BLOCKCHAIN INSPIRED PRIVACY PRESERVING AND AUDITABLE MODEL FOR ELECTRONIC HEALTH RECORDS

Thesis Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

Computer Science and Engineering

By

Badagala vasantha Rani

Registration Number:41900163

Supervised By

Dr Parminder Singh(16479)

Computer Science & Engineering(Professor)

Lovely Professional University

LOVELY PROFESSIONAL UNIVERSITY, PUNJAB

2025

DECLARATION

I, here by declared that the presented work in the thesis entitled "**Blockchain Inspired Privacy Preserving and Auditable Model for Electronic Health Records**" in fulfilment of degree of Doctor of Philosophy (Ph.D.)is the outcome of research work carried out by me under the supervision of Dr. Parminder Singh, working as Professor, in the School of Computer Science Engineering, of Lovely Professional University, Punjab, India. In keeping with general practice of report- ing scientific observations, due acknowledgments have been made whenever work described here has been based on findings of other investigator. This work has not been submitted in part or full to any of the University or Institute for the award of any degree.

(Signature of Scholar)

Name of the scholar: Badagala vasantha Rani

Registration No.: 41900163

Department/School: School of Computer Science and Engineering

Place: Lovely Professional University, Punjab, India

Date: 15.04.2025

CERTIFICATE

This is to certify that the work reported in the Ph.D.thesis entitled “**Blockchain Inspired Privacy Preserving and Auditable Model for Electronic Health Records**” submitted in fulfillment of the requirement for the award of degree of Doctor of Philosophy (Ph.D) in the School of Computer Science and Engineering, is a research work carried out by Badagala Vasantha Rani, 41900163, is bonafide record of her original work carried out under my supervision and that no part of thesis has been submitted for any other degree, diploma or equivalent course.

(Signature of Supervisor)
Name of the Supervisor: Dr. Parminder Singh
Designation: Professor
Department: School of Computer Science and Engineering
University: Lovely Professional University, Punjab, India
Date: 15.04.2025

ABSTRACT

Medical records are often kept on paper. However, the conversion of paper medical records to Electronic Health Records (EHRs) is now possible because to modern information and communication technologies. Therefore, safeguarding user data privacy is essential in healthcare environments. Finding a way to improve patient data security without sacrificing EHR system functioning and interoperability is one of the fundamental challenges. Privacy protection for electronic health records is becoming an issue that the general public is becoming more and more interested.Current EHR management systems prioritize safeguarding user privacy information above the security risks that occur when patients engage with several roles. There is currently no adequate solution to the problem of insurance companies accessing confidential patient information and violating their privacy. Users' privacy is under threat due to the increasing number of reported data breaches that jeopardize the current system, as third parties manage and obtain large amounts of personal data. In addition to identifying possible research gaps in the literature, this systematic mapping study aims to evaluate the state-of-the-art research on security and privacy needs in EHR systems. The major difficulties lie in figuring out how to increase the security of patient data while maintaining the functionality and interoperability of EHR systems. The volume of patient data stored in Electronic Medical Records (EMRs) makes preserving patients' privacy a growing priority that should not be minimized or disregarded. This study proposed a novel privacy model based on Machine Learning (ML) techniques and the conceptual privacy K-ANONYMITY for EHR systems. It highlights the difficulties that EHR systems now face, including striking a balance between user friendliness, privacy and accessibility, and regulatory compliance. The research created

a universal privacy model to effectively manage and exchange patients' sensitive and private data across various platforms in order to solve these issues.The most accurate method among them was gradient boosting, demonstrating the efficiency of our ML-based method in detecting insufficient privacy rules.

This study describes future paths for research, highlighting the need for thorough assessments, testing in real-world case studies, exploring adaptable frameworks, ethical considerations, and encouraging stakeholder participation. This study presents a novel strategy for improving the privacy of healthcare information, laying the creative groundwork for further research in this area. A sophisticated method for storing medical data, conducting medical transactions, and building trust in the integration and interchange of medical data within a decentralised international healthcare network is provided by Blockchain Technology . While the healthcare sector has shown significant interest in Blockchain Technology, concerns around privacy and security remain the main areas of disagreement when considering using blockchain for exchanging medical data. This study offers a block chain-based solution to all of the aforementioned problems. Using Bitcoin smart contract technology and homomorphic encryption, we created a feature with Blockchain Based Secure Multiple Computations Scheme using Health Care Data (BSMPCS) that allows the insurance company to decide whether to execute insurance requests even in the absence of a way to get the ID and plaintext of the EHR. Consequently, we ensure that no uninvited parties reveal any private patient information during communication, thereby enhancing user data privacy and security. The Machine Learning Privacy-Preserving Model (MLPPM) employs Fully Homomorphic Encryption (FHE) to ensure data privacy and security while performing machine learning tasks. By performing computations on encrypted data without decrypting it, FHE maintains confidentiality throughout for developing an MLPPM model that leverages the Cheon-Kim-Kim-Song-Residue-Number-System (CKKS-RNS) FHE scheme and bootstraps to overcome the constraints of conven-

tional FHE techniques.Existing models like CryptoNet, SEALion, and CryptoDL primarily cater to basic or nonstandard machine learning models and have demonstrated limited effectiveness with more sophisticated datasets. These methods typically replace non-arithmetic activation functions with approximations before bootstrapping, restricting the model's depth and complexity. This study shows a strong way to do deep learning on encrypted data by using CKKS-RNS and advanced approximation methods for functions that aren't math, like ReLU and Softmax. Validated our ResNet-50-based model using the MNIST dataset, demonstrating high accuracy and performance. The proposed MLPPM model achieved a classification accuracy of 92.43 % ,closely aligning with the original ResNet-50 model's accuracy of 91.89 % . We have developed a block chain-based solution to address all the previously mentioned issues. Using Bitcoin smart contract technology and homomorphic encryption, we created a feature with BSMPCS that allows the insurance company to decide whether to execute insurance requests even in the absence of a way to get the ID and plaintext of the EHR. Consequently, we ensure that no uninvited parties receive any private patient information during communication, there by enhancing user data privacy and security.

ACKNOWLEDGEMENT

I would like to present my deepest gratitude to Dr. Parminder Singh for his guid- ance, advice, understanding and supervision throughout the development of this thesis and study. Despite his busy schedule he has been available at every step, devoting time and energy and the much needed counsel and advice. This enabled me to sail through the tough times and complete this enormous task. I would like to thank to the research project committee members for their valuable comments and discussions. A special thanks to the management of Lovely Professional Uni- versity for their support in academic concerns and letting me involve in research study. The doctoral programme of LPU has made it possible for me to pursue my dream of research and upgrade my knowledge. My sincere feeling of gratefulness also goes to my parents and family members who always motivated me in all the endeavors of my life including this research work in LPU. I am also thankful to my Father B.Ramu for offering full support to me during the entire period of my research work. My special thanks to my daughter D.Sree Priyanka and my son D.N.S.Nikhil for giving me joyful and happy moments during the entire journey of my research work. Finally, I would like to thank each and every person who has directly and indirectly helped and motivated me in this journey.

(Signature of Scholar)

Name of the scholar: B.Vasantha Rani

Registration No.: 41900163

Department/School: School of Computer Science and Engineering

Place: Lovely Professional University, Punjab, India

Date: 15.04.202

Contents

Candidate's Declaration **i**

Certificate **ii**

Abstract **v**

Acknowledgement **vi**

Content **x**

List of Tables **xi**

List of Figures **xii**

List of Abbreviations **xiii**

1 INTRODUCTION 1

1.1 Introduction 1

1.2 Blockchain 2

1.2.1 Blockchain Types 4

1.2.2 Smart Contract 4

1.3 Blockchain Platforms and Distributed Storage 6

1.3.1 Bitcoin and Cryptocurrencies 7

1.4 Bitcoin for Preserving the Confidentiality of EHRs 15

1.5 Existing Methods in Bitcoin 18

1.5.1 Components of the Health chain Framework 19

1.6 Security and Privacy for Cloud-Based E-Health Data 20

1.6.1 Methods for Protecting Patients Confidentiality in EHRs . . 23
1.7 HE: Preserving Privacy in EHRs..25
1.8 Research Gaps... 30
1.9 Objectives.. 30
1.10 Research Methodology 30
1.11 Summary 33
1.12 Organization of the Thesis.. 33

2 RELATED WORK 35
2.1 Introduction.. 35
2.2 Evolution of EMRs in Modern Healthcare 35
2.3 Adoption Challenges to EMR Implementation 36
2.4 Security and Privacy Challenges in EMR Systems 37
2.5 Cloud-Based EMR Storage: Opportunities and Limitations.................. 38
2.6 EMR Security Challenges with Bitcoin 38
2.7 AI-Enabled Blockchain for Enhanced EMR Management 39
2.8 ECC Cryptography and its Impact on Blockchain 42
2.9 Hybrid Homomorphic Encryption 43
2.10 Data Handling in Blockchain... 46
2.11 Security Concerns in Blockchain 48
2.12 Research gaps 49
2.13 Summary 49

3 Blockchain in Healthcare: An Evaluation of Literature, Frameworks and Recommendations 53
3.1 Introduction.. 53
3.2 Blockchain's Need in Healthcare 54
3.2.1 Functionalities of Blockchain in Healthcare.............................. 55
3.3 Privacy in Healthcare 56
3.3.1 Interoperability and Standards... 56
3.3.2 Workflow Process for Blockchain in Healthcare 57

3.4 Blockchain Applications in Healthcare 58

3.4.1 Search Strategy 58

3.4.2 Databases and Search Techniques 59

3.4.3 Difficulties Associated with Security 59

3.5 Discussion 61

3.5.1 Future Recommendations 62

3.5.2 Difficulties Associated with Privacy 62

3.5.3 Access Control Problems in Medical System 63

3.5.4 Limitations 63

3.6 Summary 63

4 Deep Neural Network and Fully Homomorphic Encryption - Based Privacy Preserving Model for EHR 65

4.1 Introduction 65

4.2 Proposed Methodology 69

4.2.1 CKKS-RNS Scheme 69

4.2.2 Novelty for ResNet-50 ON CKKS-RNS Scheme 70

4.3 Implementation of Resnet-50 on CKKS-RNS 71

4.3.1 Setup in General for the CKKS-RNS Scheme 72

4.3.2 Data Range and Precision 73

4.3.3 Optimizing the Accuracy of Homomorphic Operations 75

4.3.4 Implementation of ReLU Function 75

4.3.5 Pooling Averages and Fully Connected Layer 76

4.3.6 Simulation Results 77

4.3.7 Discussion 78

4.4 Summary 79

5 Blockchain-Based Secure Multiple Computation Scheme for Preserving and Extraction of Health Care Data 81

5.1 Introduction 81

5.2 Background Work 83

5.2.1 Blockchain-Based Secure Multiple Computation Scheme……… 83
5.2.2 Smart Contract ………………………………………………………………. 84
5.2.3 Bitcoin ……………………………………………………………………………. 84
5.2.4 IPFS ……………………………………………………………………………. 84
5.3 Methodology ………………………………………………………………………….. 85
5.4 Proposed System ………………………………………………………………………. 88
5.5 Evaluation …………………………………………………………………………….. 91
5.5.1 Homomorphic Encryption……………………………………………… 91
5.5.2 Algorithm for Registering Patients …………………………………… 92
5.5.3 Algorithm for Insurance Medications …………………………… 93
5.5.4 Algorithm for claim for insurance …………………………………… 94
5.5.5 Algorithm for Doctor ………………………………………………… 95
5.5.6 Algorithm for accessing the Patients data for treatment ……… 95
5.5.7 Algorithm for treatment and insurance …………………………. 96
5.5.8 Algorithm for treating a patient ……………………………………… 96
5.5.9 Compute contract ………………………………………………………. 98
5.5.10 MPS protocol ……………………………………………………………… 98
5.5.11 Fairness robustness analysis ……………………………………… 98
5.6 Experiment Evaluation ……………………………………………………………. 98
5.6.1 Evaluation...104
5.7 Summary 108

6 CONCLUSION AND FUTURE SCOPE 110
6.1 Conclusion...110
6.2 Future Scope 112

Publications 140

A Appendix 131

List of Tables

2.1 Summary of Key Contributions 51

3.1 Findings from the work 59

3.2 Findings from the work 60

4.1 The ResNet-50 standard 73

4.2 Comparision of various models 77

5.1 Metrics 104

5.2 Transaction and execution cost 107

5.3 Performance comparision analysis 108

List of Figures

1.1 Blockchain with valid data 3

1.2 Blockchain with tampered data 3

1.3 Blockchain types 5

1.4 Submission of a smart contract to a BN 5

1.5 Categories of privacy preserving mechanisms 24

1.6 Workflow model 32

1.7 Organisation of thesis 34

3.1 Blockchain in the medical field 55

4.1 Stride-2 convolution 71

4.2 Structure of ResNet-50 74

4.3 ResNet-50's architecture for the CKKS-RNS scheme 76

5.1 EHR privacy model in Blockchain 89

5.2 Flow of Homomorphic Encryption process 90

5.3 Homomorphic Encryption process in EHR-PP model 92

5.4 Sequence diagram for EHR report in Healthcare System........................101

5.5 Transaction upload and download execution time 102

5.6 Execution time for block mining and block creation 103

5.7 Running time for transaction access by number of nodes....................103

5.8 Working mechanism of Homomorphic Encryption.................................105

5.9 Encryption process in ElGamal encryption algorithm 106

5.10 Decryption process in ElGamal decryption algorithm 106

List of Abbreviations

ABAC	attribute-based access contro
BFT	Byzantine Fault Tolerance
CKKS	Cheon-Kim-Kim-Song
CSP	Cloud Service Provider
DoS	denial-of-service
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
EMR	Electronic Medical Record
EPCBIR	Efficient and Privacy-Preserving Content-Based Image Retrieval
HE	Homomorphic Encryption
HIPAA	Health Insurance Probability and Accountability Act
IDEA	IDEA International Data Encryption Algorithm
IPFS	InterPlanetary File System
ML	Machine Learning
MPC	multiparty computation
MSP	Membership Service Provider
NTT	Number Theoretic Transformation
PCEHR	patient Controlled Electronic Health Record System
QoS	Quality of Service
ReLU	Rectified Linear Unit

RESNET	Residual Network
RNS	Residue Number System

Chapter 1

INTRODUCTION

1.1 Introduction

The healthcare sector has changed as a result of the extensive use of electronic health records, enabling efficient data management, improved patient outcomes, and better-informed clinical decision-making. However, this digital transition has also introduced new challenges, patient privacy, including data security, and interoperability across healthcare providers. Bitcoin, with its inherent properties of decentralization, transparency, and immutability, emerges as a promising solution to address these pressing concerns. A cryptographic technique called Homomorphic Encryption (HE) makes it possible to perform computations on encrypted data without the requirement for decryption. This method is used in our solution, which further improves patient data confidentiality and privacy [1]. The healthcare sector stands to gain a great deal from the integration of Bitcoin into electronic health record systems. This is because Bitcoin tackles major challenges relating to the management, integrity, and security of data. The decentralised structure of blockchain, in which data is maintained across numerous nodes, reduces the need for a centralised authority. This minimises the danger of data breaches and ensures that patient records are kept in their original state. In addition, the irreversible nature of Bitcoin makes it possible to create a tamper-evident audit trail, which in turn enables more accountability and openness in the provision of healthcare.

1.2 Blockchain

In addition to improving data integrity and advancing democratic values in the healthcare industry, a blockchain-based system puts patients at the centre of the system by empowering them with ownership over their data. Ledger system characterised by its inherent data non-repudiation and immutability, connected by an increasing series of records referred to as blocks. Blockchain constitutes a decentralised ledger technology. There are two main forms of distributed ledger network technologies: permissioned and permissionless blockchain systems. These technologies are able to accommodate With many different uses and a vast range of consequences, both technically and practically. Individuals are able to participate as nodes in the network of permissionless. This is because public blockchains do not have any network barriers that prevent them from doing so. Unlike the public blockchain, the permissioned blockchain, referred to as the private blockchain, encompasses Hyperledger Fabric. This kind of blockchain utilises an access control mechanism to decide whether or not a new node should be added to the network [1]. The technology that underpins Bitcoin is known as blockchain, and it is this technology that makes it possible for this cryptocurrency to verify a reliable third party.When it comes to online payment systems and digital currencies, Bitcoin [2] is the first and biggest decentralised digital money. Satoshi Nakamoto was the one who first presented it in 2009, and it meant that central banks were replaced by computer nodes that were operating all over the globe to authenticate transactions. The cryptocurrency known as Bitcoin is founded on evidence rather than trust, and it functions in an environment that is fully distributed and does not need any reliable third parties. Blocks constitute the records that form the blockchain, an expanding assemblage of data interconnected by encryption. Each block may include health-related data or financial activities. The Genesis Block, the first transaction in a blockchain, uniquely lacks a hash of its predecessor. Blocks are connected by hash values, therefore even a little change to one block's content might alter its hash and render all future blocks invalid as shown in Figure 5.1. A number of essential characteristics are made possible by the blockchain's one-

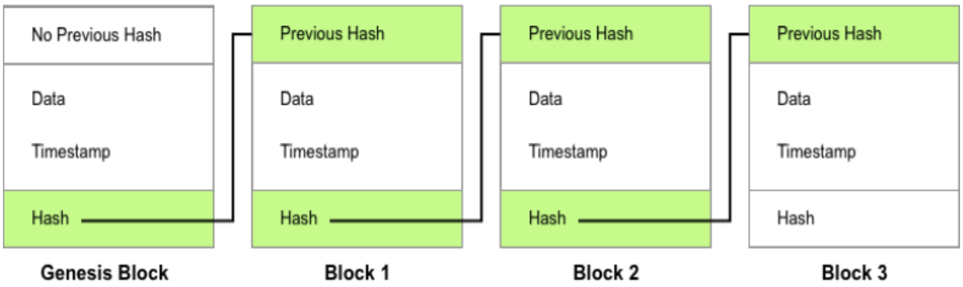


Figure 1.1: Blockchain with valid data

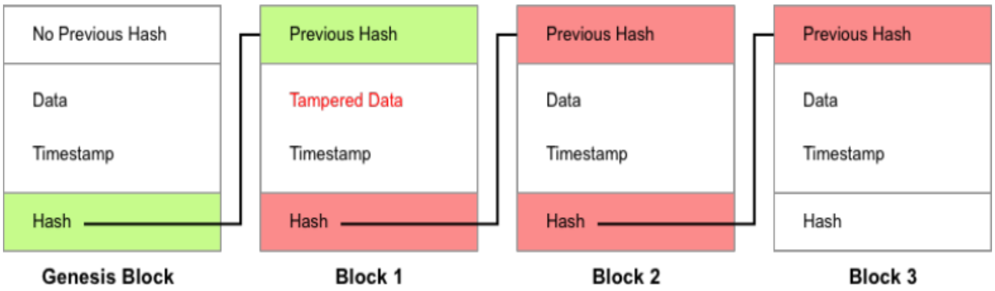


Figure 1.2: Blockchain with tampered data

of-a-kind structure: A Blockchain Network is distributed in the sense that result, Consequently, the network becomes more stable as it lacks a single point of failure. Each node independently verifies the data before adding it to the ledger, ensuring that the ledger is secure.

Records that are recorded in a blockchain are both visible and traceable since the ledger will forever maintain the history of all data alterations. This makes the records immutable and transparent. Many different technologies come together to form a blockchain as shown in Figure 5.2.

The following is a list of the most important technologies that operate inside a Blockchain Network:

1. The design of Blockchain Networks is dispersed, and nodes are connected to one another. Peer-to-peer communication methods, such as BitTorrent, are used in order to establish connections between participants in a Blockchain Network[3].

2. There are hash algorithms, such as MD5 [4], that are used for the purpose

of protecting data from being manipulated.

1.2.1 Blockchain Types

Since its inception in 2008, the Bitcoin has been the basis for the development of a great number of applications. Based on two different variables, we are able to classify them.
Validators Right to Remain Naked: In a Blockchain Network, the nodes that are responsible for validating transactions are referred to as validators. It is pos- sible for validators to be either public or private inside a Blockchain Network. Blockchain Networks that include public validators make it possible and validate transactions.They are required to first receive the requisite certifications that are described by the protocol. Bitcoin [5] and Ethereum [6] .

Therefore, proof-based consensus techniques are used by the nodes in a permissionless blockchain rather than trust-based ones. This is because the presumption in a permissionless blockchain is that everyone has the capacity to be corrupt. Proof-based consensus methods, on the other hand, need a significant amount of time and have a high energy consumption. Permissioned blockchains, on the other hand, are designed to attain a better scalability rate by distributing the trust across a predetermined group of participants as shown in Figure 4.3 .For exam- ple, the Ethereum Casper blockchain requires permission to use, but the Bitcoin blockchain does not.

