015), “Blockchain technology and decentralized governance: Is the state still necessary?” Available at SSRN 2709713.

[8]. Auto, ET., (2017), “Toyota Research Institute: Toyota Research Institute Explores Blockchain Technology to Develop New Mobility Ecosystem, Auto News, ET Auto.”

[9]. Bahga, A., and Madisetti, V. K. (2016), “Blockchain platform for industrial internet of things”, Journal of Software Engineering and Applications, vol. 9, no. 10, pp. 533-546. https://doi.org/10.4236/jsea.2016.910036.

[10]. Baliga, A. (2017), “Understanding blockchain consensus models”, Persistent, vol. 4, pp. 1-14.

[11]. Bannet, J., Price, D. W., Rudys, A., Singer, J., and Wallach, D. S. (2004), “Hack-a-vote: Security issues with electronic voting systems”, IEEE Security & Privacy, vol. 2, no. 1, pp. 32-37. https://doi.org/10.1109/MSECP.2004.1264851.

[12]. Barenji, A. V., Guo, H., Tian, Z., Li, Z., Wang, W. M. and Huang, G. Q. (2019), “Blockchain-based cloud manufacturing: Decentralization”. In Advances in Transdisciplinary Engineering, 7:1003–11. https://doi.org/10.3233/978-1-61499-898-3-1003.

[13]. Barnes, A., Brake, C., and Perry, T. (2016), “Digital Voting with the use of Blockchain Technology”, Team Plymouth Pioneers-Plymouth University.

[14]. Bela, M., Gaber, J., El-Sayed, H., Almojel, A. (2006), “Swarm Intelligence in Handbook of Bio-inspired Algorithms and Applications”, Series: CRC Computer & Information Science, vol. 7. Chapman & Hall, ISBN 1-58488-477-5.

[15]. Beni, G., Wang, J. (1989), “Swarm intelligence in cellular robotics systems”, In: Proceedings of NATO Advanced Workshop on Robots and Biological System.

[16]. Bertino, E., Deng, R., Huang, X. and Zhou, J. (2015), "Security and privacy of electronic health information systems", International Journal of Information Security, vol. 14, no. 6, pp. 485-486. Available: 10.1007/s10207-015-0303-z.

[17]. Bertrand, C., Vlasov, N., and Bani, E. (2020), “Blockchain for Supply Chains and International Trade Report on Key Features, Impacts and Policy Options”. https://doi.org/10.2861/957600.

[18]. Bocas J. (2018), “Emerging technologies that will change healthcare”.

[19]. Bordea, G., Jothi, N., Rashid, N. A., and Husain, W, (2015), "Data mining in healthcare: a review," Procedia Computer Science, vol.72, pp.306–313.

[20]. Bryanov, K. (2018), “Distributed Ledger of Ideas: Toward A Blockchain-Powered Marketplace”, RAP on Blockchain at North Dakota State University's Center for the Study of Public Choice and Private Enterprise.

[21]. Bulut, R., Kantarcı, A., Keskin, S., & Bahtiyar, Ş. (2019), “Blockchain-based electronic voting system for elections in turkey”. In 2019 4th International Conference on Computer Science and Engineering (UBMK), pp. 183-188, IEEE.

[22]. Buterin, V. (2014), “Ethereum White Paper: A Next Generation Smart Contract & Decentralized Application Platform.” Etherum, no. January, pp. 1–36. https://github.com/ethereum/wiki/wiki/White-Paper.

[23]. Chandrasekar R, (2020), “Fuzzy Crow Search Algorithm-Based Deep LSTM for Bitcoin Prediction", International Journal of Distributed Systems and Technologies, vol.11, no.4.

[24]. Chen, Y. H., Chen, S. H., & Lin, I. C. (2018), “Blockchain based smart contract for bidding system”. In 2018 IEEE International Conference on Applied System Invention (ICASI), pp. 208-211, IEEE.

[25]. Chen, Y., Ding, S., Xu, Z., Zheng, H. and Yang, S.(2019), "Blockchain-based medical records secure storage and medical service framework," Journal of medical systems, vol.43, no.1, pp.5.

[26]. Clayton N, Emery N. (2005), “Corvide cognition”. Curr Biol. vol.15.

[27]. Copel, N., and Ater, T. (2017), “DAV White Paper”. tech. rep.

[28]. Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V., (2016), “Blockchain technology: Beyond bitcoin”, Appl. Innov., vol. 2, pp. 6–10.