1.2.2 Smart Contract

Traditional contracts have been reimagined as computerised forms known as smart contracts. Once certain criteria that have been described by contract writers are satisfied, they are a collection of procedures that have been created by the designer of the Blockchain Network. Within the context of smart contracts, the contract is enforced by a computer program, which eliminates the need for any third parties to intervene. A number of parties must reach a consensus on the terms of a contract in order to form a smart contract. They then submit the

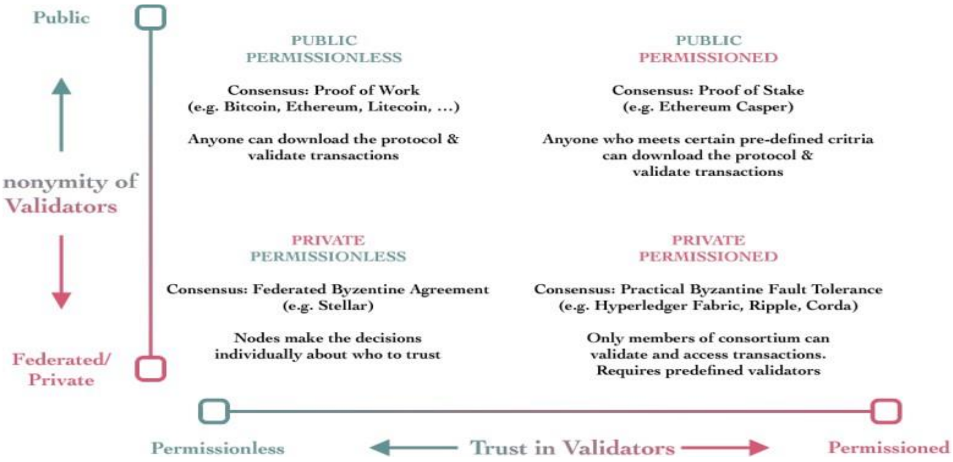

Public
nonymity of
Validators
Federated/
Private
PUBLIC
PERMISSIONLESS
Consensus: Proof of Work
(e.g. Bitcoin, Ethereum, Litecoin, ...)
Anyone can download the protocol & validate transactions
PUBLIC
PERMISSIONED
Consensus: Proof of Stake
(e.g. Ethereum Casper)
Anyone who meets certain pre-defined critria can download the protocol & validate transactions
PRIVATE
PERMISSIONLESS
Consensus: Federated Byzentine Agreement
(e.g. Stellar)
Nodes make the decisions individually about who to trust
PRIVATE
PERMISSIONED
Consensus: Practical Byzantine Fault Tolerance
(e.g. Hyperledger Fabric, Ripple, Corda)
Only members of consortium can validate and access transactions. Requires predefined validators
Permissionless
Trust in Validators
Permissioned

Figure 1.3: Blockchain types

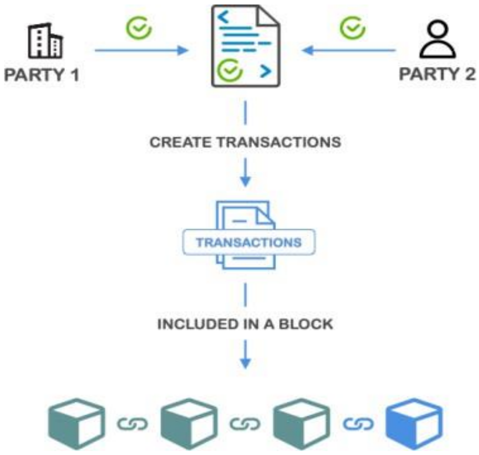


Figure 1.4: Submission of a smart contract to a BN

smart contract to the blockchain ecosystem for final confirmation after integrating it into a transaction. The smart contract is subsequently automatically executed anytime the predetermined conditions are satisfied once it has been deployed to the blockchain as shown in Figure 5.3.

1.3 Blockchain Platforms and Distributed Storage

The selected approach in the proposed framework is justified by comparing is made in order to support the technique that was chosen. Some of the most prominent blockchain systems, including Ethereum, Ganache, Quorum, and Hyperledger Fabric, are discussed in this document. As an additional feature, we investigate a number in-depth analysis of the Inter Planetary File System that has been sug- gested.

As a permissionless BN that is distributed and open source, Ethereum comes equipped with a Turing-complete programming language that is built in. This language allows anybody to use it to construct decentralised applications,via the use of smart contract capabilities [7]. These smart contracts make use of a strong cryptographic consensus protocol mechanism known as Proof of Work. Block mining takes place in the permissionless network. Ether, which is analogous to a crytocurrency, serves as the driving force behind each and every transaction that takes place on Ethereum. Due to the fact that the network is open, trustless, and decentralised, anybody is able to join it; guard against assaults that are directed against ledger changes, which makes the network susceptible. Ganache is limited to supporting a maximum of ten Ethereum addresses and is unable to engage in network mining activities due to the absence of miners embedded inside the network. Quorum is an additional Ethereum client blockchain that has been enhanced with corporate functionality. This functionality includes enhanced performance in a private network, client permission, and privacy features such as encryption and encryption. In spite of the fact that it includes a robust RAFT consensus algorithm that can handle transactions in fifty milliseconds or less, there are still problems about scalability and privacy when it comes to using it to a health data network. Due to the fact that Hyperledger Fabric offers a greenhouse structure that can be adjusted according to the requirements of the organisation, it is suitable for applications in the healthcare industry.

Transferring power from a centralised institution to a system that is more broadly spread is what we mean when we talk about decentralisation. Blockchain technologies include Ethereum and Bitcoin that decentralise financial transactions and information systems. The word ”decentralisation” is now being used in connection to these forms of technology, despite the fact that the present storage systems are restricted and that they leak data. It is a system that allows for the storage of information without the need to answer to big, centralised data silos. This makes it possible for data to be kept in a manner that is both decentralised and safe. In specifically, the major goal of Swarm is to store and disseminate Decentralised Application (DAPP) code and data as well as blockchain data. One of the key objectives, In addition, Siacoin is a platform that offers incentives, much like Storj.

IBM and the Linux foundation collaborated to build Hyperledger Fabric, a permissioned blockchain platform designed for business blockchain applications. In order to achieve its goals of robustness, flexibility, and secrecy, the Fabric design applies a paradigm known as execute-order-validate. This paradigm assigns distinct duties to each node in the network. Among the following jobs, this might be one of them: 1) Clients provide the transaction suggestions for the purpose of being carried out 2) Transaction proposals are carried out by peers, and transactions are validated by peers. All peers uphold the ledger, wherein transactions are documented as a hash chain.

1.3.1 Bitcoin and Cryptocurrencies

At current moment in time, internet business and e-commerce are seeing rapid expansion, and the majority of online payments are processed by third parties that are trusted by the companies involved. The financial institution that acts as a third party encounters a number of limits and defects, including those pertaining to cost, time, and storage, in addition to concerns about security. There is no attempt made to prevent the irreversibility of the transaction in order to resolve the disagreement via mediation. If the transactions are carried out in person and with cash, then all of these problems may be avoided. In light of the fact that this is rapidly evolving, a new system that does not rely on a central authority is required to guarantee that the payments are legitimate and devoid of fraud. Because of the pandemic, there is an increased need for a new technology that is both cutting-edge and capable of providing security. During the year 2008, a comparable electronic payment method was introduced [8]. Someone, an organisation, or an unknown individual with the moniker Satoshi Nakamoto came up with the idea first. Satoshi's proposal was based on the concept of using cryptographic-proof techniques to develop an electronic system that would allow parties to conduct transactions without the requirement for third parties to be involved. As a result of the invention, a new technology that is today known as BT was developed. A greater degree of adaptability has been achieved by this technology as a result of its widespread use, versatility, usefulness, and accessibility. This technology eliminates the need for a middleman in the payment process and eliminates the issue of duplicate spending. In the context of cryptocurrency transactions, such as Bitcoin exchanges, it functions as a protocol. Bitcoin, the very first cryptocurrency, was the first to use this for trading purposes. It offers a probabilistic strategy, which allows it to address a very well-known issue in computer science known as ”The Byzantine Generals Problem.” This challenge raises problems about the consensus about distributed systems [9]. Numerous other crypto currencies came into being and quickly acquired popularity there after.

cryptocurrencies: Bitcoin is considered by some who are involved in the cryptocurrency sector to be the internet's equivalent of the gold standard. The first cryptocurrency to be released into the market was Bitcoin. exchange assets be- tween two individuals who are not subject to the authority of a single entity. Of all the cryptocurrencies now available on the market, it has the most widespread brand awareness. Bitcoin is not susceptible to fabrication or inflation in any form. The main goal of the blockchain for Bitcoin is to ensure that records of ownership of digital currency are kept.

Ether: Swiftly ascended the ranks of the market capitalisation of cryptocurrencies to grab the second place position. In the near future, Ethereum is expected to surpass bitcoin. The Ethereum Blockchain is primarily concerned with the Ethereum Network, which may be thought of as the execution of individual computer programs. Because of the evolution of Ethereum, a single platform has the potential to host thousands of different applications [10].

When it was first released in 2011, Litecoin had the intention of eventually becoming silver. Litecoin was designed in order to address the inadequacies of Bitcoin itself. As a result, the time required to create a block for litecoin is around 2.5 minutes, while the time required for bitcoin is 10 minutes. Moreover, it is capable of managing a greater number of transactions per second. Additionally, double spending may be prevented by reducing the block time length [11].

A distributed database, a decentralised network, and a digital ledger that is able to store and update data in an efficient manner are some of the characteristics that constitute Bitcoin. By employing the traditional procedures that are used in the financial industry, peer-to-peer networks that are constructed on nodes have the potential to store and connect more general assets. It is often referred to as three-dimensional technology. In order to prevent any changes from being made to the data, cryptographic algorithms and encryption methods are used to safeguard it. Every transaction is linked to one another via the use of hashes, and it is then kept as a block that has been time stamped. BT relies heavily on both cryptography and hashing to perform its critical functions. For the purpose of recording the transactional facts, the Merkle tree concept is used [11].

The operation of Bitcoin is shown by the fact that a decentralised system is managed by its users directly, without the participation of any intermediaries or central authority from the outside. It simplifies the process of transmitting money to any other node or user on the network, eliminating any potential complications. To put it another way, Blockchain makes it possible to make payments to everyone on the network in a quick and efficient manner. A cryptocurrency, such as Bitcoin, is made up of a network of peers that operate independently of one another. On file, each peer has a copy of the whole transactional history that has been recorded.

This illustrates that bitcoin is protected by clever mathematical computations rather than by persons who can be trusted. It makes no difference to blockchain if a cryptocurrency represents a certain quantity of dollars, cursors, or any other unit of measurement. It is up to the nodes to decide the currency unit they will use. There are a variety of transactions that may be conducted using BT, not only those that are linked to payments and finances. Several other commodities, such hundreds of barrels of oil, award credits, or an electoral vote, are all examples of things that may be represented by a cryptocurrency. The user is the one that initiates both the transaction and the building of the block first. The newly created block has to be validated across every node that comprises the BN. The transaction is not considered finalised at the receiving end until the block has been added to the Blockchain, which occurs only when confirmation has been completed. Following the completion of the transaction, the dispersed network subsequently receives an update [12].

Implementation of Bitcoin : Before trying to apply Blockchain in conventional applications, it is vital to evaluate whether or not the technology is compatible with all existing systems and whether or not it produces beneficial results. Following the completion of the study, a decision tree was developed in order to choose this and then apply it to the system that is most suitable for it. In order to make a choice, one may take into consideration the characteristics of an application, which include the required degree of trust, the speed of transactions, the secure system, authorisation, and the capability to prevent reversibility. This is a representation of the Decision Tree that will be used to assist in the choosing of procedure. Following the tree, there are two fundamental sorts of ledgers: permissioned blockchains, which are private, and permissionless blockchains, which are public. If one continues to be interested in using the rapidly expanding technology, there are two types of ledgers.

1. Whether the Blockchain will be public or private is something that is decided by the Functional Requirements. The Permissioned Block is mined by verified miners who have been granted permission to do so. A miner

who is permitted to do so will be in charge of managing the Permission Blockchain network. It is possible to configure each and every function in a network that has permissions in accordance with the rights that ought to be given determined by the platform. According to [13], the main responsi- bility of the block miner is to validate a transaction. A miner is eligible to earn compensation if they are able to successfully complete the verification process.

2. Using a transaction ID, each and every transaction that is recorded in the ledger may be recognised. Specifically, the public key of the sender and the public key of the recipient are used to determine the contents of the transaction. The amount that is going to be sent to the beneficiary, in addition to the fees that are going to be charged for the verification of the transaction, is referred to as the ”input” in the transaction. The output in this case indicates the total amount of money that is now accessible in the user’s wallet.

Bitcoin Protocols : Within the realm of computer science, a protocol may be defined as either a set of principles or a method that regulates the transfer of data between different technological devices. Because of this, it is much simpler for computers to connect with one another and exchange information in an appropri- ate way by adhering to already established standards. Specifically, the protocol specifies the format of the data that will be sent and received by the parties [14]. DNS and TCP/IP are the protocols that are used the most often on the internet. The word ”blockchain” describes a dispersed collection of computers, also known as ”nodes,” that are connected to one another in a network via the use of the In- ternet. All of the computers (nodes) that are members of this distributed system and that are attempting to establish connections with one another have reached a consensus on a set of rules that have been predetermined and control how the system functions. A set of standard rules must be adhered to by networks in order for them to function properly. The governance of the BN that is responsible for controlling all of the nodes that are participating is referred to as the protocol.

This section [15] contains a list of many procedures.

First and foremost, it was developed for the digital money known as Bitcoin. All bitcoin transactions are conducted in accordance with the rules and restrictions that are outlined in this protocol.

These are the objectives that the Bitcoin Protocol aims to accomplish:

1. Due to the fact that the Network is public in nature, anybody who has both private and public keys is able to join it.

2. One is able to join this form of network without first obtaining authorisation.

3. The implementation of technical components consensus mechanisms, Peer- To-Peer (P2P) networks, digital signatures, encryption, and cryptographic hashing algorithms should be included.

4. All of the information that is stored on the Bitcoin Blockchain will be ac- cessible to any system that is connected to this network.

5. As a result of the fact that nodes are able to carry out transactions that cannot be undone, trust may exist without the participation of third parties.

Ethereum Protocol is a decentralised platform for Bitcoin. Because it is open source, Ethereum makes it possible for developers to construct and run Decentralised Applications (DApps) without the need for support from other parties. Application creation is made easier by Ethereum's native programming language, which is used for the platform. On July 30, 2015, the Ethereum main net was made available to the public. The implementation of Ethereum's concepts in a manner that is more generalised is accomplished by the use of programming in general ways (all-in-one blockchain approach). Vitalik Buterin was the one who came to the conclusion. In addition, it makes it possible for multiple of these resources, each of which has its own state and programme that is now executing, to communicate with one another by using a framework that is designed for mes- sage passing. The Ethereum MainNet is accessible to each and every person that has access to the internet. Any anybody who has access to the internet is able to generate transactions, verify them, and add them to the Ethereum production Blockchain. In addition, those connected to the main network may be able to access the recorded transaction. [16]

Intelligent Contracts : A ”Smart Contract” is a piece of code which is built on Bitcoin that is used to facilitate, execute, and enforce any conditions of an agreement between unreliable parties. When it comes to the Blockchain, smart contracts are agents that are self-sufficient and self-verifying. An IF-THEN logic structure might be used to indicate the requirements or rules that are included in the agreement; however, the agreement is much more than that. Ethereum is an implementation of the Blockchain that makes it possible to use smart contracts, which in turn increases the usefulness of the product. A contract is a complete collection of code (modules) and data (context) that is created in Solidity and is kept on the Ethereum Platform at a specific address. Contracts that are able to carry out and enforce their own conditions are referred to as smart contracts. In order to regulate them, the terms and conditions that are specifically specified within them are applicable. In his article, Szabo asserts that physical vending machines are a ”ancient predecessor of smart contracts.” As well as a product, they are given coins and are responsible for providing the appropriate change in accordance with the price that has been indicated [17].

While ”smart” refers to anything that demonstrates quick thinking, ”contract” refers to something that is intended to be upheld by a court of law or other agreement. A ”smart contract” is an intelligent agreement that is automated, self-verifiable, and written in a computer language based on JavaScript. The Ethereum platform was the first to introduce smart contracts. For instance, smart contracts are instances of bespoke logic that has been installed. The Ethereum Virtual Machine(), often known as the EVM, can carry them out. With the use of smart contracts, it is now feasible to create transactions and transfer them across accounts. They are similar to classes in object-oriented programming in a number of aspects. Calls are the means by which smart contracts communicate with one other. Certain functions could be started during the instance creation process, and specific logic might be used to update the contract's contents. During the process of developing the Smart Contract, three significant areas of study, including anonymity, privacy, and confidentiality, are given priority. With the technology sharing all of the data without any checks or barriers, anonymity is a worry that has to be addressed. Users are able to generate an unlimited number of addresses, which has an impact on their identity. One cryptocurrency that has been suggested is called zero cash, and it is designed to fulfil privacy criteria by concealing all information other than the transactions [18]. It is also possible to achieve cryptocurrency privacy by using coin mixing techniques that are compatible with Bitcoin in order to establish an entirely new cryptocurrency. In his definition of a smart contract, A digital representation of it is what we mean when we talk about a smart contract.A lot of the definitions of smart contracts that were proposed by Sean and Cooper were taken into account by the author. Rather than being written in plain English, smart contracts are constructed using computer code. This is the defining characteristic of smart contracts.

Cryptography : Inside the context of the cloud, the term ”cryptography” refers to a technique that may be used to acquire data that is either stored or utilised inside the cloud. It is possible for consumers to make use of shared cloud services in a way that is both helpful and safe since all of the information that is offered by cloud providers is secured for their protection. Over the course of the eigh- teenth century, the term cryptograph, as opposed to cryptogram, has been used for the majority of the time. Up until quite recently, the word ”cryptography” was solely used to refer to encryption, which is the act of transforming plaintext (information that is normally understood) into ciphertext (structure that is not understandable). Decoding is the opposite of decoding, which is the process of retrieving plaintext from scrambled ciphertext. There are a few calculations that make up a cypher (also known as a cypher) that are responsible for switching de- coding and encryption [19]. Together, the algorithm and a ”key” are responsible for governing the particular actions that are carried out by a cypher. The private key, which is often a string of characters that may be used to decipher ciphertext, is meant to be known only by the individuals who are communicating with one another. In the past, cyphers were usually employed directly for the purpose of encrypting or decoding data without the necessity for any further processes, such as verification or credibility checks. To talk more generally, there are two sorts of cryptosystems, which are as follows:

Cybersecurity based on symmetry : Before the 1970s, these systems used the same key for both encrypting and decrypting a message. This practice continued at that time. When contrasted with asymmetric cryptography, the length of the key that is used in symmetric cryptography is rather short by comparison.

An example of a symmetric algorithm in use for a considerable amount of time. AES is among the most extensively used encryption algorithms.

asymmetric : It is the ”public key” that is used in asymmetric systems for the purpose of scrambling a message, whereas a connected ”private key” is utilised for the purpose of unscrambling the message. Additionally, these two keys are linked to one another in some way. One of the reasons why this method makes the discussion more safe is because it is so difficult to detect the link between the two keys. This is one of the reasons why this strategy is so effective[20]. Both of these algorithms are instances of symmetric algorithms.

1.4 Bitcoin for Preserving the Confidentiality of EHRs

As EHRs are housed on centralised systems in silos, the security risk footprint is increased. Moreover, reliance on a one authority is essential, which is incapable of sufficiently safeguarding data from internal threats.. One of the challenges that the healthcare sector is now facing is a lack of interoperability in EHR. The absence of interoperability hinders the aggregation and evaluation of patient data. The fragmented nature of health data in the existing systems makes it difficult to exchange information with healthcare providers or other interested parties since these systems use diverse formats and standards. Internal attacks, in which individuals who have authorised senior management inside organisations, are the attackers, are a serious problem in respect to health records that are stored in cloud servers. These assaults are far more severe than external attacks. under the systems that are already in place since service providers are the ones who are in charge of managing them. Patients may be left susceptible to assaults that have exacerbated cyber risks [21] EHRs. Centralised databases can leave patients vulnerable to attacks.

E-Health, which stands for ”electronic health”, is a term that describes the use of information and communication technology in the medical field. Healthcare sector as a result of the development of industry 4.0, which enables the Internet of Things (IoT), mobile technologies, wearable devices, and artificial intelligence. There have been significant developments in the healthcare sector brought about by the advancements in industry 4.0. These advancements include improved treat- ment quality, greater communication, remote monitoring, and a reduction in costs, among other benefits. EHRs mobile health, and anything else that falls under the umbrella of e-health are all included. According to Eysenbach (2001), the letter ’E’ in e-health is also a symbol for the ten E’s, which are as follows: efficiency, evidence-based care, enhancing the quality of care, education, empowerment, en- couragement, expanding the scope of health, enabling information sharing, ethics, and equity.

Privacy preserving data publishing has gained good attention among researchers in the recent years. Healthcare data publishing is crucial for medical research such as innovative medicine, early diagnoses, and accurate treatments. Health- care organizations generally collaborate with research and development teams or pharmaceutical companies to perform data analytics. Healthcare organizations collect personal information from the patients. The collected data may contain personal identities, medical history, diagnosis, and test results. Such data possess huge volume of information for healthcare research. Hence, before publishing the data to the third party researchers or pharmaceutical companies the healthcare organizations should abide to the ethical and government regulations to protect the privacy of the individuals. To protect the privacy, healthcare organization needs to transform the data that does not leaks the personal information. Privacy protected version is called anonymization.Anonymized version of the data can be shared among the third party researchers for data analytics. Hence, it is important that the anonymized version of the data provides proper data utility.

Privacy preserving data publishing process comprises of three phases: data collection phase, data anonymization phase and data publishing phase. Data collection phase consists of data generation and data preparation phases. In data generation phase, the data is generated by patients, physicians, doctors, lab technicians, and medical devices. The data controller then processes the produced raw data during the data preparation stage. The data controller prepares the data for publishing without the personal identities of the patients. In data anonymization phase, the data controller applies privacy preserving anonymization techniques to protect the data. The anonymization techniques transforms the specific details of individuals to less specific details. Then in data publishing phase, the anonymized version of the healthcare data are shared with the third party researchers and pharmaceutical companies.

The Patient Controlled Electronic Health Record System(PCEHR) employs BT as a solution to address the predominant limitations of the existing distributed environment. In this approach, the patient universally consents to the sharing of personal data with all stakeholders, except in cases deemed emergencies. These blocks are interconnected to form a chain secured using public key encryption cryptographic principles. Blockchains are unalterable and publicly visible.

Due to the fact that the blocks are connected, after the data have been recorded, it is not possible to make any changes to them retrospectively with- out also modifying all of the blocks that come after them. Additionally, it makes use of a scripting language in order to execute intelligent smart contracts [23]. Our study takes use of the inherent qualities of BT in order to construct a prospective framework that offers assistance for the transition. This framework is designed to meet use cases in the health care industry place between the entities that are part of the Health chain network.

These EHR are stored in the Inter Planetary File System (IPFS) in order to construct this private Healthchain network. The Healthchain framework is constructed on Hyperledger Fabric, which is a permissioned distributed ledger solution. Hyperledger Composer is used to create the framework.

IPFS, which is a decentralised storage system. In addition, the Healthchain architecture that has been presented only permits the addition of genuine records to the blockchain, which is verified via the process of consensus information is only granted to users under the condition that they have given their consent.

For the purpose of developing solid blockchain solutions for electronic health data, the information that is kept in the IPFS will be encrypted by means of a one-of-a-kind cryptographic method for public key encryption. The design of our research project is centred over the provision of access rights to authorised stakeholders. Prototype that not only analyses the blockchain approach but also reveals the potential applications of BT in healthcare solutions.

1.5 Existing Methods in Bitcoin

This is due to the absence of network obstacles in public blockchains that would inhibit such actions. Another aspect to consider is that transactions on public chains are transparent and accessible, although maintaining anonymity; never- theless, this level of visibility is less favourable in the healthcare sector, which is tasked with safeguarding sensitive health information. When compared to the pub- lic blockchain, the permissioned blockchain, also known as the private blockchain, which includes Hyperledger Fabric, utilises an access control mechanism to decide whether or not a new node should be added to the network at any given time. The earlier studies, on the other hand, call for ether to be provided in exchange for transactions in the healthcare sector.

On the other hand, this system accesses data without the patient's express consent, and it does not let other members of the data should be accessible to the patient's relatives in case of an emergency. Scalability is a significant challenge, since on-chain data storage results in the centralisation of the blockchain. This is due to the fast expansion of e-health data. Distributed ledger, and scalabil- ity presents an additional problem as the volume of EHRs increases each second. [22] have created an additional blockchain application, namely a blockchain that utilises EHRs to store healthcare data in a public and secured manner. Another use of blockchain innovation in the healthcare sector is Medchain, a permissioned collaboration between stakeholders created to make it easier for individuals, pharmacists, and hospitals to share medical data [23]. On the other hand, the architecture that stores the real data on the blockchain has serious problems with both privacy and scalability. An alternative that is decentralised was presented by Zyskind et al.[24], responsible for enforcing access control measures. Due to the fact that the metadata of the patient is revealed, which in turn exposes all other information, the safeguarding of data privacy is an extremely important concern with this BT. There is a lack of security, privacy, and scalability amongst all of the options that have been considered, and these problems have not yet been resolved [25].

Despite the fact that there are many techniques that employ BT to sharing healthcare information, such as EMRs and personal health records (PHR), these methods do not yet solve the issue of data storage or the effective exchange of health data [22] [18] .It was hypothesised that a different Internet of Things-oriented blockchain platform may use blockchain-based smart contracts to monitor patients' vital signs [26]. Andrea and colleagues came up with the idea of using Hyperledger Fabric blockchain smart contracts to create a provenance management platform that would allow for the monitoring of electronic healthcare information . Using Bitcoin and open electronic health record interoperability.

1.5.1 Components of the Health chain Framework

The Membership Service Provider (MSP) [9] is responsible for abstracting all of the cryptographic processes that are involved in the health chain. Participating organisations have the option to establish an external CA if they want to do so.

The consensus mechanism for transactions is a core layer of BT that is one of its most important properties. It was developed by IBM under the Linux Foundation with the purpose of providing solutions for distributed ledger transactions. Hyperledger Fabric, a permissioned blockchain infrastructure composed of pre-specified parties, is used in this research to enable the safe and reliable transmission of medical data without the need for a central authority.

Go programming language and are distributed and instantiated on channel peers by authorised participants. The study uses smart contracts, which include the application logic for electronic health record transactions. These contracts are especially beneficial for data transfer, access management, and request processing. They may be used to update medical records, enable physicians to document information, transmit electronic referrals to other practitioners, modify ownership details, and issue electronic prescriptions to pharmacies.

The Internet Protocol File System is a peer-to-peer distributed file system that might potentially replace HTTP. It aims to convert the existing iteration of the web into a decentralised one. In the case that the data surpasses a specified threshold (dimensions exceeding 256 KB), IPFS will distribute the encrypted data over many nodes. This research use the Internet Protocol File System (IPFS).

1.6 Security and Privacy for Cloud-Based E-Health Data

A pressing need to protect and preserve data in order to ensure patient confidentiality. The following are crucial requirements for EHR security and privacy:

1. The protection of data confidentiality guarantees that sensitive health information is not disclosed to anyone who are not permitted to receive it. Encryption of data is the most significant method for protecting the secrecy of data transmissions. Authenticity is the third component, and it guar- antees that only allowed and genuine authorities have access to sensitive health information. The need to be accountable and to defend the acts and

choices of people or organizations is what we mean when we talk about accountability. The concept of non-repudiation relates to the fact that the legitimacy of a sender and recipient is not undermined. Patients and medical professionals, for example, are unable to renounce their claims after the theft of health information[29]. This paradigm is less patient-centric and is more susceptible to assaults from insiders, which renders individual health data more susceptible to being compromised. This is one of the most signif- icant drawbacks associated with cloud computing. In spite of the fact that cloud computing approaches successful when used in e-health, taking into consideration the security concerns.

2. The electronic health system is a relatively new invention in the health- care industry that makes use of electronic operations and communication. According to [15] , an EHR and EMR is a methodical compilation of the electronic health information of patients. Additionally, the cloud enables cost-effective storage for any information that is stored. As a result of the fact that all of this information is saved on several servers, it is readily accessible to users from a variety of places whenever they need it. E-health systems offer to provide patients with quick, reliable, and on-demand access to their medical information, as well as a reduction in medical errors and an improvement in the quality of treatment. However, they also put pa- tients' privacy at risk by allowing incorrect authorization and allowing EHR data to be misused. When it comes to the sharing or accessing of patient data amongst several stakeholders, security and privacy are regarded to be essential needs.

3. In order to ensure the confidentiality of electronic health record EHRs data, which contains sensitive patient information and is stored on servers owned by a third party, access control techniques are necessary. In the health- care system, access control is a security barrier that restricts the operation of healthcare documents and the access to those documents. The ability to give specific responsibilities to users in order to provide them access to data is

made possible by role-based systems [27]. In contrast to IBAC, which makes use of identity-based encryption procedures that make use of user identification for the purpose of data encryption, Attribute Based Access Con- trol (ABAC) [28] makes use of both cryptographic and non-cryptographic approaches. A distinguishing characteristic of e-health systems is the ability to share data. It is possible for numerous parties, including healthcare providers, hospitals, healthcare organisations, and others, to exchange data with one another. One further significant function that an electronic health record system may do is search. When compared to paper-based records, EHRs need less time, personnel, and physical storage [20] .EHRs provide a number of benefits, including the facilitation and acceleration of medical expenses, and the improvement and reinforcement of clinical decision-making support. This is because these institutions have recognised the advantages that an EHD system offers.

In spite of the fact that EHRs face a number of issues in the healthcare industry, the most significant of these challenges deal to the protection of personal information and the prevention of unauthorised access [1] . Distributed Denial-Of-Service (DoS) attacks, which have the potential to prevent a system from providing effective patient care, are two examples of the many types of risks that may occur. The consequences of cyberattacks, such as those generated by ransomware, are deeper and more far-reaching than the loss of financial resources or the invasion of personal privacy [5] . Anonymous, a group of online vigilantes, attacked a number of hospitals and executed a distributed denial of service assault (DDoS) on their websites, which rendered medical services inoperable [2]. There are already a number of methods that are being used in order to protect the confidentiality and safety of intelligent health systems that are hosted on the cloud.

It is possible to apply some of the more sophisticated privacy-protecting measures that are used to maintain cloud security to e-health, while others cannot be used because of security concerns. This is because of the security concerns that are still there. At the same time as it offers the highest possible degree of data privacy, the system is immune to attacks that include collaboration. This strategy has the potential to be used in the e-health cloud for the purpose of achieving efficient data storage. In addition, this method cannot be considered for EHRs since it does not prioritise the patient and is computationally impossible to implement for issues of a real-world size.

1.6.1 Methods for Protecting Patients Confidentiality in EHRs

Additionally, the difficulties that these methods provide in the field of e-health are also discussed. In addition, a number of methods that protect data privacy, data anonymity, and data security in the cloud are reviewed and assessed. Cer- tain searchable encryption (SE) approaches are offered which are discussed below. Normal searching strategies are unable to be used since the data is encrypted and kept on cloud servers that are owned and operated by a third party. Because it is difficult to search encrypted data, Searchable Symmetric Encryption (SSE) has been offered as a solution. This encryption method allows keyword searches to be conducted across encrypted cloud data. When compared to more current surveys, our research study is distinct.

Covers in a methodical manner all topics and approaches of electronic health record EHRs privacy and security in the cloud. Additionally, the study sheds light on the sophisticated cloud computing security solutions as well as the research issues associated with them. At the same time, it combines the possible advantages of the BT in order to compensate for the deficiencies that have been identified. In addition, we bring the conversation to a close by addressing the areas of data privacy and security. Cryptographic systems make use of encryption methods, such as symmetric key encryption, public key encryption, and a number of other cryptographic primitives. The categorisation of the methods that protect individuals' privacy

As an early system, PEKS was suggested by Boneh et al. [22]. This technique does not reveal any information that is related and it also has a reduced communication

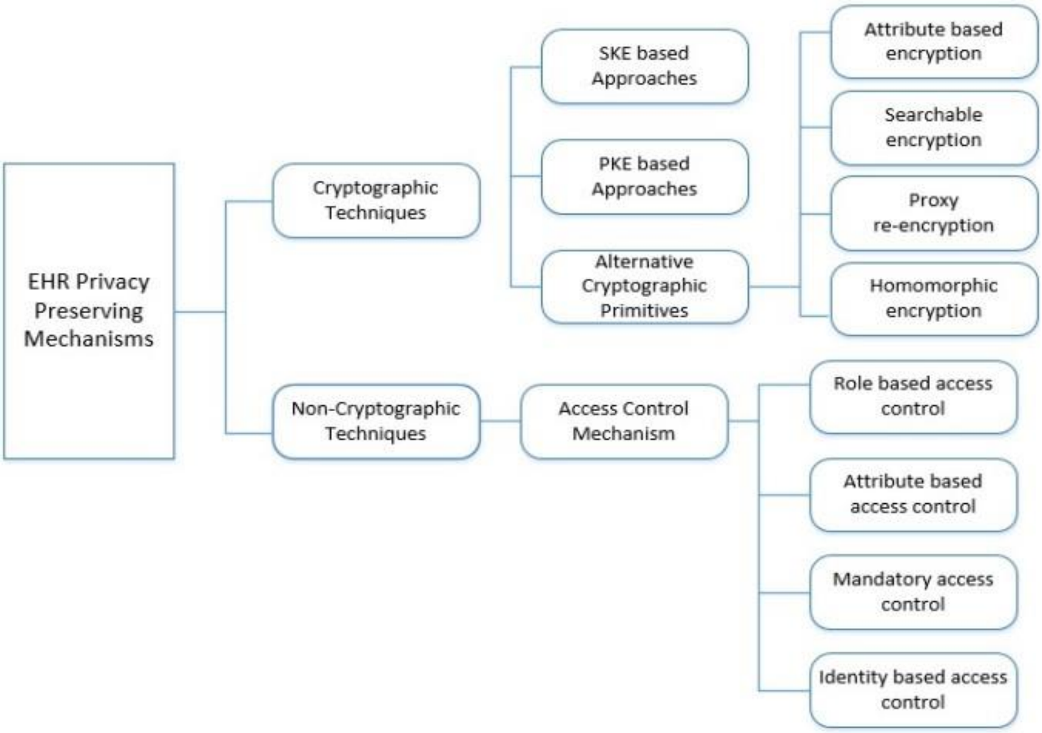

EHR Privacy Preserving Mechanisms
Cryptographic Techniques
Non-Cryptographic Techniques
SKE based Approaches
PKE based Approaches
Alternative Cryptographic Primitives
Attribute based encryption
Searchable encryption
Proxy re-encryption
Homomorphic encryption
Access Control Mechanism
Role based access control
Attribute based access control
Mandatory access control
Identity based access control

Figure 1.5: Categories of privacy preserving mechanisms

complexity. The elimination of a secure channel, the processing of numerous keywords, and the renewing of keywords are the three primary concerns that are addressed by this technique [11], which addresses the PEKS scheme. The ones who first proposed the concept of PEK being combined with a registered keyword search (PERKS). The flexibility offered by this technique allows the sender to construct material that can be searched. This allows the sender to design content that is also searchable. Because of this, the technique is more effective and safe against attacks that involve guessing keywords away from the system.

Using this method, the cloud service provider is responsible for performing partial decryption duties that have been given by the data user. However, the cloud service provider does not have any knowledge on the plain text that has been selected. Keyword search that is based on verified associated attributes.

1.7 HE: Preserving Privacy in EHRs

Patients EHRs [1] include comprehensive information on their medical history and health problems. The records include sensitive information that the patient would wish to remain private, such as previously diagnosed medical conditions and drug abuse. Whether done purposefully or inadvertently, sharing such infor- mation might have very negative effects on the patient in question. Unfavourable outcomes might include things like social shame, trouble finding work or health insurance, and more [3]. Legislation like as the Health Insurance Probability and Accountability Act (HIPAA) has been established in an effort to give individuals greater control over their EHRs. As a result, the privacy of these documents has to be safeguarded, and this has led to extensive study and analysis [5] as shown in Figure 5.4.

It is because of its vast storage capacity, resource savings, easier querying, and enhanced efficiency in diagnosis and treatment that EMRs, Concurrently, the rapid expansion of EMRs has resulted in the easy disclosure of patient privacy, which has become a problem [10]. The two basic ways in which EMRs have the potential to jeopardise medical privacy are the leaking of information from hospital internal information systems and the leaking of patient information owing to the sharing of EMRs inside the hospital. There is also an issue where medical staff members sell patient private data in certain regions. Additionally, privacy leaks are simple to occur during the publication of EMRs. Hospitals, for instance, provide patient data to medical analytic organisations in order to compile statistics on patient data. Patient data, particularly very sensitive illness information, will be fully visible if privacy information is not safeguarded. The problem of Electronic Medical Record (EMR) privacy leaks is receiving more attention these days.

In order to safeguard the sensitive data, cryptography approaches make use of security precautions including encryption mechanisms [12, 13]. Lastly, policy approaches protect patient privacy by using guidelines and limitations to validate identity and provide access to confidential information [14, 15]. Consequently, anonymization techniques cannot ensure the privacy of a diligent patient who is now receiving medical care or undergoing a surgery as identification is lost across several datasets. As a result, the workable solution in these situations necessitates the use of policy techniques, cryptography, or possibly both [16].

A topic that is both fascinating and difficult to tackle is the publication of data that protects patients' privacy in EHRs. When it comes to releasing data, there is always a trade-off between one's privacy and their usefulness. As a result of the fact that the majority of privacy-preserving models exhibit significant privacy disclosure concerns, these models are not resilient when applied to actual datasets. The k-anonymity model is a privacy model that is often used to analyse privacy disclosures; however, with the exception of identity revelation, this model is only helpful against privacy disclosures. In the last several years, a number of privacy model modifications have been developed in order to solve the restrictions that are associated with k-anonymity.

Recent years have seen a significant advancement in information technology, with cloud computing seeing an increase in applications and the widespread usage of HE technologies in cloud computing and cloud storage [1]. But as cloud com- puting has grown, so has the issue of protecting data privacy, which has grown in importance and is now a critical security issue that has to be resolved. However, HE technology based on public key cryptosystem has a more complicated calcu- lation process that cannot handle high volumes of calculations and many users, and there is no reliable cloud centre [2–3]. Consequently, while aggregating data, the HE technique is used to safeguard data privacy, thereby safeguarding user privacy as well. The ultimate outcome of aggregation is what the cloud centre re- ceives, and because no user's personal information is revealed, user data security is guaranteed. The HE technique offers several benefits over the RSA encryption method in terms of computing speed and data privacy protection, demonstrating its ability to successfully safeguard users data security.

The primary issue with cloud computing is security. One major problem is the data that is sent to outside service providers for processing and automation. Every company or organisation wants access to the user's private and sensitive information. All organizations public, corporate, healthcare, or academic—need data to design new marketing campaigns, conduct research, develop policies, or introduce ground-breaking products. Our primary worry is healthcare privacy since, by 2026, the healthcare cloud computing industry is expected to surpass US$ 40 billion, according to a report conducted by Acumen Research and Consulting [4]. Cloud computing in healthcare lowers costs while also boosting efficiency. It is quick, but the most important thing is to preserve patient-sensitive data since doing so will boost patient trust and support economic growth. The goal of digitising patient medical records is to save expenses while increasing the effectiveness and quality of service. However, patient records include a significant amount of private information. Patients must thus be able to quickly provide a variety of medical affiliations access to their private data in a straightforward, reliable, effective, and safe manner. Thus, it is essential to examine the use of HE in the healthcare industry and evaluate several homomorphic algorithms for data querying and sickness prediction while maintaining patient privacy.

The rapid digitization of healthcare data has led to a significant increase in the availability of EHRs. However, this abundance of data has also raised con- cerns about patient privacy, as sensitive medical information could be accessed by unauthorized parties. The use of HE has emerged as a potentially useful solution to this problem. It makes it possible to do safe computations on encrypted data without going through the process of decryption. The use of HE makes it possible to carry out certain mathematical operations on encrypted data, with the end result being identical to what would have occurred if the operations had been carried out on the data that had not been encrypted in the first place. This has significant implications for the healthcare industry, where large datasets of med- ical records can be analyzed while preserving patient privacy. One application of HE in the medical field is private predictive analysis on encrypted data. This technique allows for the development of predictive models using machine learning, contributing to advancements in medical science and public health. HE has also been proposed for use in secure medical cloud computing. By utilizing fully HE, data can be stored and processed in the cloud without the cloud provider being able to access the sensitive information. Researchers have demonstrated the feasibility of implementing HE for medical applications. A study on private Naive Bayes classification of cancer data showed that fully HE can provide accurate re- sults while preserving patient privacy. Similarly, another study on cardiac health monitoring in the cloud found that HE can be a viable solution for secure medical data processing. The literature on the use of HE in healthcare is growing, with several studies highlighting the potential benefits and challenges of this technol- ogy. One study examined the use of HE for machine learning in medicine and bio informatics, demonstrating the ability to perform tasks such as data classification and model training on encrypted data. Another study explored the application of private Naive Bayes classification on personal biomedical data, including can- cer data analysis. The potential for HE to enable private predictive analysis on encrypted medical data has also been explored, with researchers highlighting the need to balance privacy concerns with the potential public good that can come from such analyses.

The encryption and decryption processes of private key encryption are carried out using a single key. For the purpose of transmission, the asymmetric key encryption key makes use of a pair of keys. During the transmission process, the public key is typically accessible to both of the people involved. There is a possibility that the public key may be accessed via the directory that is generally accessible and has access to resources. The information included in the private key is only accessible to the individual who is sending the message. It will be kept confidential. In terms of the pace at which the encryption is performed, the private key encryption is a little bit quicker than the public key encryption. Users who are already familiar with one another may employ private key encryption. Because the sender and the recipient are required to have access to the secret key at the same time. Because of its adaptability, public key encryption may be used by users who are not known to the user.

Various types of data such as text, image, audio, video and any multimedia images can be encrypted using the encryption algorithm which is available in the Cryptography. By seeing the confidential level, availability of data and Size of the key a particular types of Encryption schemes are used. If the message is very confidential and important like military data, medical data, bank account data and privacy data various levels of the performance is retrieved by using the types of the Cryptography algorithm.