[29]. Curran, K. (2018), “E-Voting on the Blockchain”, The Journal of the British Blockchain Association, vol, 1, no. 2, pp. 4451.

[30]. Daely, P. T., and Shin, S. Y. (2016), “Range based wireless node localization using dragonfy algorithm”, In 2016 ighth nternational Conference on Ubiquitous and Future etworks, pp. 1012–1015.

[31]. Dahlberg, C. (2008), “Challenges in Designing an Electronic Voting System”. Cs.Hmc.Edu.

[32]. Dennis, R., and Owen, G. (2015), “Rep on the block: A next generation reputation system based on the blockchain”, In 2015 10th International Conference for Internet Technology and Secured Transactions, pp. 131-138.

[33]. Dey, K. C., Rayamajhi, A., Chowdhury, M., Bhavsar, P., and Martin, J. (2016), “Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication in a heterogeneous wireless network–Performance evaluation”. Transportation Research Part C: Emerging Technologies, vol. 68, pp.168-184.

[34]. Dhaliwal, N., Harison, E. and Lima, C., (2018), “IAGON .”

[35]. Dinh, T. T. A., Wang, J., Chen, G., Liu, R., Ooi, B. C., & Tan, K. L. (2017), “Blockbench: A framework for analyzing private blockchains”, In Proceedings of the 2017 ACM International Conference on Management of Data, pp. 1085-1100.

[36]. Dubovitskaya, A., Xu, Z., Ryu, S., Schumacher, M. and Wang, F. (2017), “Secure and trustable electronic medical records sharing using blockchain”, In AMIA annual symposium proceedings, p. 650, American Medical Informatics Association.

[37]. Duong, T., Chepurnoy, A., Fan, L., and Zhou, H. S. (2018), “Twinscoin: A cryptocurrency via proof-of-work and proof-of-stake”, In Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts, pp. 1-13.

[38]. Dwork, C., and Naor, M. (1992), “Pricing via processing or combatting junk mail”, In Annual international cryptology conference, pp. 139-147, Springer, Berlin, Heidelberg.

[39]. Dylan Yaga, P. M. (2018), “Blockchain Technology Overview”.

[40]. Elhariri, E., El-Bendary, N., and Hassanien, A. E. (2016), “Bio-inspired optimization for feature set dimensionality reduction”, In 2016 3rd nternational Conference on dvances in Computational Tools or ngineering pplications, pp. 184–189.

[41]. Emmanuelle,G. (2018), “Can Blockchain Revolutionize International Trade? Can Blockchain Revolutionize International Trade? “https://doi.org/10.30875/7c7e7202-en.

[42]. Evans, R. (2016), "Electronic Health Records: Then, Now, and in the Future", Yearbook of Medical Informatics, vol. 25, no. 01, pp. S48-S61. Available: 10.15265/iys-2016-s006.

[42]. Fernández-Alemán, J., Señor, I., Lozoya, P. and Toval, A. (2013), "Security and privacy in electronic health records: A systematic literature review", Journal of Biomedical Informatics, vol. 46, no. 3, pp. 541-562. Available: 10.1016/j.jbi.2012.12.003.

[43]. Frank, O. (2011), “Interoperability, Technical.” In SpringerReference. https://doi.org/10.1007/springerreference_62308.

[44]. Gao, G., Wan, X., Yao, S., Cui, Z., Zhou, C., and Sun X.(2017), "Reversible data hiding with contrast enhancement and tamper localization for medicalimages", Inf Sci, vol. 385–386, pp. 250–65.

[45]. Ge, C., Sun, S. and Szalachowski, P. (2019), "Permissionless Blockchains and Secure Logging", In 2019 IEEE International Conference on Blockchain and Cryptocurrency, pp. 56-60.

[46]. Golub, B. (2019), "Decentralized Cloud? How the Intersection of Blockchain, Decentralization and Open Source is Impacting Cloud Storage".

[47]. Gómez, J., Oviedo, B., and Zhuma, E. (2016), "Patient monitoring system based on internet of things", Procedia Computer Science, vol. 83, pp. 90-97.

[48]. Gubbi, J., Buyya, R., Marusic, S., and Palaniswami, M. (2013), "Internet of Things (IoT): A vision, architectural elements, and future directions", Future generation computer systems, vol. 29, no. 7, pp. 1645-1660.