Encryption algorithms are coming under Cryptography concept. Cryptography deals with the encryption algorithms. It may be key based algorithms, classical algorithms and modern algorithms. All the algorithms are written for the sake of data from the adversaries and hackers who are available in the insecure commu- nication channel. Each and every algorithm in the Cryptography considers the hacker of the data and hackers arrival from all the sides like efficient algorithms, efficient secret and public keys. Various attacks are analyzed by the Cryptography mechanisms. The communication network is insecure. Secret key algorithm and the secret key used to protect the message.

The encryption technique and information are known to everybody save the Keys. It is a straightforward process that involves the encryption of plain text and the There is a decryption of the enc(f(m)). According to the encryption of m, it ought to be equivalent. The complete definition of the speed, efficiency, performance, and security of the crypto system is provided by these metrics. used in order to render the system susceptible to assaults including cryptographic analysis. Block by block, the pixels are processed in order to carry out the computations during the processing of the picture.

HE Crypto System, various data types and its applications, OHE implemented Electronic voting, Medical data storage and access and Private Information Retrieval.Security Performance of Symmetric and asymmetric are shown with the comparison of various Key Size. A comparison is made between the public key encryption techniques and the stream cyphers, block cyphers, transposition cyphers, and substitution cyphers. As the size of the key rises, the level of security afforded to the data likewise increases. With the help of the public key cryptography technique, arithmetic operations performed on the huge number went through verification. It is feasible to launch a Brute Force attack against the Private Key Encryption algorithm. Because of this, the size of the key is somewhat less complicated than that of the Public Key Encryption. It is a procedure that involves making assumptions and estimating values by comparing the plain text value to the cypher text that is provided. Private key encryption algorithms such as DES, AES, and IDEA International Data Encryption Algorithm (IDEA)are very well- known and usage by a large number of people. The comparison of the public key encrypted arithmetic operations across large amounts of data has been accomplished with the help of Java Net beans. In order to facilitate comparison, the run time of that Java Platform has been recorded. The outcome of the Runtime demonstrates that the level of security offered by public key methods is superior than that offered by private key encryption.

Among the several types of public key encryption schemes, the homomorphic crypto system is one that enables algebraic operations to be performed on the cypher texts. It is a significant and cutting-edge method that enables computing and analytical processing to be performed on encrypted data that has been sent across an unsecure intermediate communication channel. A multiplicative encryp- tion technique is being used here. The plain text that has been encrypted may be obtained by the multiplication of the ciphered text in this approach. When com- pared to the Plain text, the Cypher text expansion is much lengthier. The Cipher text has a higher ratio than the Plain text does to begin with. Comparatively, the least amount of expansion results in the least amount of noise in the calculation.

1.8 Research Gaps

1. The typical cloud-based healthcare data management systems have several problems, including vulnerabilities in the system and concerns over the privacy of the data [13].

2. In the field of healthcare, the majority of the current research works on

blockchain have mostly concentrated on the Bitcoin network, which has a number of limitations, including a high energy consumption, restricted scalability, and poor transaction throughput[26].

3. To meet the demands of the healthcare industry, there is a significant need for the development of a blockchain that is safe, cost-effective, and protects data privacy[13] [20] [23].

1.9 Objectives

1. To study and analyze the existing privacy persevering models developed for electronic healthcare records.
2. To design a more efficient privacy preserving model for healthcare record using homomorphism encryption.
3. To propose energy efficient auditable EHR model using blockchain.
4. To compare the performance of the proposed model and existing models with various performance metrics.

1.10 Research Methodology

The expected outcome of the research work is to develop block chain inspired privacy preserving and auditable model for electronic health record in fog envi- ronment keeping in view of computation cost, communication cost, consensus cost and energy consumption.

A flow chart in figure is a list activities to achieve the mentioned objectives followed by the research methodology for each objective as shown in Figure 5.5.

1. To achieve the first objective, studied various research papers and analysed the existing privacy preserving models for the electronic health records.

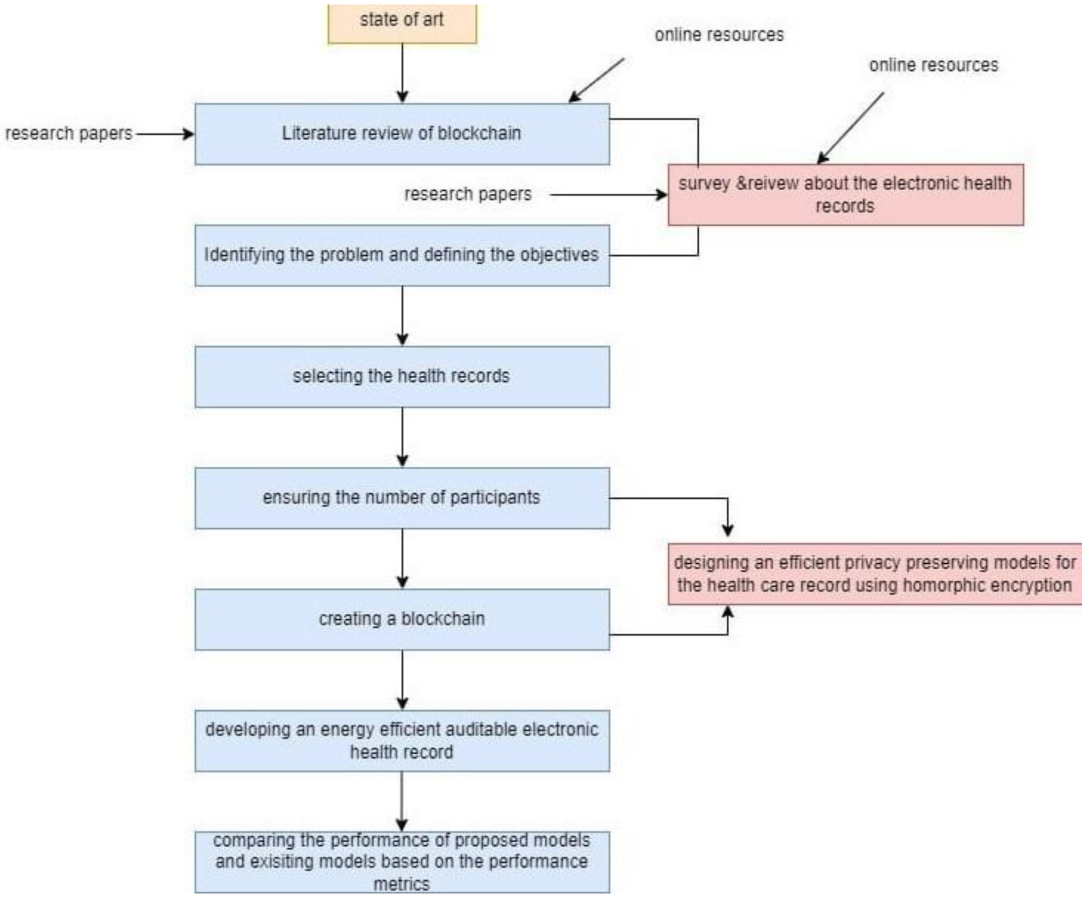

state of art
online resources
online resources
research papers
Literature review of blockchain
research papers
survey &reivew about the electronic health records
Identifying the problem and defining the objectives
selecting the health records
ensuring the number of participants
designing an efficient privacy preserving models for the health care record using homorphic encryption
creating a blockchain
developing an energy efficient auditable electronic health record
comparing the performance of proposed models and exisiting models based on the performance metrics

Figure 1.6: Workflow model

2. To achieve the second objective ,used Seal library popular implementation of Fully Homomorphic Encryption developed by C++, CKKS algorithm ,Bootstrapping, RESNET 50 designed a new privacy model.
3. To achieve the third objective, deployed a Blockchain into six machines some of them are UBUNTU 16, OS, windows10.Implementation of encryption and decryption of Homomorphic Encryption is done in Java and edited tools notepad++.IDE for deploying the solidity frame work.

4. To achieve the fourth objective , comparision of existing model with the proposed model based on the performance metrics.

1.11 Summary

This chapter introduces the significance of blockchain .It also explains the existing methods of healthcare industry ,security and privacy standards for cloud based e-health data .The motivation behind the development of this research work is also explained in this chapter.At the end ,it highlights the research gaps, objectives of the thesis and the research methodologies adopted to achieve the privacy and security using the blockchain.

1.12 Organization of the Thesis

As shown in Figure 1.7 ,the subsequent sections of the thesis are arranged into six parts . Chapter 1 presents the introduction of blockchain ,its platforms and distributed storage, existing methods in health care industry, components, security and privacy standards for cloud based e-health data. Chapter 2 deals with the background of healthcare, blockchain, privacy and homomorphic encryption .Chapter 3 presents how the blockchain is evaluated ,its framework and recommnedations. Chapter 4 discuss about the network that is using machine learning privacy preserving models with fully homomorphic encryption for deep neural network.Chapter 5 presents the implementation of a novel design blockchain based

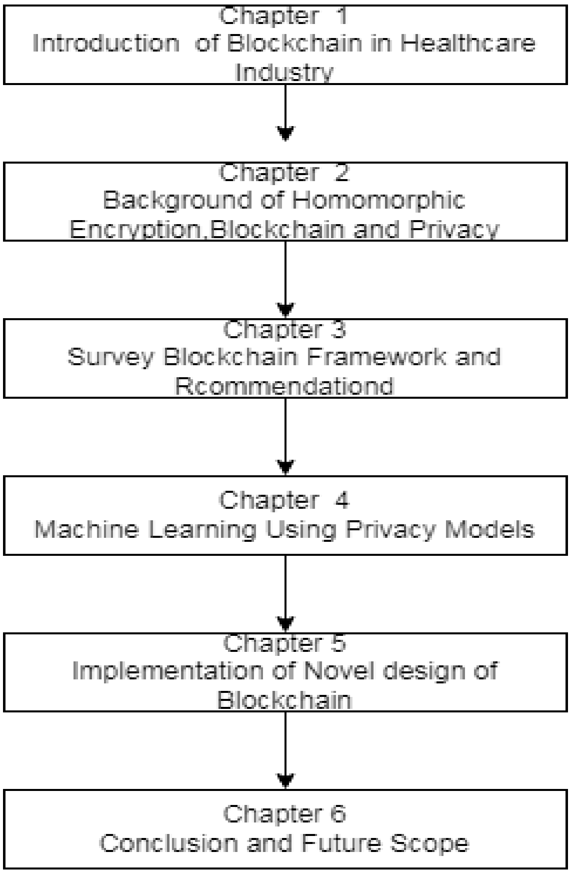

Chapter 1
Introduction of Blockchain in Healthcare Industry
Chapter 2
Background of Homomorphic Encryption,Blockchain and Privacy
Chapter 3
Survey Blockchain Framework and Rcommendationd
Chapter 4
Machine Learning Using Privacy Models
Chapter 5
Implementation of Novel design of Blockchain
Chapter 6
Conclusion and Future Scope

Figure 1.7: Organisation of thesis

secure multiple computations scheme for preserving and extraction of health care data. Chapter 6 presents the conclusion and future scope of the thesis wor

Chapter 2

RELATED WORK

2.1 Introduction

In this chapter, we explore the critical intersections of Bitcoin and healthcare data management. They focus on data security, privacy, and integrity. As health- care systems increasingly transition to EHRs, the vulnerabilities associated with access become more pronounced. EHR security and transparency, as its decentral- ized ledger system ensures that patient data is immutable, traceable, and securely shared among stakeholders while preserving confidentiality. Coupled with homomorphic encryption, this combination offers a powerful framework for developing privacy-preserving and auditable EHRs systems.This literature review investigates innovative solutions, particularly the synergies between blockchain and homomorphic encryption. It highlights their potential to revolutionize healthcare data management by improving patient privacy, data security, and regulatory compliance. By examining the current state of research and emerging frameworks, this chapter aims to elucidate the transformative potential of these technologies in safe guarding patient information and enhancing healthcare delivery efficiency.

2.2 Evolution of EMRs in Modern Healthcare

Rathi et al.[29] proposed Health care’s journey towards digital transformation has been marked by the transition from paper-based medical records to EMRs.Healthcare records were initially stored in bulky files and folders that were inaccessible, hard to maintain, and easily damaged. On the other hand, EMRs allow patients data to be stored, managed, and retrieved digitally in a systematic and efficient manner. EMRs improve quality and continuity of patient care. They streamline communication and coordination between healthcare providers, laboratories, and pharmacies, enabling faster diagnosis and better decision-making.

Nkenyereye et al. [30] proposed the time needed to make critical healthcare decisions by providing test results, medication lists, and treatment plans by digitizing patient data. Furthermore, EMRs improve the overall healthcare ecosystem by enabling population health management, where aggregated data can be used to identify health trends, predict disease outbreaks, and implement preventative measure. Kaushik et al. [14] as EMR adoption grows, the volume of sensitive patient data in digital form increases, posing security, privacy, and accessibility challenges.

2.3 Adoption Challenges to EMR Implementation

Mistry et al.[31] proposed the numerous benefits of EMRs, the healthcare industry has faced notable challenges adopting and implementing EMR systems universally. One of the key barriers is the high costs associated with EMRs. Software acquisition, staff training, and maintenance costs are significant initial implementation expenses, often burdening small healthcare facilities, especially those with low or middle incomes. Budhiraja et al.[32] proposed, migrating from paper records to a fully digital system can be overwhelming, causing disruptions in daily opera- tions. Healthcare providers often resist adopting cutting-edge technologies due to concerns about usability,complexity, and time needed to adapt to the system.

Srinivasu et al.[33] proposed EMR adoption is also challenged by interoperability. Due to the fragmentation of healthcare IT infrastructure, it can be difficult to integrate disparate EMR systems from different vendors. Data may be stored and transmitted in different formats by different systems, preventing seamless data exchange between healthcare providers. This lack of interoperability hampers coordinated care, particularly in cases where patients seek treatment from multiple healthcare providers or facilities.

2.4 Security and Privacy Challenges in EMR Systems

Feng et al.[34] proposed a digital health record can pose security and privacy risks. Cyber criminals often target patient data in data breaches because it includes sensitive information, such as personal identifiers, medical histories, and treatment records. Over 30 million records will be exposed to healthcare data breaches in 2020 alone, underscoring the vulnerability of digital health systems. In addition to leading to identity theft, these breaches can cause significant financial and reputational damage to healthcare organizations.

Khujamatov et al.[35] proposed a primary security challenge is unauthorized access to the EMR. Inadequate access controls can allow inappropriate personnel to gain access to patient information. Among the common issues that expose EMRs to unauthorized access are poor password management, lack of encryption, and limited monitoring of user access. Further, insider threats pose a growing threat to healthcare organizations as employees misuse access privileges. There are over 50% of healthcare data breaches caused by internal actors, which highlights the need for robust access control policies and regular training for staff on data privacy and security.

Vivekanandan et al.[36] proposed Inaccuracies or alterations in patient data can lead to incorrect diagnoses, inappropriate treatment plans, and even fatal out- comes. Cyber attacks such as ransomware and malware pose significant threats to data integrity because they are capable of altering, deleting, or locking critical health information. As a result of these attacks, healthcare services are disrupted, patients in critical conditions are delayed, and patients’ risks increase. A health- care systems data protection needs are governed by legal and regulatory requirements. In the United States, regulations such as Health Insurance Portability and Accountability Act (HIPAA) require strict protocols for securing patient information. Due to resource constraints and cyber threats, achieving full compliance with these regulations remains challenging.

2.5 Cloud-Based EMR Storage:Opportunities and Limitations

Gao et al.[37] proposed that healthcare providers have adopted cloud-based EMR storage solutions to deal with some of these security challenges. Cloud-based EMR systems offer several benefits, including scalability, remote access, and reduced hardware costs. Healthcare facilities can streamline data management and ensure continuity of care by outsourcing data storage to cloud providers.

Zhou et al.[38] proposed Cloud-based EMR systems are not without limitations. Cloud storage introduces new security risks, such as unauthorized access by third parties and potential vulnerabilities during data transmission. According to a study, 88% of cloud service users express . Among these concerns are the lack of control over data and the possibility of data interception during transmission. In addition to encryption and multi factor authentication, cloud providers implement security measures. However, healthcare organizations must also comply with data protection laws, which may differ from jurisdiction to jurisdiction. The challenge of balancing data accessibility with strict security measures remains a major one in cloud-based EMR storage.

2.6 EMR Security Challenges with Bitcoin

Moreover, Bitcoin offers potential solutions to healthcare providers' interoperabil- ity challenges. By eliminating complex integration processes, patients could access a single, blockchain-based health record via any authorized healthcare provider, eliminating the need to transfer data between incompatible EMR systems.

2.7 AI-Enabled Blockchain for Enhanced EMR Management

Zhang et al.[39] proposed with the integration of Bitcoin into EMR systems, healthcare data management could be improved even further. With the help of AI, large volumes of patient data can be analyzed on a blockchain in order to identify patterns, predict outcomes, and support clinical decision-making. AI algorithms can detect early warning signs of chronic diseases, so that preventative care can be provided and personalized treatment plans can be devised. As part of a blockchain-based EMR system, AI could also automate data access and sharing permissions based on predefined rules, reducing manual interventions and ensuring compliance with privacy laws.

A champong et al.[38] proposed implementing AI-enabled blockchain systems stages and faces several technical, regulatory, and ethical challenges. AI and blockchain's high computational requirements may limit their scalability in resource-constrained healthcare settings. Moreover, ensuring data privacy while leveraging AI analytics remains a significant challenge, as AI models require access to large datasets to deliver accurate predictions. Nevertheless, AI-enabled blockchain systems hold significant potential for transforming EMR management by enhancing security, interoperability, and data accessibility in healthcare.

Alanazi et al.[1] proposed Bitcoin integration into EHRs represents a significant advancement in healthcare data management, focusing on enhancing security, privacy, and data integrity. It also ensures immutability and transparency of transactions. This is particularly critical in healthcare. Furthermore, Khezr et al. Offer a comprehensive review of blockchain applications in healthcare, identifying key benefits such as transparency, traceability, and regulatory compliance facilitation. These foundational studies underscore enhancing both patient privacy and security.

Allard et al.[40] proposed combination of homomorphic encryption and blockchain enhances the privacy-preserving capabilities of EHRs, enabling data processing without decryption.This cryptographic technique ensures that sensitive health information remains confidential, even during data analysis. In this paper, demonstrate how homomorphic encryption can be applied to EHRs to provide healthcare providers with insight into patient data while maintaining privacy. The ability to operate encrypted data is particularly crucial when data is shared for research or collaborative patient care. In these scenarios, patient confidentiality must be strictly maintained. As a result of blockchain's decentralized architecture and ho- momorphic encryption's privacy-preserving features, healthcare environments are able to address the dual challenges of data security and privacy. Furthermore, Be- naloh et al.[41] proposed review blockchain applications in healthcare, including frameworks, prototypes, and implementations, demonstrating their potential to revolutionize health data management. To promote patient trust and compliance with privacy regulations, emphasize the importance of privacy-friendly platforms using blockchain environments to secure health data. The importance of inte- grating these advanced technologies into existing healthcare systems cannot be overstated.

Chen et al.[12] proposed to facilitate effective implementation of blockchain-based EHR systems that incorporate homomorphic encryption, several challenges must be addressed. Scalability, computational efficiency, and regulatory compliance are important factors to consider. Data security and privacy are significantly enhanced by blockchain and homomorphic encryption, but computational overhead associated with such operations can impede system performance and responsiveness. Sengupta et al. note that blockchain adoption in healthcare requires interoperability with existing health information systems. Describe the potential threats and security concerns related to Internet of Things (IoT) and Industrial Internet of Things (IIoT) applications, which further complicate healthcare environments. Blockchain protocols and homomorphic encryption techniques need to be optimized continuously in order to facilitate the widespread adoption of this integrated healthcare approach.

Chenthara et al.[42] proposed Aside from ensuring model secrecy, Byzantine Fault

Tolerance (BFT) is important for maintaining high standards of traceability, transparency, and error tolerance. BFT is effective not only because it is resilient to various faults but also because it enhances distributed system reliability. In sensitive applications, such as healthcare, where data integrity and availability are crucial, this is particularly important. The system achieves a notable convergence rate, demonstrating its ability to rapidly approach optimal solutions even in the face of uncertainties. It is imperative to note, however, that although these advancements have been significant, there is still no compelling evidence that this system has significantly improved its feasibility over traditional methods. A novel system that safeguards user privacy in cloud environments automatically by using deep learning architectures is required to address these identified challenges. As well as providing efficient solutions to complex problems, this advanced technology system aims to protect data and enhance user trust by leveraging advanced techniques.

Dainton et al .[43] proposed Input files in Bitcoin can be managed and executed by a diverse array of parties using distributed ledgers. With this decentralized architecture, multiple stakeholders can participate in system maintenance without relying on a central authority. By maintaining multiple datasets collaboratively, stakeholders are able to trust that the information being processed is accurate and accurate. A standard protocol for interaction is then created by utilizing this information to establish the rules governing transactions within this blockchain framework. Though these advancements address previous inefficiencies in data management and communication, the current landscape of medical information management remains chaotic and fragmented. Errors, delays, and a lack of coordination among healthcare providers can occur as a result of this disorganization. In addition, the blockchain is designed to function as an immutable, secure, and traceable method of depositing funds. Effective data governance relies on operations such as addition, deletion, modification, and querying medical information. Blockchain, however, focuses on simpler functions such as modification and inquiry. Compared to general activities, this streamlined approach significantly reduces the time and effort spent processing medical information.