[49]. Gunter, T., and Terry, N. (2005), "The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions", Journal of Medical Internet Research, vol. 7, no. 1. Available: 10.2196/jmir.7.1. e3.

[50]. Guy,Z. and O. N. (2015), "Decentralizing Privacy: Using Blockchain to Protect Personal Data", IEEE CS Security and Privacy Workshops, pp. 180-184, IEEE.

[51]. H.Huang and W.Fang. (2011), "Integrity preservation and privacy protection for medicalimages with histogram-based reversible data hiding", Life Science Systems and Applications Workshop,pp.108–111.

[51]. Hamdy, M., Nguyen, A. T., and Hensen, J. L. (2016), "A performance comparison of multi objective optimization algorithms for solving nearly-zero-energy-building design problems", Energy and buildings, vol. 121, pp. 57–71.

[52]. Hariharan, M., Sindhu, R., Vijean, V., Yazid, H., Nadarajaw, T., Yaacob, S., et al. (2018), "Improved binary dragonfy optimization algorithm and wavelet packet based non-linear features for infant cry classifcation", Computer methods and programs in biomedicine, vol 155, pp. 39–51.

[53]. Harsh, A. (2020), "Siacoin (SC) Cryptocurrency: An Ultimate Beginner's Guide".

[54]. Haynes, P. (2014), "Online Voting: Rewards And Risks."

[55]. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., and Hjálmtýsson, G. (2018), “Blockchain-based e-voting system”, In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983-986.

[56]. Hufnagel, S. (2009), "National Electronic Health Record Interoperability Chronology", Military Medicine, vol. 174, no. 5, pp. 35-42. Available: 10.7205/milmed-d-03-9708.

[57]. Hurlburt, G. F., and Bojanova, I. (2014),“Bitcoin: Benefit or curse?”, It Professional, vol. 16, no. 3, pp. 0-15.

[58]. Hussein, A. F., ArunKumar, N., Ramirez-Gonzalez, G., Abdulhay, E., Tavares, J. M. R., and de Albuquerque, V. H. C. (2018), “A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform”. Cognitive Systems Research, vol. 52, pp. 1-11.

[59]. Islam, M. A., Islam, M. A., Islam, N., and Shabnam, B. (2018), “A modified and secured RSA public key cryptosystem based on “n” prime numbers”, Journal of Computer and Communications, vol. 6, no. 3, pp. 78.

[60]. Ivanov, A., Babichenko, Y., Kanunnikov, H., Karpus, P., Foiu-Khatskevych, L., Kravchenko, R., and Nevmerzhitskyi, I. (2018), “Technical comparison aspects of leading blockchain-based platforms on key characteristics”.

[61]. Jafari, M., and Chaleshtari, M. H. B. (2017), “Using dragonfy algorithm for optimization of orthotropic infnite plates with a quasi-triangular cut-out”, European journal of mechanics A/Solids, vol. 66, pp. 1–14.

[62]. Jothi, N., and Husain, W. (2015), “Data mining in healthcare–a review”, Procedia computer science, 72, pp. 306-313.

[63]. Karame, G. and Capkun, S. (2018), "Blockchain Security and Privacy", IEEE Security & Privacy, vol. 16, no. 4, pp. 11-12. Available: 10.1109/msp.2018.3111241.

[64]. Kessler, G. C. (2003), “An overview of cryptography”.

[65]. Kim S., Lee H., and Chung Y.D.(2017), “Privacy-preserving data cube for electronic medical records:an experimentalevaluation”, Int J Med Inform, vol. 97, pp. 33–42.

[66]. Kotas, B. (2017), “The Decentralized Cloud and the Future of Data are Here—Influencive”. October, 22, 2017.

[67]. Ks, S. R., and Murugan, S. (2017), “Memory based hybrid dragonfy algorithm for numerical optimization problems.Expert Systems with pplications, vol. 83, pp. 63–78.

[68]. Kumar, C. A., Vimala, R., Britto, K. A., and Devi, S. S. (2018), “FDLA: Fractional dragonfy based load balancing algorithm in cluster cloud model”, Cluster Computing, pp. 1–14.

[69]. Lee,H.,Kim,S., Kim, J.W. and Chung Y.D.,(2017), “Utility-preserving anonymization for health data publishing”, vol.17, no.104.

[70]. Levi, S. D., and Lipton, A. B. (2018), “An introduction to smart contracts and their potential and inherent limitations”, In Harvard law school forum on corporate governance & financial regulation.

[71]. Li, T., Abla, P., Wang, M., and Wei, Q. (2017), “Designing Proof of Transaction Puzzles for Cryptocurrency, IACR Cryptol, pp. 1242.

[72]. Li, Z., Kang, J., Yu, R., Ye, D., Deng, Q., and Zhang, Y. (2017), “Consortium blockchain for secure energy trading in industrial internet of things”, IEEE transactions on industrial informatics, vol. 14, no. 8, pp. 3690-3700.

[73]. Li,Y., Bai, C., and Reddy, CK.A.(2016). “Distributed ensemble approach for mining healthcare data under privacy constraints”, Information Science, vol. 330, pp. 245–59.

[74]. Liang, X. J. Z. (2017), “Integrating Blockchain for Data Sharing and Collaboration in Mobile Healthcare Applications”, Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, pp. 1-5, IEEE.

[75]. Liang, X., Zhao, J., Shetty, S., Liu, J. and Li, D., (2017), "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," In proceedings of IEEE Annual International Symposium on Personal, Indoor, and Mobile Radio Communications, pp. 1-5.

[76]. Lima, E. G., Chinelli, C. K., Guedes, A. L. A., Vazquez, E. G., Hammad, A. W., Haddad, A. N., and Soares, C. A. P. (2020), “Smart and sustainable cities: The main guidelines of City Statute for increasing the intelligence of Brazilian cities. Sustainability”, vol.12, no. 3, pp. 1025.

[77]. Litke, A., Anagnostopoulos, D., and Varvarigou, T. (2019), “Blockchains for supply chain management: Architectural elements and challenges towards a global scale deployment”, Logistics, vol. 3, no.1, pp.5.

[78]. Liu, J., Li, X., Ye, L., Zhang, H., Du, X., and Guizani, M. (2018), “BPDS: A blockchain based privacy-preserving data sharing for electronic medical records”. In 2018 IEEE Global Communications Conference (GLOBECOM), pp. 1-6, IEEE.

[79]. Macdonald, M., Liu-Thorrold, L., and Julien, R. (2017), “The blockchain: a comparison of platforms and their uses beyond bitcoin”, Work, pp. 1-18.

[80]. Mafarja, M., Jaber, I., Eleyan, D., Hammouri, A., and Mirjalili, S. (2017), “Binary dragonfy algorithm for feature selection”, In 2017 nternational Conference on ew Trends in Computing Sciences, pp. 12–17.

[81]. Marco e. G. Maltese. (2015), “Blockchain-Based Decentralized Cloud Storage: Storj And Competitors.”

[82]. Marr, B. (2018), “How much data do we create every day? The mind-blowing stats everyone should read”, In Forbes, pp. 1-5.

[83]. Mearian, L. (2015), “New Service Wants to Rent Out Your Hard Drive’s Extra Space| Computerworld”.

[84]. Mendling, J., Weber, I., Aalst, W. V. D., Brocke, J. V., Cabanillas, C., Daniel, F., and Zhu, L. (2018), “Blockchains for business process management-challenges and opportunities”, ACM Transactions on Management Information Systems (TMIS), vol. 9, no. 1, pp.1-16.

[85]. Millonas, M. (1994), “Swarms, Phase Transitions, and Collective Intelligence” Addison-Wesley.

[86]. Minni, R., Sultania, K., Mishra, S., and Vincent, D. R. (2013), “An algorithm to enhance security in RSA”, In 2013 Fourth International Conference on Computing, Communications and Networking Technologies, pp. 1-4.

[87]. Mirjalili, S., (2016),"Dragonfly algorithm: a new meta-heuristic optimization technique for solving single-objective, discrete, and multi-objective problems," Neural Computing and Applications, vol.27, no.4, pp.1053-1073.

[88]. Mrvosevic, M. (2019), “Blockchain Based Decentralised Cloud Computing.”

[89]. Müller, A., Ludwig, A., and Franczyk, B. (2017), “Data security in decentralized cloud systems–system comparison, requirements analysis and organizational levels”, Journal of Cloud Computing, vol.6, no.1, pp.1-9.

[90]. Nakamoto, S. (2008), “Bitcoin: A peer-to-peer electronic cash system”, Decentralized Business Review, pp. 21260.

[91]. National Security Agency. (2020), “Mitigating Cloud Vulnerabilities.”