Dehling et al.[6] proposed implementing Bitcoin, high levels of security and irreparability are guaranteed. Each block's information includes both the creation time. The linked structure provides traceability, tracking, and regular audits over time. Besides increasing medical records security, this chain architecture facilitates an increased use of medical information across multiple healthcare systems. BT can improve healthcare outcomes by promoting interoperability and centralizing rules governing data distribution and benefit exchange.

Dorgham et al.[7] proposed , enhancing automated information sharing efficiency can be achieved through block connections and smart contracts. By properly designing these contracts, automated processes can be achieved, ensuring that transactions are executed without interference from third parties. By combining these technologies, we can enter an exciting era of healthcare data management, where efficiency, security, and transparency are prioritized.

2.8 ECC Cryptography and its Impact on Blockchain

Since ECC does not require as much schemes, it offers significant advantages. ECC employs smaller key sizes while providing equivalent security levels, making it an efficient choice for various applications, especially in environments with limited computational resources.

Edemekong et al.[44] proposed ECC could be used to enhance data security in the healthcare field by efficiently encrypting medical data, according to the proposed model. The addition operation in ECC symbolizes the most fundamental group operation performed on an elliptic curve, which is essential to the encryption process. The combination of two points on the curve, denoted as P and Q, yields a new point on the curve, denoted as P + Q. Cryptographic functions based on this mathematical operation form the basis of ECC's security mechanisms.

With Elliptic Curve Cryptography (ECC), rapid computations can be performed without sacrificing security, which highlights its efficiency in handling cryptographic calculations. Prior communications inadvertently omitted the conditions required to complete.

To ensure data confidentiality, elliptic curve-based cryptography relies on specific mathematical properties of elliptic curves. ECC is a formidable choice for protecting sensitive information due to its difficulty with the Elliptic Curve Discrete Logarithm Problem (ECDLP). Therefore, these assumptions must be maintained during the implementation of the proposed model. Specific cryptographic meth- ods and elliptic curves will significantly influence the equations' characteristics and properties.

2.9 Hybrid Homomorphic Encryption

Gao et al.[45] proposed the context of a blockchain-based healthcare system, hy- brid homomorphic encryption. This advanced encryption technique combines the benefits of homomorphic encryption with the flexibility of hybrid systems to pro- vide robust data protection. This secure collaboration and data analysis is a key advantage of implementing hybrid homomorphic encryption in conjunction with Bitcoin, as it promotes trust among participants and enhances the overall security of the system.One of the standout features of hybrid homomorphic encryption is its ability to allow computations to be performed directly on encrypted patient data stored on the blockchain.

Geetha et al.[46] proposed Hybrid homomorphic encryption significantly enhances patient privacy, facilitates secure data sharing, and allows encrypted data to be processed securely. In addition to strengthening, this powerful combination also fosters trust among stakeholders, thereby making healthcare more efficient and secure. In an increasingly interconnected world, adopting these advanced technologies will be crucial to protecting patient information.

The integration of Bitcoin within 5G networks is set to revolutionize various sec- tors, particularly healthcare and smart city applications. Blockchain-enabled data sharing for flying drones in the 5G era is discussed by Feng et al.[36]. Proposed as drone technology becomes increasingly prevalent, ensuring data integrity and confidentiality is crucial. As well as addressing security concerns, the proposed framework demonstrates the potential for real-time applications in logistics, surveillance, and emergency response.

By having access to medical data in real time, decision-making processes are enhanced, resulting in improved patient outcomes. In addition, blockchain can facilitate better healthcare delivery by building trust between patients and healthcare providers because it is secure and transparent.

A blockchain-based protocol for device-to-device authentication is introduced by Vivekanandan et al.[36] proposed in the context of IoT and smart cities. In smart city applications, where devices are interconnected, this protocol is essential for securing interactions among IoT devices. As a result of using blockchain for authentication, the system can streamline processes and boost overall network security. With the development of a blockchain-SDN-enabled Internet of Vehicle environment, Bitcoin becomes even more versatile. Additionally, Zhou et al.[38] proposed PIRATE, a secure framework for distributed machine learning in 5G networks, demonstrating how blockchain can facilitate secure data processing and analytics. The integration of blockchain with AI technologies in the context of beyond 5G networks also holds promise for future innovations, as Zhang et al. [**?**] suggest. It is clear from these studies that BT is capable of creating secure, efficient, and reliable systems across a wide range of applications.

There are additional pathways for enhancing the effectiveness the emphasis on federated learning. For the creation of a secure, privacy-preserving, auditable electronic health record framework, a synthesis of Bitcoin with homomorphic encryption holds considerable promise. It heralds a new era in healthcare data management, navigating the complexities associated with implementing these advanced technologies while prioritizing patient security and confidentiality. Consumers may still be hesitant to entrust their private data to virtual storage, such as medical records, emails, or government documents, despite cloud computing's many benefits. The cloud user has no further control over the use or the loca- tion of information once it has been uploaded to the cloud data center. Although Cloud Service Providers (CSP)have promised to deploy safeguards like virtualization and firewalls to keep their customers' data safe, network flaws often prevent these systems from providing comprehensive data security. CSPs have full access to their customers' cloud-based software, hardware, and data, so encrypting data before hosting is essential to protect it. For cloud computing to keep information private and secure, reliable storage and management systems are necessary since most cloud access patterns incur high communication costs.

To deliver high-quality treatment, healthcare providers must effectively manage patient-related media data, including text, images, audio, and other multimedia. The popularity of cloud-based healthcare applications has increased recently as they offer large computing power, flexible storage, and a variety of software applications. On this platform, however, there remain several challenges associated with delivering and sharing large amounts of healthcare media data to distant terminals with guaranteed Quality of Service (QoS).

Theoretical knowledge of cloud computing in healthcare is inadequate compared to its actual implementation. In some research, cloud computing has been conceptualized or interpreted within healthcare settings, but most of it relies on broader interpretations, which may give cloud computing a distorted perspective. Cloud Computing Services (CCS) provided cloud-based applications, according to Haque et al.[18] .The scalability of cloud-based solutions allows hospitals to analyze vast amounts of data with complex mathematical models as a key benefit. Despite its restrictions on confidential, internal patient information, the CCS is not a real-time system, and medical professionals use it, but the general public cannot access the data management process.

The authors of Keshta et al.[47] proposed an efficient network model combining wireless body area networks and cloud computing for reliable data exchange. It was shown that the proposed architecture could deliver healthcare data over a traditional IP-based network in real-time using the OPNET simulator. As a result of insufficient security protocols, a network flooding attack could compromise cloud storage availability, and a malicious insider could pose a serious threat.

A diagnosis and treatment plan that is tailored to diabetes patients needs is essential given the lifelong and systemic damage they experience. Min Kruse et al.[13] proposed a cloud-based, intelligent, and tailored solution for diabetes diagnosis. Furthermore, 5G-Smart diabetes offers a method for data sharing and an individualized data analysis model.

Smart city innovations are causing significant changes in healthcare, one of the largest industries in the world. Increasing public demand for ubiquitous, pre- ventative, and personalized healthcare at lower costs and risks is a driving force. By recording and analyzing patient data anywhere, anytime, mobile cloud com- puting could meet future healthcare needs. A major challenge in implementing next-generation healthcare is network latency, capacity, and reliability. To ad- dress these issues, Lafky et al. [13] proposed to improve cloud-enabled networked healthcare systems for smart cities in terms of security, privacy, reliability, and scalability.

Lemke et al.[11] proposed a cloud-based architecture for implementing EMR sys- tems in Pakistani hospitals, although some healthcare providers use their own EMRs. By reducing the cost of maintaining paper-based records, this proposed architecture would enhance patient care, diagnosis, disease prevention, and acces- sibility to electronic health information around the clock.

Li et al.[28] proposed cloud services have many benefits, several security risks remain. For instance, consumers are often unaware of how much data CSPs store. In addition to storing and processing sensor data online effectively, cloud comput- ing and IoT present a unique approach to privacy preservation. The healthcare industry collects data from patients and shares it with authorized clinics or spe- cialists, as well as pharmaceutical companies and life insurance companies. Data synchronization and transfer, however, can lead to unauthorized access to patient information.

2.10 Data Handling in Blockchain

Liu et al .[15] proposed Healthcare and medical data must be shared in order to improve the quality of healthcare providers and make the healthcare system more intelligent. It is possible for a patient to share his medical history with his physician at their first appointment. By providing a secure method of exchanging EMRs, Bitcoin can enhance communication and cooperation with the health- care sector. To improve the exchange of health data across European nations, Muhammed et al.[48] proposed a private blockchain-based recording system.

It has become increasingly important to conduct research on BT and healthcare data management, particularly in the area of privacy and security. In cloud computing environments, Roy et al.[49] proposed emphasize the importance of maintaining healthcare data privacy. A significant risk to sensitive health information is often associated with traditional data storage methods, thus the need for advanced solutions such as blockchain, its decentralized nature, is highlighted in their work. As a result, we need effective data governance frameworks that maintain patient confidentiality while providing seamless access to data for authorized users.

This notion is further expanded by Sarwar et al. [50] proposed the concept of Healthcare Data Gateways (HDGs), which utilize Bitcoin to facilitate secure healthcare data sharing. Their model not only protects data integrity but also gives patients control over their health information. This focus on patient-centric data management is critical, since it addresses both privacy concerns and the in- creasing demand for interoperable health systems that can function across various healthcare institutions. The Efficient and Privacy-Preserving Content-Based Im- age Retrieval (EPCBIR) scheme presents a method for managing and retrieving medical images securely in cloud environments. Bitcoin can be applied to diverse types of healthcare data, emphasizing its role in improving operational efficiency without compromising privacy.

By reinforcing these findings, Thavamani et al. [51] proposed the importance of blockchain to the development of intelligent healthcare systems. By integrating blockchain into existing healthcare infrastructure, they claim that a trust-based ecosystem can be created, ensuring that sensitive information is only accessible to authorized individuals. Through better data sharing practices, their work illustrates how blockchain can not only enhance security, but also enhance healthcare

delivery. Furthermore, recent studies have investigated the role of blockchain in facilitating secure data transactions, especially in light of emerging technologies like 5G, which present new opportunities for healthcare data exchange.
Wang et al.[52] proposed Data privacy and security challenges continue to plague the healthcare industry, but BT provides promising solutions that enhance patient privacy while facilitating efficient data management. The works reviewed collectively contribute to the growing body of literature that advocates the adoption of blockchain as a foundational element in future healthcare system, addressing current shortcomings as well as future demands for data-driven healthcare solutions.

2.11 Security Concerns in Blockchain

Xia et al.[53] proposed encrypting data, especially text and images, and secur- ing its transmission through blockchain solutions, cryptography is often used to offer security. A decentralized EMR management system utilizing blockchain for data authorization, C.H. Ravikumar et al. [54] proposed combines suppliers' full medical data for verification, confidentiality, and exchange, making such data and services accessible to patients. In the future, cloud computing and blockchain will offer promising solutions. In order to overcome current limitations in privacy, security, and scalability across cloud-based and blockchain-enabled healthcare systems, advanced data science approaches, encryption, and decentralized frameworks are necessary.
C. Ravikumar et al.[55] proposed the challenges of maintaining data confidentiality and privacy for customers and security vulnerabilities. Previous research on cloud storage mechanisms, key management, security, cryptographic primitives, and potential risks is reviewed in this review. It emphasizes the limitations of cloud environments, especially services stored in a central location. This study will analyze existing key management methods and distinguish between common cloud-based key management techniques and chaotic encryption based on Bitcoin. A comparison of the respective capabilities of various blockchain systems is also provided, as is the importance of integrating AI into blockchain.

2.12 Research gaps

1. There is limited empirical research on the effectiveness of integrating homomorphic encryption with blockchain for privacy-preserving EHRs, highlighting a need for real-world case studies [1][2].

2. Current studies often overlook the computational efficiency of homomorphic encryption when applied to large-scale healthcare datasets, raising concerns about its practicality in EHRs systems [3][4].

3. The security implications of combining blockchain with homomorphic encryption are not thoroughly examined, particularly regarding potential vulnerabilities and attack vectors [5][6]

4. Insufficient exploration exists on user perspectives regarding the usability and accessibility of blockchain-driven, homomorphic encryption-based EHRs systems, which could affect adoption [7][8].

5. There is a lack of comprehensive frameworks for evaluating the performance and scalability of EHR systems that utilize both blockchain and homomorphic encryption, complicating the assessment of their effectiveness [9][10].

6. Ethical considerations surrounding data ownership and patient consent in blockchain systems employing homomorphic encryption are under-researched, which may hinder trust and compliance [11][12].

7. The interplay between regulatory requirements has not been adequately addressed, posing challenges for compliance [13][14].

2.13 Summary

The existing literature highlights the importance of robust, secure, and interoperable EMR systems for improving healthcare delivery and patient outcomes. While EMRs have transformed patient data management, security and privacy challenges continue to threaten the integrity of digital health records. BT, with its decentralized architecture and immutability, presents a promising solution to these challenges, offering enhanced security, transparency, and data control. Assessing their scalability, cost-effectiveness, and regulatory compliance. Moreover, the integration of AI with blockchain in healthcare warrants further exploration to unlock new possibilities for data-driven, personalized healthcare solutions.

Table 2.1: Summary of Key Contributions

Reference	Authors	Key Contributions	Feature
[63]	Roy et al.	Proposes a secure framework that ensures fine-grained access control to healthcare data across multiple cloud servers, enhancing security and accessibility in mobile healthcare applications. The study emphasizes the importance of user authentication and authorization mechanisms.	Enchancing Cloud Security, Multi level access.
[64]	Sarwar et al.	Presents a comprehensive cloud-based architecture designed for EHR systems in Pakistan. It discusses integration challenges and proposes solutions to enhance data security and improve interoperability among health- care providers. This work highlights the importance of cloud technology in facilitating efficient EHR management.	Enchance Data Security, efficient data mobility
[65]	Thavamani & Rajakumar	Investigates methods for preserving the privacy of healthcare data in cloud environments, focusing on encryption techniques and access controls. The authors discuss the implications of privacy breaches and propose a framework that combines cloud computing with secure data management practices.	Data Privacy by working on Security breaches
[66]	Wang & Li	Introduces Healthcare Data Gateways (HDGs) that leverage blockchain technology to enable secure sharing of healthcare data. The authors discuss how HDGs facilitate patient-centric data management while ensuring data integrity and confidentiality, addressing privacy risks inherent in tradi- tional systems.	Blockchain Technology
[67]	Xia et al.	Proposes a novel scheme for securely managing and retrieving medical images in cloud settings. The study highlights the role of privacy-preserving techniques in ensuring the confidentiality of sensitive medical data while allowing efficient access and retrieval.	Pricacy model on Medical data

[68]	Ravikumar et al.	Reiterates the critical role of blockchain in healthcare, emphasizing the creation of a trustworthy ecosystem through HDGs. The authors explore how integrating blockchain with existing systems can improve data sharing and enhance security.	Blockchain Integration on HDG

Chapter 3

Blockchain in Healthcare: An Evaluation of Literature, Frameworks and Recommendations

3.1 Introduction

Blockchain has increasingly been utilised in various sectors, including healthcare [51-53]. Given that blockchain is an immutable, transparent, and extensively distributed database that facilitates the creation of a reliable transaction sequence, this is unsurprising. The digitization of the healthcare sector has resulted in the creation of medical information systems. An individual's existence relies on their healthcare, as do the accompanying statistics that assist in illness diagnosis and inform treatment options. Information was historically inscribed and documented on easily degradable or alterable mediums [55, 56].These systems must convey data efficiently and securely [13] .They must also furnish each user with enhanced access control, privacy, and anonymity. Individuals may hesitate to disclose sensitive information or delay pursuing therapy without sufficient security protocols, privacy protections, and a basis of trust [11] .Data protection is crucial. Consequently, Bitcoin has emerged as an innovative solution that ensures data protection against vulnerabilities and breaches.

The reliance on Bitcoin may evolve due to its decentralized nature. It enables resilience against setbacks and assaults in a distributed and steadfast manner. Furthermore, it acts as a verification of the authenticity and ownership of the data [60]. As a result, blockchain is receiving growing acknowledgement as a multifaceted technology relevant to several industries and contexts, such as identity management and dispute resolution [48] , traceability, transparency, and reliability. Blockchain has the potential to resolve challenges related to interoperability, security, and confidentiality. Blockchain enables uncertain parties to execute various network transactions. A blockchain can be utilised to record and preserve data from a decentralized network of devices .

Nonetheless, there are concerns over blockchain's security and privacy within the healthcare sector, especially about safeguarding confidential patient data[49] .Although recognizing the persistence of challenges, such as the necessity for interoperability and a legal framework, the authors ultimately contend that Bitcoin can improve security[50] .This will facilitate the attainment of the ultimate goals of accountability, authenticity, and assurance in data transmission. Nonetheless, hurdles persist, including the necessity for suitable access controls, regulatory obstacles, and interoperability issues. Additional inquiry is necessary to comprehensively assess healthcare sector and ensure its ethical application in protecting patient confidentiality and privacy. While other intriguing research exists on this subject in the literature [54] ,the technique and aims of this paper diverge.

3.2 Blockchain's Need in Healthcare

The demand for progress in the healthcare sector is intensifying rapidly. Advanced state-of-the-art technology is essential to ensure the delivery of superior healthcare facilities. Moreover, the healthcare landscape is transitioning towards a patient-centred approach that emphasizes two fundamental components: consistently available services and enough medical resources. BT assists healthcare organizations in delivering superior medical services and suitable patient care. The implementation of technology can efficiently address the arduous and repetitive task of exchanging health information, a significant contributor to the elevated costs within the healthcare sector. Citizens can engage in health research efforts through the utilization of Bitcoin. Furthermore, enhanced public welfare research and data dissemination will augment care for numerous demographics. All health-

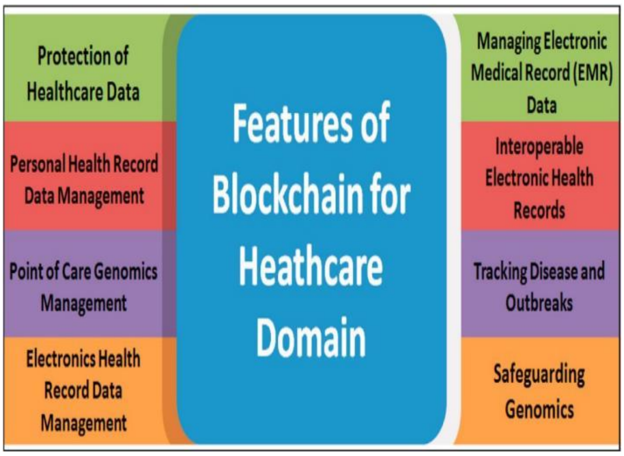

Protection of Healthcare Data
Personal Health Record Data Management
Point of Care Genomics Management
Electronics Health Record Data Management
Features of Blockchain for Heathcare Domain
Managing Electronic Medical Record (EMR) Data
Interoperable Electronic Health Records
Tracking Disease and Outbreaks
Safeguarding Genomics

Figure 3.1: Blockchain in the medical field

care organizations and systems are managed using a singular database [63–65]. When used properly, this technology promotes interoperability, enhances data interchange, ensures security and integrity, and makes real-time changes and access easier. Data security is a vital issue, particularly for wearables and personalized therapy.

3.2.1 Functionalities of Blockchain in Healthcare

Blockchain performs multiple tasks and has diverse uses in the medical field. BT enables healthcare practitioners. Figure 1 illustrates the spectrum of attributes and fundamental enablers of the Blockchain concept across several healthcare sectors and associated domains. The advancement and utilization of BT encompass intricate functionalities, like cryptocurrency security, digital tracking, and outbreak management. Bitcoin are its total digitization and its applicability within the healthcare industry [68, 69].

The newly incorporated element is superfluous and results in inefficiency, presenting a considerable health risk. The rights or opportunities for accessibility may vary for each individual based on their position throughout the supply chain. Furthermore, the data transparency feature of Blockchain architecture would enable comprehensive tracking of the root cause and the termination of counterfeit pharmaceutical distribution. The information gathered from custodians at the individual establishments frequently lacks publicly accessible data.

3.3 Privacy in Healthcare

Bitcoin is a viable solution for enhancing healthcare privacy due to its numerous advantages. Data is disseminated over multiple network nodes. Consequently, the likelihood of encountering a singular site susceptible to failure or attack is diminished. [64]. Pseudonymized to protect private information while permitting access to essential data for authorized parties. A primary issue is the incompatibility among various blockchain platforms, as healthcare providers may utilise disparate, non-interoperable technologies [56] .One problem lies in the complex deployment of BT, as it requires resources and technical skills that may not be readily available in medical environments.Patients who possess the autonomy to determine who can access their data, thereby guaranteeing that healthcare data governance conforms to their wishes [57].