[92]. Pangbourne, K., Stead, D., Mladenović, M., and Milakis, D. (2018), “The case of mobility as a service: A critical reflection on challenges for urban transport and mobility governance”. In Governance of the smart mobility transition. Emerald Publishing Limited, pp. 33-48.

[93]. Park, J. H., and Park, J. H. (2017), “Blockchain security in cloud computing: Use cases, challenges, and solutions”, Symmetry, vol.9, no. 8, pp.1-13.

[94]. Pathania, A. K., Mehta, S., and Rza, C. (2016), “Economic load dispatch of wind thermal integrated system using dragonfy algorithm”, In 2016 7th ndia nternational Conference on Power lectronics (IICPE), pp. 1–6.

[95]. Patil, S., and Puranik, P. (2019), “Blockchain technology”, International Journal of Trend in Scientific Research and Development, vol. 3, no. 4, pp. 573-574.

[96]. Peterson K, Deeduvanu R, Kanjamala P, Clinic KBM, (2016), "A Blockchain-Based Approach to Health Information Exchange Networks”.

[97]. Pilkington, M. (2016), “Blockchain technology: principles and applications”, In Research handbook on digital transformations. Edward Elgar Publishing, pp. 225–53.

[98]. Pilkington, M. (2016),“Blockchain Technology: Principles and Applications.” In Research Handbooks on Digital Transformations, 225–53. Edward Elgar Publishing Ltd. https://doi.org/10.4337/9781784717766.00019.

[99].Politou, E., Casino, F., Alepis, E., and Patsakis, C. (2019), “Blockchain mutability: Challenges and proposed solutions”, IEEE Transactions on Emerging Topics in Computing.

[99].Poulis G., Loukides G., Skiadopoulos, S. and Divanis, A. (2017), "Anonymizing datasets with demographics and diagnosis codes in the presence of utility constraints”, J Biomed Inform, vol. 65, pp. 76–96.

[100]. Pramanik PKD, Pal S, and Mukhopadhyay M. (2018), “ Healthcare big data”, igi-global, pp. 72–100.

[101]. Prior H, Schwarz A, Güntürkün O. (2008), “Mirror-induced behavior in the magpie (pica pica): evidence of self-recognition”. PLoS Biol, vol.6, no. 8.

[102]. Raghupathi, W., and Raghupathi, V. (2014), “Big data analytics in healthcare: promise and potential”, Health information science and systems, vol. 2, no. 1, pp. 1-10.

[103]. Rincon, Paul, Science/nature|crows and jays top bird IQ scale, BBC News.

[104]. Rouse, M. (2017), consensus algorithm. Retrieved from whatis.techtarget.com: https://whatis.techtarget.com/definition/consensus-algorithm

[105]. Rubin, A. D. (2002), “Security Considerations for Remote Electronic Voting”, Communications of the ACM, vol. 45, no. 12, pp. 39–44.

[106]. Russell RW, May ML, Soltesz KL, Fitzpatrick JW. (1998), “Massive swarm migrations of dragonflies (Odonata) in eastern North America”, Am Midl Nat 140:325–342.

[107]. Sagirlar, G., Carminati, B., Ferrari, E., Sheehan, J. D., and Ragnoli, E. (2018), “Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains”, In 2018 IEEE International Conference on Internet of Things) and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data, pp. 1007-1016.

[108]. Salam, M. A., Zawbaa, H. M., Emary, E., Ghany, K. K. A., and Parv, B. (2016), “A hybrid dragonfy algorithm with extreme learning machine for prediction”, In 2016 nternational Symposium on Nnovations in ntelligent SysTems and pplications (INISTA) pp. 1–6.

[109]. Sambandam, R. K., and Jayaraman, S. (2016), “Self-adaptive dragonfy based optimal thresholding for multilevel segmentation of digital images”, Journal of King Saud University-Computer and information Sciences.

[110]. Sarkar, B. K. (2017), “Big data for secure healthcare system: a conceptual design”, Complex & Intelligent Systems, vol.3, no. 2, pp. 133-151.

[111]. Sekhar, A. H., and Devi, A. L. (2016), “Analysis of multi tcsc placement in transmission system by using fring angle control model with heuristic algorithms”, ARPN journal of engineering and applied Sciences, vol.11, no. 21, pp. 12743–12755.

[112]. Sen, J.(2010), “Security and Privacy Issues in Cloud C Loud Computing”.

[113]. Shah, S., Kanchwala, Q., and Mi, H. (2016), “Block Chain Voting System”. Northeastern University.