3.3.1 Interoperability and Standards

The heterogeneous nature of healthcare systems, marked by the utilization of various EHR systems and medical devices that conform to distinct data formats and standards, obstructs the fluid exchange of healthcare information. Integrating several systems into a Blockchain Network necessitates meticulous design and data transformation. The existence of legacy systems that are fundamentally incompatible without BT exacerbates this challenge [58] .To tackle the challenges of interoperability and fully leverage BT in healthcare, various approaches and solutions are available. The standards encompass standardized data structures for test results, pharmacological information, patient records, and other pertinent data, to establish a unified language for data across various systems [59] .Implementing blockchain-based solutions for identity management may enhance interoperability and data security. These systems administer patient identities and access permissions discreetly, offering a secure framework for data transit. Various ways for mitigating interoperability challenges in healthcare blockchain integration encompass meticulous planning, data conversion, consensus on standards, implementation of middleware solutions, promotion of collaboration, and identity management.

3.3.2 Workflow Process for Blockchain in Healthcare

Further advantages of implementing Bitcoin in healthcare encompass enhancements in patient record management, improved oversight of the medical supply chain, greater interoperability among various systems, and the ability to collect both individual and longitudinal data. The aforementioned advantages have been recorded in references [60] and [61]. The initial phases of the interactive workflow encompassed the establishment of distributed network flow, shared data, and ledger systems. These developments facilitated the operation of Blockchain drivers[93, 94]. The foundation of the interactive workflow consists of distributed network traffic, shared data, and a ledger. These elements facilitate the operation of Blockchain drivers.Bitcoin fundamentally operates as an ever-expanding network of blocks, which can be customized to meet diverse industry needs and specific characteristics. The autonomous Blockchain will mitigate theft and unauthorized document transfers, while significantly diminishing financial failures. It can address problems related to data surveillance and outcome manipulation. The capacity to transmit clinical research data and findings with immutable time stamps mitigates the danger of fraud and errors in clinical investigations. The healthcare sector predominantly holds the responsibility for implementing Bitcoin [62] .Bitcoin influences every area in some capacity. Blockchain technologies are utilized, especially in domains requiring the establishment of trust among multiple parties and stakeholders. Blockchain possesses the capacity to significantly transform the existing disjointed consent process that patients must sign for each consultation, healthcare procedure, or medical test. Blockchain promises to facilitate the sharing of clinical trial data and to identify benefits for trial participants. Blockchain possesses the potential to serve as a pivotal element in healthcare consent management, facilitating the efficient exchange of information. Bitcoin enables patients to promptly access their medical information from various organizations [63] [64] [65] .Bitcoin influences every area in some capacity. Blockchain promises to facili- tate the sharing of clinical trial data and to identify benefits for trial participants. Blockchain possesses the potential to serve as a pivotal element in healthcare consent management, facilitating the efficient exchange of information. Bitcoin enables patients to promptly access their medical information .

3.4 Blockchain Applications in Healthcare

Blockchain is an emerging technology gaining traction because of its novel uses in the healthcare sector. Digital transformation profoundly impacts the enhancement of quality of life, establishing it as a leading domain for innovation. BT is progressively being adopted, especially within the financial industry. The healthcare sector faces numerous significant and unique opportunities, particularly in research, logistics, and practitioner-patient relations.

3.4.1 Search Strategy

The present study adapted techniques that synthesized complete criteria for ar- ticle assessment from previously published works. Our methodology had three primary phases: preparation, execution, and information reporting. To identify previously examined study contexts and primary constructs: to summarize find- ings and limitations to ascertain current intellectual capital; to extract key health informatics. Three suitable keyword combinations were identified for a database search: ”Health management”, ”blockchain in healthcare” and ”medical manage- ment”. The keywords were extracted from an analysis of previous studies in this domain that employed analogous keywords, including blockchain, healthcare and medical.

Step 1: Planning

1. **Identified Research gaps need for our requirement**
2. **Research questions & Objectives delineated**

3. Specifying appropriate database & Selection criteria

Step 2: Execution

1. Database Search

2. Article Screening

3. Select articles curated for the present study

Step 3: Assimilation

1. Information Extraction & Structuring

2. Synthesis of focal areas

3. Proposition of future research issues

3.4.2 Databases and Search Techniques

A variety of industries may derive the greatest advantages in medical sector, where patient confidentiality is paramount and the verification of financial transactions is essential, blockchain's principal objectives of secure data transmission and transaction documentation may be most advantageous. Moreover, Bitcoin could enable expedited data transmission and contribute to the development of a secure re- mote patient monitoring system for tele medicine. The decentralized architecture of blockchain may complicate patients ability to modify their data. These are but a few of the gaps that Bitcoin could potentially address.

Table 3.1: Findings from the work

Research	**Objective**	**Challenges**	**Ref**
System for Managing	Development of a decentralized data	Data privacy, data transit, data security, and accessibility	[69-73]
Data security and storage	Creating technologies for safe data transfer and storage	Data integrity, data security, data permission, and safe transmission	[71-81]

3.4.3 Difficulties Associated with Security

The blockchain's application and architecture are riddled with security holes. Blockchain security weaknesses are often the result of problems with the consensus

Table 3.2: Findings from the work

Aspects	**Criteria**	**Explanation**
Cost saving	Regulation of drugs and medical equipment	Medical facilities are able to track the movement of medications and equipment in real time.
Community organization	Management of Health	Blockchain-based consumer health data collection
Medical Records	Digitalized	Blockchain helps maintain data

mechanism that authorizes and verifies transactions. The following are examples of security flaws: 51 per cent, block rejecting, greedy mining, block holding, DDoS, difficulty climbing, transaction malleability, eclipse, and double-spending attacks. These security vulnerabilities are not addressed by the consensus process algorithms of the distributed blockchain system. Threats cannot be eliminated by theoretical reasoning alone since the required resources are very expensive.

Consensus approaches have very little role in addressing these security issues. That is to say, a protocol with defenses against such attacks should be part of the perfect solution. Malicious software may construct decentralized applications by taking advantage of security flaws in the blockchain. These malevolent assaults use security gaps in the execution of smart contracts to carry out more serious offenses like data and identity theft.

The usage of blockchain introduces another possible weakness (i.e., pseudo-anonymity), wherein the public nature of the Blockchain Network allows the stream of transactions to be monitored to get true identities or other pertinent information [66].

3.5 Discussion

Bitcoin lends clinical investigations more validity and useful information. The digital fingerprint may be used to save the documents as smart contracts on the Blockchain. There are numerous advantages to using Bitcoin in the healthcare industry, including the implementation of uniform permission protocols for accessing electronic health data, participant identity verification and authentication, and network infrastructure security at all levels. The pharmaceutical supply chain is managed and drug commitments are tracked using a blockchain. This technology can be utilized for the analysis and validation of certain treatments because it can save patient data at the individual level. Blockchain is used to monitor patients, manage clinical trials, maintain medical records, enhance safety, disseminate information, and promote transparency. It preserves hospital financial statements while cutting down on the time and expense of data translation. It tackles many issues in the context of a data-driven society. Each block of patient medical records will use Bitcoin to create a hash. Additionally, the blockchain approach would encourage patients to provide third parties with necessary information while maintaining the privacy of their identities. Several data sets must be completed for a clinical inquiry. These data sets are the subject of the study, and regular systematic experiments are carried out to produce analyses, estimates, and efficiency ratios under various circumstances. Once we analyze the data, we draw conclusions from the results. However, many scientists might manipulate the results by fabricating the evidence and data gathered. Numerous pharmaceutical companies would also like to document the results that could lead to these benefits for their operations. Because of this, researchers are using Bitcoin to make clinical studies more transparent and equitable. It will make it possible to record clinical research that is safe, asymmetrical, and straightforward. The information gathered could improve post-market research and patient care, leading to maximum efficiency gains. These guidelines are based on the core features of Bitcoin, which include robustness, enhanced security and privacy, open management, visible audit trails, and unambiguous data visibility. This enables medical professionals to adhere to the most recent regulations, particularly those pertaining to pharmaceutical supply chain safety.

3.5.1 Future Recommendations

The healthcare sector utilizes Bitcoin, which presents certain issues that require resolution. The principal obstacle encountered by medical institutions in using this advanced technology is a lack of knowledge. However, it relates to the responsibilities of medical groups and regulators. The healthcare industry has to be improved. This technical advancement will increase its usefulness in the medical field by offering a thorough understanding of treatment results and developments. The fundamental framework for communication of data and transaction verification is provided by Bitcoin. Bitcoin will make it easier in the future to record and authenticate transactions with network members' consent. By providing strong security at the patient level via public and private key encryption, blockchain will be the cornerstone of a new era in the transmission of health information. This technology ensures improved patient records, prevention of violations, heightened interoperability, optimized processes, effective medication and prescription management, and robust monitoring of medical. The healthcare industry is expected to significantly profit from the implementation of Bitcoin in the next years.

3.5.2 Difficulties Associated with Privacy

However, if Bitcoin is used to improve current EHR programmes, the requester will want dependable patient data to provide customised services. It is now considerably more difficult to identify the specific patient using their account number thanks to this capability. Any such structure should address issues.Additionally, a few extra steps are added to confirm the patient's reliability and credibility when a second node is added to the distributed ledger system that new patients need.

3.5.3 Access Control Problems in Medical System

The authors of [41] addressed the issue of centralized authentication and protected the system from certain security vulnerabilities that arise when patient data is transferred between healthcare providers by developing a safe, decentralized authentication provider. The proposed solution addresses authorization and authentication problems associated with the sharing of private data in the existing EHR healthcare systems. It's incredible that blockchain technology can be utilized for authentication. In [67], they suggested using IoT RPM in conjunction with a blockchain-based technique to safely authenticate and connect in healthcare systems.

3.5.4 Limitations

Although these are acknowledged, prior research suggests that there are technical challenges. The protocols, novel algorithm development have divided the current limitations into four groups based on our research: performance, ethics, protection, assumptions, and restraints.

3.6 Summary

The intrinsic decentralization and encryption of Bitcoin render it very adaptable for various applications in the medical industry. It increases the profitability of health information, improves the security of people's electronic medical data, helps combat counterfeit drugs, and develops the capacity of healthcare organizations to work together. Some healthcare occupations might undergo significant changes Using smart contracts to enable digital contracts is one important way that they eliminate middlemen from the payment process, smart contracts save costs. The degree to which the ecosystem incorporates and makes use of the related advanced technology will have a substantial impact on how well Blockchain is used in the healthcare industry. Clinical studies, medication monitoring,and system surveillance health insurance,are all included in the research. The reliance on a central storage system in the meta verse poses risks of data leakage, manipulation, or deletion. In these and numerous instances, Bitcoin may play a crucial role in achieving a balance between interoperability and security.

Chapter 4

Deep Neural Network and Fully Homomorphic Encryption -Based Privacy Preserving Model for EHR

4.1 Introduction

The growing concern for data privacy in Machine Learning (ML)has propelled the adoption of FHE as a leading solution. FHE allows for operations on encrypted data without exposing the underlying sensitive information, ensuring that computations can be performed securely. The fundamental security model for FHE is known as indistinguishable under chosen-plaintext attack (IND-CPA) [68] , providing a high level of assurance against data breaches. To execute machine learning tasks while maintaining data confidentiality, MLPPM systems rely on FHE, which enables computations to be performed on ciphertext's without requiring decryption.The Fast Fully Homomorphic Encryption (FFHE) for the Torus,developed by Lou and Jiang, has been notable for its efficiency in processing homomorphically encrypted data [97]. Unlike a fully homomorphic extended (FHE) version, TFHE employs a leveled approach that avoids bootstrapping. This method predetermines network characteristics, bypassing the need for bootstrapping but requiring impractically large parameters for complex neural networks. Additionally, the packing technique in TFHE can lead to inefficiencies in runtime and memory usage, especially when processing multiple data points simultaneously [97]. Thus, bootstrapping in conjunction with FHE is preferred to enhance the packing approach and improve the performance of MLPPM simulations.

The Cheon-Kim-Kim-Song (CKKS) scheme, along with the Brakerski-Fan-Vercauteren (BFV) scheme, represents a category of word-wise FHE systems. The CKKS scheme, in particular, is well-suited for handling encrypted real data and has been widely adopted for MLPPM applications[59]. Traditional FHE-based models have struggled with complex classification tasks when applied to datasets beyond simple examples like MNIST. One approach to address this limitation has been to approximate non-arithmetic activation functions using basic polynomials. The introduction of bootstrapping, which involves generating a new cipher text by increasing the level of the existing one, has been crucial for enabling deeper lay- ers in neural networks [63][64]. Early methods faced challenges with limited layer depth due to inefficient bootstrapping techniques. However, recent advancements have improved the accuracy, temporal complexity, and implementation of boot- strapping methods [65][69]. Utilizing pre-trained model parameters helps mitigate the high cost of training, which requires extensive computational resources and time.

In this study, we utilize the SEAL library (version 3.6.1) [107], which implements the CKKS-RNS for the MNIST dataset. CKKS-RNS scheme according to guidelines [64] [70] to enable operations. ResNet-50, a well-established convolutional neural network (CNN) model, is chosen for its precision and effectiveness in image classification. The model’s architecture, featuring multiple residual blocks, enhances its ability to achieve high classification accuracy by combining more layers.

To address the challenges of evaluating non-arithmetic functions in encrypted form, we use advanced approximation techniques. The ReLU function is approximated using min max polynomials [71] , which provide a practical approach for evaluating activation functions within the constraints of FHE. By integrating bootstrapping with the CKKS-RNS scheme, we demonstrate the potential for deep learning models to perform effectively on encrypted data.

Model extraction attacks pose a significant risk to MLPPM systems, particularly when Softmax functions are not evaluated within the FHE scheme [72] . To mitigate this risk, we utilize FHE to evaluate the Softmax function directly, ensuring that the model's privacy is protected against extraction attacks. This approach represents a novel application of FHE in preserving privacy while performing machine learning tasks.

The pretrained model parameters for ResNet-50 were computed with encrypted input images with pre-trained plain text parameters to achieve accurate results. The proposed model's performance is evaluated based on its similarity to the original ResNet-50 model. The MLPPM model achieves a classification accuracy of 92.43% ± 2.65%, which is comparable to the original model's accuracy of 91.89%. This demonstrates the effectiveness of the MLPPM model in handling encrypted data while maintaining high classification performance.

Considerable research has been dedicated to adapting machine learning mod- els for compatibility with Homomorphic Encryption (HE) schemes. A notable approach involves modifying traditional models to align with HE by substituting standard activation functions with simple nonlinear polynomials. This adaptation results in what is known as the "HE-friendly network" [69] [73]. Despite the po- tential advantages of this method, such as enhanced privacy guarantees, it has not yet resulted in a superior MLPPM machine learning model. For instance, CNNs with word-wise HE implementations using basic polynomial activation functions have demonstrated a classification accuracy of 91.5% on the MNIST dataset [73]. While this represents a significant achievement, these models frequently show lim- ited efficacy on more complex datasets and tasks. The simplistic substitution of well-established activation functions with basic arithmetic functions may not be the optimal solution, given the nuanced role that activation functions play in ad- vanced machine learning models. Additionally, these models often necessitate a time-consuming pre-training phase. Given the substantial data requirements and the prolonged training duration, leveraging pre-trained parameters from standard models such as ResNets and VGGNet on plain text data is advantageous for preserving the privacy of the test datasets.

Moreover, prior research has explored the use of Multi Party Computation (MPC) methods for evaluating non-arithmetic activation functions within privacy- preserving machine learning frameworks [73] [74] [75] [76] [77]. While MPC can accurately process non-arithmetic functions, it poses significant privacy risks. Specifically, the client must be privy to the model's activation functions, which undermines the confidentiality of the MLPPM server's model. This requirement is problematic for MLPPM scenarios where maintaining data privacy is paramount. Additionally, the necessity for client participation in computations complicates the communication process, which is not ideal for privacy-preserving applications where communication efficiency is crucial.

This research highlights the importance of optimizing the configuration of lev- eled homomorphic encryption systems, which often necessitates substantial cir- cuit depth. Consequently, achieving practical implementations requires defining parameters that can accommodate deeper circuits. The challenge lies in the fact that the required parameters for evaluating more comprehensive learning models may be impractical within typical computational environments. Furthermore, the running time for homomorphic encryption operations may exceed linear time as circuit depth increases. This limitation underscores the need for efficient homo- morphic encryption strategies that balance practical feasibility with the complex- ity of deep learning models. Therefore, a critical area of research is the application of deep learning models based on FHE heuristics, which offer initial parameter sizes unconstrained by circuit depth. By addressing these challenges, researchers aim to develop practical solutions for implementing deep learning models within privacy-preserving frameworks.

Overall, the landscape of privacy-preserving machine learning is marked by ongoing efforts to enhance model accuracy and efficiency while ensuring robust privacy protection. The exploration of HE-friendly networks, MPC methods, and leveled homomorphic encryption techniques reflects the complexity of achieving effective and practical solutions in this field. Continued research is essential for advancing the state-of-the-art in privacy-preserving machine learning in sophisticated models.

4.2 Proposed Methodology

4.2.1 CKKS-RNS Scheme

The CKKS scheme represents a significant advancement in FHE by facilitating arithmetic operations on encrypted data, whether the data is in the form of real or complex numbers. This encryption method organizes each element is referred to as a ”slot”. The CKKS scheme allows for manipulation of encrypted data without requiring decryption, provided the user possesses the public key ring learning with errors (ring-LWE) assumption, a well-established cryptographic concept.

Most operations, with the exception of homomorphic rotation, are executed on a component-wise basis. Non-scalar multiplication is applied directly to the cipher text, while scalar multiplication is performed with plain text values. Rotation operations shift the vector homomorphically across multiple stages.

During the encryption process, data is approximated to the nearest integer and scaled by a large number known as the scaling factor. Homomorphic multiplication also involves multiplying the scaling factors of the data being multiplied, necessitating a rescaling operation to restore the original scaling factor. Traditional implementations of CKKS use a multi-precision library to manage the significant numerical demands, which results in increased computational costs. To enhance efficiency, the CKKS-RNS variant was introduced. In the Residue Number System (RNS), large integers are decomposed into smaller, more manageable components, allowing arithmetic operations on these smaller integers to correspond with operations on the larger values. This approach reduces computational overhead and improves overall efficiency Homomorphic rotation, we consider left rotation with r steps. Evaluating the Rectified Linear Unit (ReLU) function is essential for many neural network models but presents a challenge due to the need for high computational precision. In the context of the original ResNet-50 model, approximating the ReLU function with a single high-degree min max polynomial requires substantial computational resources.

To address this, we employ an alternative method for approximating the ReLU function. This approach reduces the computational resources and time needed for homomorphic evaluation, making it more feasible to process non-arithmetic functions like ReLU within a homomorphic encryption framework.

Overall, the CKKS-RNS scheme enhances the efficiency of fully homomorphic encryption by breaking down large integers into smaller components, which allows for more manageable computations. The improved approximation techniques for functions such as ReLU further optimize the performance of encrypted machine learning models, making it practical to deploy complex models like ResNet-50 in privacy-preserving environments.

$$\mathrm{ReLU}(x) = 1\ 2\ x(1 + \mathrm{sign}(x))\text{............}(4.1)$$

To determine the optimal composite polynomials for approximating the sign function, a systematic methodology is applied. This involves first identifying each polynomial that forms part of the composite polynomial. To minimize the computational complexity while achieving the desired precision, a dynamic programming method is employed to calculate the degree of the polynomials. This approach ensures that the number of non-scalar multiplications needed is optimized, balancing computational efficiency with accuracy in the approximation.

4.2.2 Novelty for ResNet-50 ON CKKS-RNS Scheme

Since stride of one or two is the sole convolution used in ResNet-50, we take it for granted.

Initially set to zero, this parameter is incremented by one during the strided convolution process. Gazelle's convolution technique is used for non-strided convolution, with steps modified by 2 slot str. Strided convolution resembles non-strided convolution, however with particular modifications for filtering. Bootstrapping in ResNet-50 is the most time-intensive phase, and the cipher text level for every

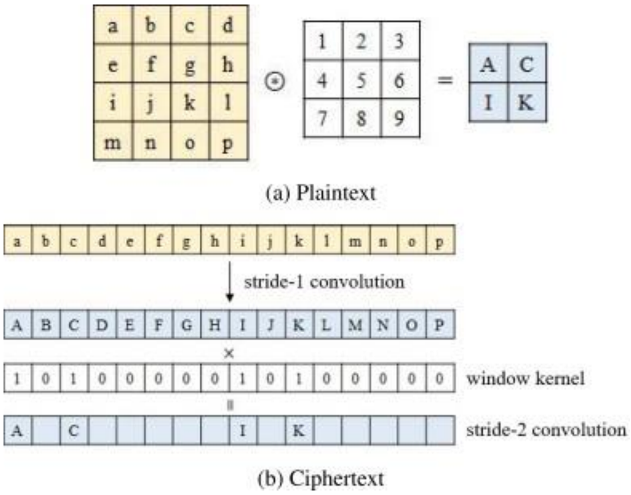


Figure 4.1: Stride-2 convolution

key-switching transaction during bootstrapping stays invariant, irrespective of the Residual Network-50 (RESNET) design. Due to the multiple rotation operations involved in convolution, the number of key-switching operations is considerably higher compared to that in the ReLU function. Hence, bootstrapping should be performed immediately after the convolution process, with subsequent convolu- tion operations executed at the lowest level of cipher text to reduce the number of required rotation operations.

4.3 Implementation of Resnet-50 on CKKS-RNS

The ResNet-50 model’s structure is shown in Fig.2, and its specifications are displayed in Table 1. via this framework, we create our ResNet-50 implementation structure via the CKKS-RNS scheme, as seen in Fig.4. This framework includes convolution, fully connected layer and Softmax. With the exception of the addition of bootstrapping processes, This device and the original ResNet-50 model are almost identical.

4.3.1 Setup in General for the CKKS-RNS Scheme

Parameters

Bootstrapping, the number of levels is 13, while for general homomorphic processes, it is 11. With a maximum bit length of 1450 modulus, the system meets a security criterion of 111.6 bits. The hybrid dual attack, The most effective method for attacking the LWE with a sparse key and is used to establish the security level . The details are provided in Table 2.

Each image is processed simultaneously, represented as a 32 × 32 × 3 MNIST RGB image. By selecting suitable parameters, we use 215 message slots within a single cipher text, which is half the polynomial degree. To efficiently compress an MNIST image channel into one cipher text, we apply the sparse packing technique and use only 210 sparse spaces, rather than all available slots. This approach allows for more efficient convolution operations with fewer rotation steps, resulting in a significant reduction in bootstrapping time compared to fully packed cipher text. Since the slot structure parameter produced by strided convolution alone is inadequate, we build the encrypted tensor structure, taking into account the tensor's dimensions within the encrypted data to aid comprehension.

Table 4.1: The ResNet-50 standard

Layer		**Input size**	**Inputs**	**Output Size**	**Outputs**
Conv1		32 x 32	3	32 x 32	16
Conv2	2-1	32 x 32	16	32 x 32	16
	2-2	32 x 32	16	32 x 32	16
	2-3	32 x 32	16	32 x 32	16
Conv3	3-1-1	32 x 32	16	16 x 16	32
	3-1-2	16 x 16	32	16 x 16	32
	3-1-s	32 x 32	16	16 x 16	32
	3-2	16 x 16	32	16 x 16	32
	3-3	16 X 16	32	16 x 16	32
Conv4	4-1-1	16 x 16	32	8 x 8	64
	4-1-2	8 x 8	64	8 x 8	64
	4-1-s	16 x 16	32	8 x 8	64
	4-2	8 x 8	64	8 x 8	64
	4-3	8 x 8	64	8 x 8	64
Average PoolIng		8 x 8	64	-	64
Fully Connected		64 x 1	1	-	10

4.3.2 Data Range and Precision

ResNet:

The Residual Blocks idea was created by this design to address the issue of the vanishing/exploding gradient. We apply a method known as skip connections in this network. The skip connection bypasses some levels in between to link-layer activations to subsequent layers. This creates a leftover block. These leftover blocks are stacked to create resnets. The strategy behind this network is to let the network fit the residual mapping rather than have layers learn the underlying mapping. The benefit of including this kind of skip link is that regularisation will skip any layer that degrades architecture performance. As a result, training an extremely deep neural network is possible without encountering issues with vanishing or expanding gradients.

Polynomial estimation is often used to estimate continuous functions in situations with sparse data sources. The output’s absolute value might increase significantly and result in classification problems if any one value in the message exceeds slots beyond this limited range. ReLU, bootstrapping, as well as Softmax functions are examples of non-arithmetic procedures, polynomial approximations are necessary because FHE supports only arithmetic operations. Therefore, the approximation range must encompass the input values for these functions. In the context of ResNet-50, we evaluate the absolute values of inputs for Softmax, bootstrapping, and ReLU functions using multiple images. It is hypothesized that the actual input values for these processes are highly likely to be below 40, as the highest absolute value recorded for these functions is 37.1. Based on this observation, all techniques are implemented accordingly. We also employ an average accuracy of 16 bits while estimating all non-arithmetic functions since investigations show that the precision of estimated polynomials or functions must be at least 16 bits beyond the decimal point.

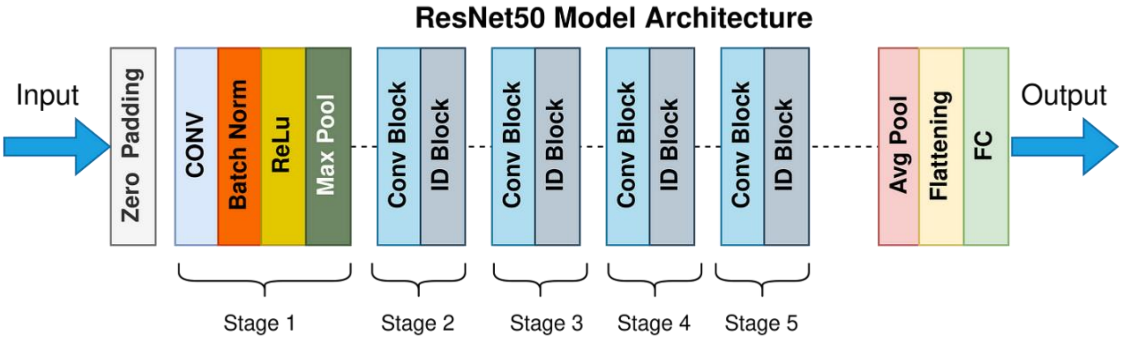


Figure 4.2: Structure of ResNet-50

4.3.3 Optimizing the Accuracy of Homomorphic Operations

To optimize accuracy while minimizing rescaling and linearization, we employ several techniques, including scaling factor management helps in maintaining ac- curacy and avoiding errors in the resulting message. Since Number-Theoretic Transformation(NTT) can be computationally intensive, lazy rescaling and lazy relinearization provide alternative methods to enhance processing efficiency.

.

4.3.4 Implementation of ReLU Function

Using the CKKS-RNS scheme, we first implemented the ReLU function in ResNet-50 by using the the min max polynomials approximation method created[114]. This method involves conducting iterative simulations of ResNet-50 under the CKKS-RNS framework while adjusting accuracy parameters as needed. Our findings indicate that a precision of 16 bits consistently provides effective performance. By integrating state-of-the-art bootstrapping techniques with FHE, we demonstrate the feasibility of running deep neural networks like ResNet-50 on encrypted data while preserving data privacy. The SEAL library was utilized for this purpose, along with advanced bootstrapping methods [72] [78] .We implemented Coeff to Slot and Slot to Coeff operations with a depth of two using FFT structure [79].

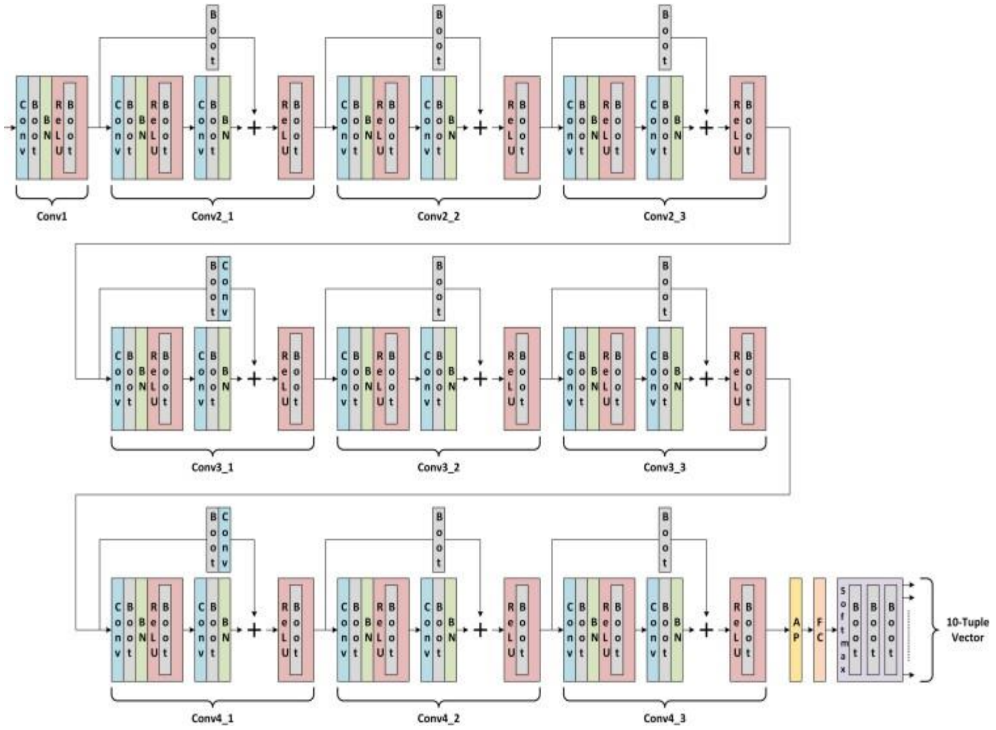


Figure 4.3: ResNet-50's architecture for the CKKS-RNS scheme

Mod Reduction was constructed using Remez technique is used to properly esti- mate the cosine function and double-angle formulae [80] [76].

A significant challenge in using the CKKS-RNS system is bootstrapping failure, which can severely impact the overall performance of the neural network. This issue typically arises when a slot in the Mod Reduction procedure's input cipher text falls outside the defined approximation range, leading to potential failures in bootstrapping.

4.3.5 Pooling Averages and Fully Connected Layer

After completing all convolutional layers, the tensor is reduced to a size of 8 × 8 × 64. To convert this tensor into a vector of length 64, we apply average pooling across each channel. A completely linked layer is then used to produce a final vector with a length of 10. Each member of the 64-length array of cipher texts that is the result of the average pooling procedure includes information related to the starting slot. During the fully connected layer operation, no rotation is necessary as the data are divided among separate ciphe rtexts.

4.3.6 Simulation Results

The proposed method was implemented using Microsoft's SEAL library [81] ,augmented with our CKKS-RNS bootstrapping solution. The simulation environment consisted of 512GB of RAM. To enhance the execution speed of ResNet-50, we utilized the OpenMP library, assigning a single thread to each channel across all layers. The total memory requirement for the simulation was 172GB. For training the model parameters, we first normalized the training dataset by removing the mean pixel values. We used 32 × 32 RGB images and applied data augmenta- tion techniques such as horizontal shifting and mirroring. He initialization was employed for weight initialization without dropout. The model was trained using a cross-entropy loss function with 32 × 32 mini-batches. The learning rate was initially set to 0.001 and was reduced to one-tenth after 80 epochs, with a further reduction after 120 epochs.

Table 4.2: Comparision of various models

.

Model	Accuracy
CNN	90.56
VGG16	89.12
ResNet-501	91.89
ResNet-502	92.00
MLPPMResNet-50	92.43

The model is deployed on a Hardware with 24gb Internal Ram along with GPU Processed machine with NVIDIA Graphic Chip set for processing the data. The model has an estimated running time of 38mins. The original ResNet-50's classification accuracy for the same plain text picture was 92.95%± 2.56%, but the ResNet-50's classification accuracy for the encrypted data is 92.43%± 2.65%. The proportion of cases where the classification output in the proposed MLPPM model matches We also measure what is called the agreement ratio in the original

ResNet-50 model. We have a rather good agreement ratio. 98.43%± 1.25%. As a result, we confirm that the CKKS-RNS scheme can effectively run the ResNet-50 with enough accuracy for classification and the right bootstrapping procedure.

4.3.7 Discussion

Running Time

The model's current execution time of approximately 3 hours reveals significant challenges for practical applications. This duration highlights the necessity for substantial optimization to make the use of FHE in deep learning models more feasible. Our research shows that FHE can be used with respectable accuracy on common deep learning models. However, a few adjustments are necessary to make this strategy workable for real-world applications.. Future improvements could involve incorporating hardware accelerators such as GPUs, FPGAs, or ASICs, which are known to enhance computational efficiency significantly. Additionally, advancements in FHE techniques and implementations could contribute to faster processing times. By leveraging these accelerators, it may be possible to reduce the runtime substantially, making FHE more viable for deep learning applications. Moreover, applying the MLPPM model to individual images rather than batches and optimizing the CKKS-RNS scheme's packing mechanism could further reduce execution time. This approach will be explored in subsequent research to optimize batch processing and enhance overall performance.

Security Level

Model is set at 111.6 bits, which represents a minimal threshold of security considered adequate for many applications. However, this level is somewhat below the commonly accepted standard of 128 bits, which is often used to ensure higher security levels. Although 111.6 bits provides a foundational level of protection, there is room for improvement. The security parameters of the CKKS-RNS scheme can be adjusted to enhance security, as higher security levels generally result in longer processing times. Therefore, adjusting the parameters to achieve a higher security level may be necessary depending sensitivity of the data being processed.

Classification Accuracy

In training machine learning models, the initialization of weights is typically random, which introduces variability in the results even with identical hyper parameters. To accurately assess model performance, it is important to consider the average accuracy obtained over multiple training sessions. For this study, we focused on demonstrating the feasibility of applying ResNet-50 to homomorphically encrypted data. Despite training the model only once, our results show that the accuracy achieved with the encrypted ResNet-50 is nearly identical to that of the original, non-encrypted model. This finding is consistent with our earlier research [32] , which indicates that FHE bootstrapping can preserve accuracy in deep learning models.Additionally, it is anticipated that deeper networks beyond ResNet-50 could achieve similar results when bootstrapped with FHE, further validating the approach.

4.4 Summary

This study has successfully applied the advanced FHE technique CKKS-RNS to the ResNet-50 deep neural network, demonstrating that it is possible to achieve high classification accuracy while maintaining the confidentiality of the data. By employing precise approximations for critical functions such as ReLU, models can be effectively utilized with word-wise FHE. This approach eliminates the need for retraining and provides a robust framework for future research. The results obtained indicate that FHE can be integrated into deep learning models without compromising accuracy, paving the way for further exploration and optimization in this area. The promising results of this study suggest that with continued advancements in FHE technology, its application to more complex models and larger datasets will become increasingly practical and efficient.The Machine Learning Privacy-Preserving Model (MLPPM) employs FHE to ensure data privacy and security while performing machine learning tasks. This study focuses on advancing MLPPM models by utilizing the CKKS-RNS FHE scheme and bootstrapping to address the limitations of traditional FHE methods. Existing models like CryptoNet, SEALion, and CryptoDL primarily cater to basic or nonstandard machine learning models and have demonstrated limited effectiveness with more sophisticated datasets. These methods typically with approximations before bootstrap- ping, restricting the model's depth and complexity. By integrating CKKS-RNS and employing advanced approximation techniques for non-arithmetic functions such as ReLU and Softmax, this study presents a robust approach. Our model, based on ResNet-50, was validated using the MNIST dataset and demonstrated high accuracy and performance. The proposed MLPPM model achieved a classi- fication accuracy of 92.43% ± 2.65%, closely aligning with the original ResNet-50 model's accuracy of 91.89%. Inference was performed in 20 minutes on a dual Intel Core i7 CPU with 8 GB RAM, showcasing the feasibility of applying FHE to complex machine learning models.

Chapter 5

Blockchain-Based Secure Multiple Computation Scheme for Preserving and Extraction of Health Care Data

5.1 Introduction

The initial purpose of Secure Multiple Computation was to provide a decentralized solution to ”The Millionaires Problem”.The two-party calculation was expanded to include many parties [82]. A collaborative computing issue that safeguards privacy amongst a collection of untrusted individuals is solved using MPC. In this case, many parties with secret input want to compute a function together and get separate outputs. The intended outcome is the only information the participant receives throughout this process [83].

A variety of health-related data about individuals is collected in Electronic Healthcare Information (EHI). This data includes both medical information (diseases, prescription drugs, medical images, doctor names, hospital names, etc.) and person-specific information (social identity number, patient name, age, gender, address, etc.). Some patients (individuals) in this data have sensitive values and choose to disclose their identities to the public. Therefore, safeguarding this private information from unwanted access while providing it to insurance companies and researchers is the healthcare system’s most important responsibility. The conventional method of storing and managing this electronic medical data via a centralized system has the disadvantage that it is hard to guarantee the data integrity of the EHI. With its evolution, cloud storage has become a reliable third-party service provider for data storage and data transfer [84].

Single points of failure, vulnerability, and inadequate privacy and security characterise cloud-based data systems. Additionally, since third-party services are necessary for cloud-based data sharing, there is a greater chance of data theft, leakage, manipulation, or misuse [85]. While certain cloud-related problems have been resolved by prior cryptography and anonymity solutions, the single point of failure issue still cannot be resolved. On the other hand, access control for electronic health information is often centralized and based on roles. On the other hand, the role-based access control (RBAC) paradigm requires the definition of complex rules in order to restrict access for different types of data users [86]. The process of establishing and modifying rules is especially susceptible to an attack because of the centralized data storage, which might swiftly elevate privileges and get authorization for the whole dataset [87].

Distributed ledger technology, or blockchain, seeks to decentralize data storage while also making it more secure and impossible to mess with. Substituting it for centralized cloud storage solutions might be a smart move [88] [89]. Thanks to the smart contract function in the blockchain ecosystem, players from vari- ous organizations, such as policy makers, insurance corporations, and hospitals, may decentrally check requests for data access. To further simplify the setup of data access limitations based on user attributes, the Attribute-Based Access Control(ABAC) approach may be used.

To protect the confidentiality of electronic health record data, we propose BSM-PCS, a blockchain-based substructure. Before being uploaded to the blockchain, the whole dataset is encrypted using the homomorphic encryption approach. Using this technique for comparisons and other operations only necessitates encryption; decryption is not necessary. On top of that, the owner will have the option to decode the encrypted text in order to get plain text from the generated output. Data that has to be sent between various organizations or in decentralized situations is best protected by this kind of encryption.

The paper is organized with background work in section two which refers how actually technology works and its application in the current work. Literature survey in section three. Proposed work in section four with methodology in section five followed by experiments and results in section six and finally conclusion.

5.2 Background Work

5.2.1 Blockchain-Based Secure Multiple Computation Scheme

Many effective secure multiple computing techniques have now been suggested by researchers [86] [89] . They have finished the secure multiple calculation for func- tion, even in a lab setting [90] .Under the assumption of a semi-honest opponent model, the majority of this study focuses on increasing the efficiency of MPC as much as feasible. In other words, everyone involved in secure multiple compu- tation is sincere. Regretfully, the present circumstances do not align with this. In actuality, there are malevolent opponents that deliberately alter the protocol's execution in order to achieve the desired attack outcomes.Under the malicious adversary concept, there are also a few secure multiple computation techniques
[91] [92].
However, two things really continue to occur:

1. When one party receives findings that are more beneficial to him than to others, he won't disclose them, which prevents other parties from receiving the desired benefits.

2. Attacks by hostile opponents are a persistent source of disruption to the protocol, preventing it from functioning properly.Therefore, in practice, a realistic MPC is also very desired to be resilient.

5.2.2 Smart Contract

A PC convention that meticulously works with, verifies, or executes the ar- rangement or execution of an agreement is known as a smart agreement. Astute contracts enable confidential conversations, comprehensive body of legislation, or external execution element [93] [94]. They provide observable, uncomplicated, and irreversible algorithms for trades.

5.2.3 Bitcoin

The Bitcoin distributed computing platform allows users to access the chain and perform smart contract functions. The block chain is available to the public [8]. Each user has access to an authenticated account in order to conduct block chain transactions. All operations and transactions are recorded in terms of units of gas. Every petrol unit may be mined or bought with cryptocurrency. At the moment that a user triggers a transaction, the triggered transaction 's execution cost is added up.

$$\mathbf{Po\ T=(EC\ +T\ C)*p.} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\mathbf{(5.1)}$$

Transaction cost and P is the price of 1 gas unit.

5.2.4 IPFS

IPFS is both a convention and an organisation designed to provide a common, substance-addressable inside a conveyed record framework [95]. This eats away at the material that it keeps inside the company. An archive, audio file, image, videostored data. The arrangement of these identifiers is merkle dag. PKI-based character is used by IPFS as an organisational model[96]. A programme that can locate, share, and replicate merkledag items is called an IPFS Node. A private key identifies its personality [97].

$$\underline{K}eyGen \rightarrow PUKey,PRKey \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5.2)$$

$$\mathbf{Node\ Id= Multi\ Hash(PUKey).} \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \mathbf{(5.3)}$$

5.3 Methodology

Bitcoin offers a decentralized, immutable network where all nodes may verify transactions using smart contracts and consensus techniques. The blockchain has been employed by a number of healthcare systems [98] [99] because it is a trustworthy way to increase communication security and privacy.

Authors have used smart contracts in [100] to create a system that allows for remote patient monitoring and emergency notifications to medical professionals.Through blockchain, this remote monitoring system ensures the patient's protection and privacy [97]. There are three actors and three functions in the sug- gested system. The platform's patient and physician registration process is its primary use. They use a smartphone to access it and securely register personal information like name, age, and ID. They are also able to review and amend these records. Data from the IoT sensor will be processed for patient monitoring, and smart contracts on the blockchain will store the processed data. It is now sim- pler for physicians to monitor their patients in real time thanks to this step. The business and the medical gadgets are the subject of the final function. A smart contract is made between the patient and the corporation at the time of purchase to register the device in his name. The patient's data that the IoT instrument obtained is therefore recorded in the care facility [64] [101] [102] [103].