[114]. Sharma, T.K. (2018), “Advantages and Disadvantages of Permissionless Blockchain”.

[115]. Sharma, Y., and Balamurugan, B. (2020), “A survey on privacy preserving methods of electronic medical record using blockchain”, Journal of Mechanics of Continua and Mathematical Sciences, vol.15, no. 2, pp. 32-47.

[116]. Shrier AA, Chang A, Diakun-thibault N, Forni L, Landa F, Mayo J, van Riezen R. (2017), "Blockchain and Health IT: Algorithms, Privacy, and Data,".

[117]. Siahaan, A. P. U. (2000), “Factorization Hack of RSA Secret Numbers”, International Journal of Engineering Trends and Technology, pp.15-18.

[118]. Sikeridis, D., Papapanagiotou, I., Rimal, B. P., & Devetsikiotis, M. (2017), “A Comparative taxonomy and survey of public cloud infrastructure vendors”.

[119]. Singh, M. and Kim, S. (2018), “Branch Based Blockchain Technology in Intelligent Vehicle.” Computer Networks, vol. 145, pp. 219–31. https://doi.org/10.1016/j.comnet.2018.08.016.

[120]. Srinivasan, C. R., Rajesh, B., Saikalyan, P., Premsagar, K., and Yadav, E. S. (2019), “A review on the different types of Internet of Things (IoT)”, Journal of Advanced Research in Dynamical and Control Systems, vol. 11, no. 1, pp. 154-158.

[121]. Storj Labs. (2018), “Storj: A Decentralized Cloud Storage Network Framework”, pp. 1–90.

[122]. Sugave, S. R., Patil, S. H., and Reddy, B. E. (2017), “DDF: Diversity dragonfy algorithm for cost aware test suite minimization approach for software testing”, In 2017 nternational Conference on ntelligent Computing and Control Systems, pp. 701–707.

[123]. Suresh, V., and Sreejith, S. (2017), “Generation dispatch of combined solar thermal systems using dragonfy algorithm.Computing, vol. 99, no. 1, pp. 59–80.

[124]. Szalachowski, P., Reijsbergen, D., Homoliak, I., and Sun, S. (2019), “Strongchain: Transparent and collaborative proof-of-work consensus”. In 28th Security Symposium, pp. 819-836.

[125]. Taylor, P. J., Dargahi, T., Dehghantanha, A., Parizi, R. M., and Choo, K. K. R. (2020), “A systematic literature review of blockchain cyber security”, Digital Communications and Networks, vol.6, no.2, pp. 47-156.

[126]. Thakkar, M., and Davis, D. C. (2006), “Risks, barriers, and benefits of EHR systems: a comparative study based on size of hospital”, Perspectives in Health Information Management/AHIMA, American Health Information Management Association, 3.

[127]. Thorp JH, Rogers DC. (2014) “Thorp and Covich’s freshwater invertebrates: ecology and general biology”, Elsevier, Amsterdam.

[128]. Tian, H., He, J. and Ding, Y. (2019), "Medical Data Management on Blockchain with Privacy," Journal of medical systems, vol.43, no.2, pp.26, 2019.

[129]. Ubiergo, G. A., and Jin, W. L. (2016), “Mobility and environment improvement of signalized networks through Vehicle-to-Infrastructure (V2I) communications”, Transportation Research Part C: Emerging Technologies, vol. 68, pp. 70-82.

[130]. Underwood, S. (2016), “Blockchain beyond Bitcoin”. Communications of the ACM vol. 59, no. 11, pp. 15–17. https://doi.org/10.1145/2994581.

[131]. Vera Maltseva, A. M. (2019), “Blockchain and the Future of Global Trade (Review of the WTO report “Can Blockchain revolutionize international trade)”, International Organisations Research Journal, pp. 191-198.

[132]. Vijayakumar, V., Sabarivelan, K. M., Tamizhselvan, J., Ranjith, B., and Varunkumar, B. “Utlization of Blockchain in Medical Healthcare Record using Hyperledger Fabric”.

[133]. Vora, J., Nayyar, A., Tanwar, S., Tyagi, S., Kumar, N., Obaidat, M. S., and Rodrigues, J. J. (2018), “BHEEM: A blockchain-based framework for securing electronic health records”, In 2018 IEEE Globecom Workshops, pp. 1-6.

[134]. Wang W., Chen L., and Zhang Q.(2015), “Outsourcing high-dimensionalhealthcare data to cloud with personalized privacy preservation”, Computer Networks, vol. 88, pp. 136–48.

[135]. Wang, B. (Ed.). (2014), “Big Data Analytics in Bioinformatics and Healthcare”, IGI Global.

[136]. Wang, L., and Alexander, C. A. (2020), "Big data analytics in medical engineering and healthcare: methods, advances and challenges", Journal of medical engineering & technology, vol. 44, no. 6, pp. 267-283.

[137]. Wang, L., Shen, X., Li, J., Shao, J., and Yang, Y. (2019), "Cryptographic primitives in blockchains", Journal of Network and Computer Applications, vol. 127, pp. 43-58.

[138]. Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., and Kim, D. I. (2019), "A survey on consensus mechanisms and mining strategy management in blockchain networks", IEEE Access, vol. 7, pp. 22328-22370.

[139]. Wang, X., and Zhanqiang L. (2016), "Traffic and Transportation Smart with Cloud Computing on Big Data." International Journal of Computer Science and Applications vol. 13, no.1, pp. 1–16.

[140]. WEI SHE, Q. L. (2019), "Blockchain Trust Model for Malicious Node Detection in Wireless Sensor Networks". Special Section On Mobile Service Computing With Internet Of Things, pp. 38947-38956, IEEE Access.

[141]. Wikelski M, Moskowitz D, Adelman JS, Cochran J, Wilcove DS, May ML. (2006), "Simple rules guide dragonfly migration", Biol Lett 2:325–329 33.

[142]. Xia, Q., Sifah, E. B., Smahi, A., Amofa, S., & Zhang, X. (2017), "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments: Information, vol. 8, no.2, pp. 44.

[143]. Yang, J. J., Li, J., Mulder, J., Wang, Y., Chen, S., Wu, H., and Pan, H. (2015), "Emerging information technologies for enhanced healthcare", Computers in industry, vol. 69, pp. 3-11.

[144]. Yu, B., Liu, J. K., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P., and Au, M. H. (2018), "Platform-independent secure blockchain-based voting system", In International Conference on Information Security, pp. 369-386.

[145]. Yuan, Y., and Wang, F. Y. (2016), "Towards blockchain-based intelligent transportation systems", In 2016 IEEE 19th international conference on intelligent transportation systems (ITSC), pp. 2663-2668, IEEE.

[146]. Yue, X., Wang, H., Jin, D., Li, M. and Jiang, W. (2016), "Healthcare data gateways: found healthcare intelligence on Blockchain with novel privacy risk control," Journal of medical systems, vol.40, no.10, pp.218.

[147]. Zhang K., Liang X., Baura M., Lu R., and Shen X. (2014), “PHDA:a priority based health data aggregation with privacy preservation for cloud assisted WBANs”, Information Science, vol. 284, pp. 130–41.

[148]. Zhang, R., Xue, R., and Liu, L. (2019), “Security and privacy on blockchain”, ACM Computing Surveys (CSUR), vol. 52, no. 3, pp.1-34. https://doi.org/10.1145/3316481.https://doi.org/10.1145/3316481.

[149]. Zhang, Y., Chen, M., Huang, D., Wu, D., and Li, Y. (2017), “iDoctor: Personalized and professionalized medical recommendations based on hybrid matrix factorization”, Future Generation Computer Systems, vol. 66, pp. 30-35.

[150]. Zheng, Z., Xie, S., Dai, H., Chen, X., and Wang, H. (2017), “An overview of blockchain technology: Architecture, consensus, and future trends”, In 2017 IEEE international congress on big data, pp. 557-564.

[151]. Zhou, E., Sun, H., Pi, B., Sun, J., Yamashita, K., and Nomura, Y. (2019), “Ledger data refiner: a powerful ledger data query platform for hyperledger fabric”. In 2019 Sixth International Conference on Internet of Things: Systems, Management and Security, pp. 433-440.

[152]. Zhu, L., Wu, Y., Gai, K. and Choo, K.K.R. (2019), "Controllable and trustworthy blockchain-based cloud data management," Future Generation Computer Systems, vol.91, pp.527-535.

[153]. Zou, X., Li, H., Li, F., Peng, W., & Sui, Y. (2017), “Transparent, auditable, and stepwise verifiable online e-voting enabling an open and fair election”, Cryptography, vol.1, no.2, pp. 13. https://doi.org/10.3390/cryptography1020013.