The authors of the study [104] use the concepts of smart contracts and multi-agent systems to oversee and manage pharmaceutical logistics operations. They provide a framework that enables transactions between the various system participants to be stored on the blockchain. These transactions are managed via smart contracts, independent of any other party. As a result, the system is less costly and delivers information more quickly. But in order to assess its effectiveness and performance, a working prototype must be created concurrently with empirical validation. Study game theory and safe two-party computation [6]. When a safe two-party system is transformed into a computation protocol, it preserves two sides' privacy, nash equilibrium, accuracy, and security [105].

The stated RMPC is reliant on game theory, which addresses MPC fairness but falls short in addressing robustness issues. The MPC protocols are expressly engineered to provide near-fairness and include a decentralized trusted third-party system, both of which are absent in real-world settings. As a result of the growing demand for block chain technology, which is embodied by Bit Coin [88], Bit Coin incentive mechanism became inseparable from Game Theory, and academics started incorporating Bit Coin's fail-safe mechanisms into MPC economics. It gives parties a great incentive to take part in MPC processes. Based on the Bit coin network, [89] [90] offered a safe two-party lottery mechanism. The parties get economic remuneration in the form of Bit currency or the product.

Multiple rounds of communication with the Bit coin network are required for the startup procedure. Several functions, such as the claim-or-refund functionality, the t (secure computation with penalties functionality), and the q (secure lottery with penalties functionality) [91]. They created the MPC protocol, which requires calling a continuous round. FCR Iddo Bentov and Ranjit Kumaresan conducted more study on using Bit Coin to inspire patients obtaining the accurate calculations [106]. Four unique features are included into the work: verifiable computation, fair secure computation, non-interactive reward, and secure computation with limited leakage.

Bit coin is beneficial for building a decentralized poker game, as explained [107] .In 2017, he once again put up an enhanced plan to achieve favourable outcomes [92]. He discussed the optimization process in this technique to produce a safe computational model. Many of the scientists looked at the bit coin concept in order to fulfill the criteria. To ensure the protocol's resilience, accuracy, and fairness, they made complete changes to the framework. Although there are sev- eral implementation restrictions for bit coins and block chains in the real world, scientists' evolving tactics provide successful outcomes in real-world situations. Due to the incompleteness of BitCoins scripting language, it is limited in its abil- ity to enable complicated tasks that are intricate and challenging to implement. These tactics work well in theory, but they are not recommended for the bit coin's implementation stage.

Global ledger-based multi-party computing protocol developed.Three elements are included in their work. Then, in order to achieve our objectives of robustness and fairness, an outsourced MPC scheme based on the EOS block chain was put forward. Nowadays, almost all of the top businesses choose and use the OAuth protocol [93] for their proprietary authentication, which functions as a reliable and trustworthy authority. Many researchers have put forward different methods to secure personal data from a security standpoint. Sensitive data in these anonymized datasets has to be protected. Every record at this location can be distinguished from at least k-1 other records [108] .A sufficiently wide range of feasible values of k-anonymity 1-diversity is used to represent the sensitive data. These methods are widely utilized nowadays to show how data sets are employed in our study [96] [97]. Numerous privacy-preserving techniques have differences that cause data exchange to be disrupted [64], and there are questions about how to compute encrypted data. One such method is called FHE for short
[101] . This method's use over encrypted data has a special quality. Although it may be effective in tackling real-world problems, it also has certain drawbacks. Thus, a plethora of alternative methods, such as accountable systems, have been developed as a remedy for this problem. It can safely transmit Bit Coin money between users without requiring a centralized system. Additionally, it has an open ledger and public verification capability. As block chain regulators, all projects are adopting this bit coin 2.0 together. We can accomplish trusted audibility with trusted functions by putting this into practice.Transparency, security, and effective, secure data are the outcomes.

The BiiMed platform was recommended by the authors of [109] . This strategy aims to distribute the patient's electronic health record across many parties. Data interoperability and integrity are provided via the blockchain. The BiiMed blockchain and the Health Information System (HIS) make up the two halves of the proposed architecture. Medical data is gathered, stored, and disseminated by the HIS, and shared data is maintained via the BiiMed platform [110].It is based on smart contracts and the Bitcoin blockchain. Data integrity and interoperability are essential components of electronic medical record interchange. These attributes are guaranteed by the technology built on a decentralized trustworthy network.

5.4 Proposed System

The platform that the proposed system, BSMPCS, uses to facilitate the sharing and exchange of patient medical data. Multi-agent systems and blockchain technologies are combined in this approach. Smart contracts and access control (ABAC and RBAC) are used to guarantee the security of the data that is altered by many stakeholders [111] [112] [113] [114]. A few conditions must also be met by the system. The identification of those authorized to take part in the elec- tronic medical record management procedure in the blockchain-based healthcare system has to be confirmed. In fact, in order to access resources, participants must verify themselves. Every participant also has a predetermined role in the way the patient file is processed. Actually, all of the resources people need to do their duties are available to them. Scalability is important because of the massive amounts of data that are transferred in the healthcare industry and the way the network grows with each new user. An electronic medical record system should have a flexible user interface that makes resource use simple and effective for all users in order for them to gain from the necessary medical data service. The CIA trifecta (confidentiality, integrity, availability) must be met by the application. To guarantee correctness and dependability, patient data must be shielded against viewing and any unauthorized access or change. Those with authorization who need it may also access it [115].

As shown in Figure 5.1 and the EMR system, several agents communicate with one another to share information. They make requests for or supply health information using a web application. They need to authenticate in order to access it. The automated and secure part of this transfer is added by the smart contract, depending on the kind of user. The relevant interface then displays the data that have been recorded on the blockchain. In order to protect patient data from

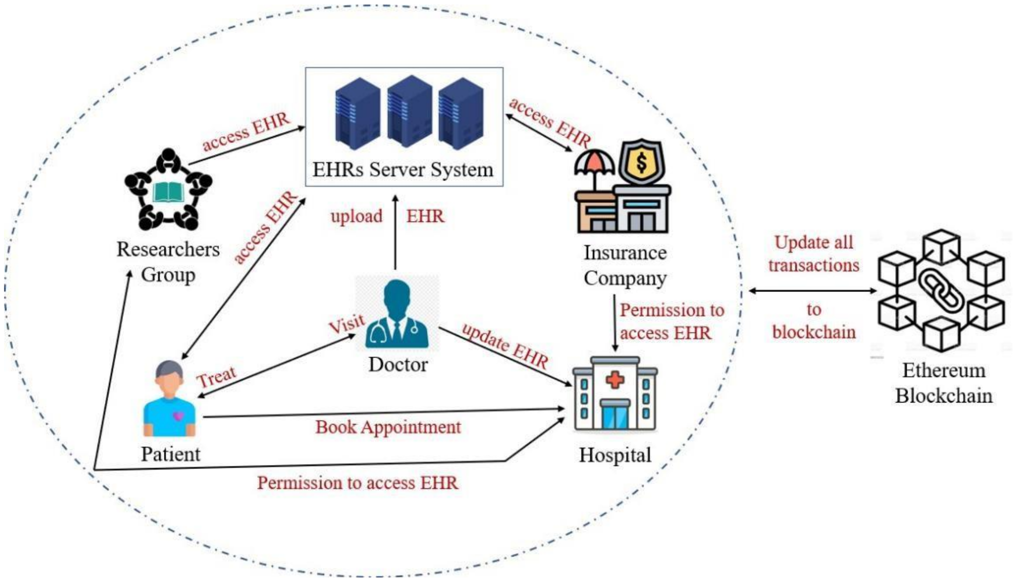


Figure 5.1: EHR privacy model in Blockchain

assaults, we attempt to give each user an access role because of the blockchain's transparency and immutability.

As shown in figure 5.1 , the entities of our EHR Privacy Model on Blockchain include patients, physicians, insurance companies, research groups, and hospitals. A patient's duties include updating the system with his medical information. The only legitimate form of identification the patient has is his Aadhar card, which is immediately connected to all the information he updates. A doctor's duties include making sure the patients they have registered are being treated [116] [117]. The physician obtains authorization to see the patient information stored in the hospital module. The physician establishes a treatment ID for the patient after reviewing the patient's medical data. He administers the precautions to the patient while also keeping an eye on them. The patient information that was registered for insurance is kept up to date by the insurance company. They keep records of information divided into categories, such as drugs that are covered by insurance and those that are not.

As shown in picture 5.2, The patient compiles all of his medical documents. He creates digitised versions of the medical records. The EHRs are transformed into encoded data. The encoded EHR is created by assembling the encoded components. The blockchain has been updated for these encoded EHRs. The doctor

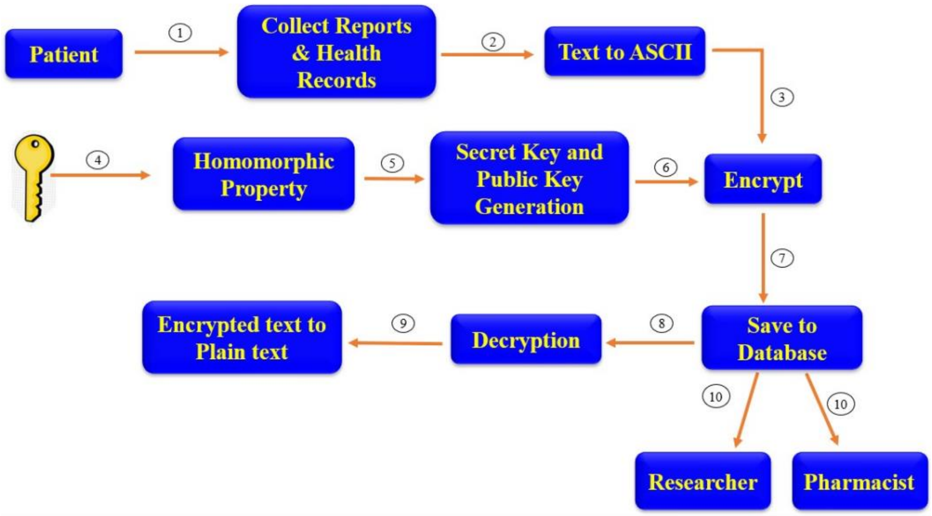


Figure 5.2: Flow of Homomorphic Encryption process

obtains authorization to see the patient’s information. The physician generates a treatment ID for further care after reviewing the patient’s electronic health record. The patient receives the prescription from the doctor after receiving treatment. The prescription reports are also prepared by the doctor and sent to the insurance company so that they may be included in the database’s list of prescribed drugs. The blockchain has been updated with the files in 8 and 9. The doctor sends the papers to the insurance company. In order for patients to register with them, they update the terms and conditions and medication files. The patients sign up with the insurance provider on their own. They produce the medical records that are linked to insurance. The blockchain is updated with these entries. To access the EHRs, the research team asks authorization from the hospital. RG secures the necessary authorizations to carry out different types of analysis on the EHRs.

In order to provide predictions and outcomes, RG analyses and evaluates the EHRs in a variety of ways. All of the produced forecasts and outcomes are updated on the blockchain. The hospital keeps an eye on other organizations and has the authority to grant or revoke them access to patient privacy-protected data.

5.5 Evaluation

5.5.1 Homomorphic Encryption

The algorithm used for performing homomorphic encryption is If the public key is (G, q, g, h),where = gx, and x is the secret key, then the encryption of a message is m (m) = (gr, m, r)for any random r{0, . . . , q − 1} in the ElGamal cryptosystem, which is a cyclic group G of rank q with generator g. Then, the homomorphic characteristic is

”(m1).m2 = (gr1,m1.hr1)(gr2,m2.hr2) = (gr1+r2,(m1.m2)hr1+r2)”=(m1.m2)

The formula Y= gx (mod p) ....(5.4)

He will email this to Alice. His public key is Y, g, and p.After that, Alice creates a message (M) and chooses a

arbitrary value (k). Next, she calculates a and g.

a = gk (mod p). ....(5.5)

b = ykM (mod p).............................(5.6)

After receiving these, both decrypt using

M=x (mod p)..................................(5.7)

This is effective because

$$\frac{b}{a^z}(modp) = \frac{y^kM}{(g^k)^x}(modp) = \frac{(g^z)^k\ M}{(g^k)^x}(modp) == \frac{g^{zk}M}{g^{zk}}(modp) = M$$

If we have

a 1 = gk1 (mod p)

a2 = gk2 (mod p)

b1 = yk M1 (mod p)

Following b2 = yk M2 (mod p), we get a=a1 × a2 = gk1×gk2 = gk1+k2.

ykM1 × yk M2 = b= b1×b2

$$M = \frac{b}{a^x} = \frac{y^kM_1 \times y^kM_2}{g^{k_1+k_2{}^z}}$$

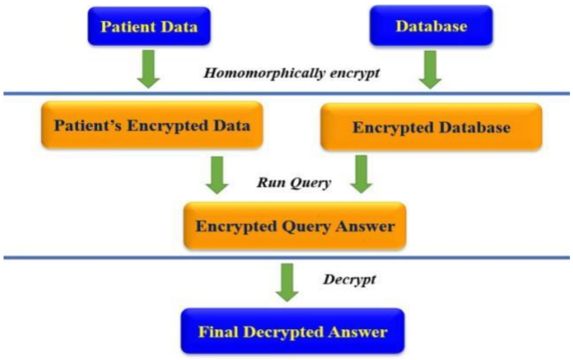


Figure 5.3: Homomorphic Encryption process in EHR-PP model

5.5.2 Algorithm for Registering Patients

This smart contract is responsible for registering the patients, fetching details of patients and updating the precautions of patients to the blockchain.

```
1. Begin
2. P_details[] ← Read patient's details (Aadhar number, Name, address, phone number)
3. if (P_ details[aadhar_ number].isValid()) then
    (a) if (P_details[aadhar_number].isAlreadyRegistered) then
        i. Display the message: "User already registered"
    (b) else
        i. Add details to blockchain
4. else
    (a) Display: "Please enter valid user details"
5. End
```

This function fetches the aadhar card number of the patient and checks whether he is registered.If the user is patient and already registered then the details will get updated.

5.5.3 Algorithm for Insurance Medications

This contract's responsibility is to maintain the data of the patients who registered for insurance. They also maintain the data of medications that are covered under insurance claim. If any necessary medications were not covered in the list formulated earlier, authorized doctors are given permissions to add the necessary medications to the insurance company data. This function takes in input of medication details. It checks whether the entered medications are covered under insurance or not.

```
1. Begin
2. Company details[] ← fetch(company id, name, phone number)
3. If (Company details[id].isNotRegistered) then
    (a) Add company details to blockchain
4. Else
    (a) Display("ID already registered. Please enter a new ID")
5. End
```

Medications:

```
1. Begin
2. Medication[] ← fetch(Medication details)
3. UADDRESS ← fetch(User Address)
4. if (UADDRESS.isInsurance Company) then
    (a) Medic[] ← fetch(stored medication details)
    (b) If (Medic.Exists(Medication)) then
        i. Display("Medications not covered under insurance")
    (c) Else
```

```
            i. Display("Medication covered under insurance")
5. Else
    (a) Display("Only insurance company can do this operation")
6. End
```

5.5.4 Algorithm for claim for insurance

This function takes in input of patient's aadhar card number. It checks whether the entered aadhar number has already claimed for insurance or not.

```
1. Begin
2. Medication[] ← fetch(Medication details)
3. UADDRESS ← fetch(User Address)
4. if (UADDRESS.isInsuranceCompany) then
    (a) Medic[] ← fetch(stored medication details)
    (b) If (Medic.Exists(Medication)) then
            i. Display("Medications not covered under insurance")
    (c) Else
            i. Display("Medication covered under insurance")
5. Else
    (a) Display("Only insurance company can do this operation")
6. End
```

5.5.5 Algorithm for Doctor

This contract takes care of all the operations performed by the doctor. First a doctor has to register himself with the system in order to perform any operation. The doctor requests permissions for accessing the patient's medical data. After receiving the required permissions, the doctor creates a treatment id for the pa- tient, treats him and then uploads the prescription & the bill to the blockchain. He also sends a copy of the medication details that are not covered in insurance company's details to the insurance company for addition.

```
1. Start
2. get(user details)
   userDetails[]
3. User Address (UADDRESS) ←− fetch
4. Display "user already registered" if (UADDRESS.isAlreadyRegistered)
5. Other
6. Register doctor details to the blockchain
7. End
```

5.5.6 Algorithm for accessing the Patients data for treatment

This function reads the patient's aadhar card number. It creates an OTP for the entered aadhar card number, using which doctor can access the patient's medical records.

```
1. Begin
2. Paadhar ←− fetch(Aadhar details of the patient)
3. UADDRESS ←− fetch(User Address)
```

```
4. If (UADDRESS.isDoctor) then
    (a) OTP ← keccak256(Paadhar)
    (b) Update OTP to blockchain
5. Else
    (a) Display("Only doctor can get access permissions to patient")
6. End
```

5.5.7 Algorithm for treatment and insurance

```
1. Begin
2. UADDRESS ← fetch(User Address)
3. If (UADDRESS.isDoctor) then
    (a) Tid ← (142317 × Paadhar) mod 1000003
4. Else
    (a) Display("Only doctor can create a treatment id")
5. End
```

5.5.8 Algorithm for treating a patient:

This function takes in input of patient’s aadhar card number. It checks whether the entered aadhar number has already claimed for insurance or not.

```
1. Start
2. User Address (UADDRESS) → fetch
3. Then, if (UADDRESS.isDoctor)
    (a) PatientDetails[] ← fetch(stored patients details)
```

```
   (b) If (PatientDetails.Exists) then
         i. Prescription $\longleftarrow$ Create(prescription, bill)
        ii. PatientDetails.add(Prescription)
       iii. Display("Prescription and bill updated to patient")
        iv. Update blockchain
   (c) Else
         i. Display("Register the patient first")
4. Else
   (a) Display("Only doctor can treat a patient")
5. End
```

The following modules make up the MPS (multiple computation scheme) Contract, and the following is a detailed description of each module’s functions:

1. Register: To become an MPS node, a participant must first register once this is done will the participant be eligible services in exchange for money.

2. Reputation System: According to this contract, every MPS node has a reputation value. The reputation value of the MPS node will rise if it cooperates and does the calculation work successfully; if not, it will fall. The MPS nodes’ long-term usefulness is determined by their reputation value.

3. Incentive Mechanism: The MPS node receives revenue from two sources: the price charged to users who use the service, and the penalty imposed on dishonest MPS nodes. The allocation of rewards after the completion of each service is a reflection of the real usefulness of MPS nodes, as determined by the Incentive Mechanism.

4. Choose Quorum: In order to complete the present calculation work, users may choose. A low reputation does not guarantee selection, but the likelihood will drop very rapidly as the reputation value drops. The poor players

should be given another opportunity to make up for their previous actions. We must also take a newbie into account. This is in line with what is really true.

5.5.9 Compute contract

Users that need the multi-party computing service negotiate and implement Compute Contracts into the BN. The Compute Contract contains information about the MPS settings for the present calculation work. The accuracy of the given data will be confirmed by the smart contract. The smart contract will also determine which member failed to provide the right message at the start of the next round. The blockchain will then decide whether or not the computation may continue. This time restriction may represent the future height of a certain block. To get a quorum of MPS nodes taking part in the present calculation work, it will submit a transaction to MPS Contract in the first phase.

5.5.10 MPS protocol

We may make use of some research on contracts in this section [118] [119]. Our primary concerns in this research are MPS robustness and fairness. It is beyond the purview of this study to discuss how to build a secure MPS protocol using contracts. The parties calculate hidden shares of the function f's outputs or a pointless intermediate value, as stated in [101] . Thus, upon the completion of each round in the blockchain. The blockchain platform's Smart Contract automatically executes rewards or punishments. At the conclusion of every cycle, what the Users and MPS nodes must do.

5.5.11 Fairness robustness analysis

Bitcoin and (t, n)-threshold contracts form the foundation of BSMPCS, which operates in rounds. Time stamps on a blockchain may make it possible for protocols to run synchronously. The Smart Contract will identify and eliminate any player who sends an improper message outside of the protocol at the start of the next round. All of this operates automatically in a blockchain context and is visible to the public. This is not feasible in earlier work when there isn't a centralized node. On the blockchain, every member has a unique account and matching key pairs, making identity theft impossible. The following features primarily demonstrate BSMPCS robustness:

Setup Phase: Each participant's reputation value is publicly maintained by the ledger based on their previous actions. To make selection easier, individuals must build up their reputation values over an extended period of time. In order to prevent ”The Sybil Attack,” a deposit is required in the contract in order to become an MPS node. In other words, the attacker cannot add additional nodes to break the protocol. The phase may be repeated and a new subset can be chosen to begin with if the procedure is aborted.

Phase of Input: When submitting the input, users must charge for the current job. The accuracy of the user's input will. The service fee will be charged to the truthful Users if they fail to provide the accurate input within the allotted period. The service price will allow the programme to withstand denial-of-service assaults from users.

Compute Phase: The Smart Contract also detects the MPS node's intermediate value.

In conclusion, the Smart Contract will identify any BSMPCS participant who violates the protocol and will prevent them from taking part in the subsequent task. The plan makes use of a (t, n)-threshold secret share, which provides some fault tolerance as long as an appropriate t is specified. Users may choose a new subset to resume the agreement even in the event that the protocol is terminated. As a result, BSMPCS is resilient.

5.6 Experiment Evaluation

All things considered, there are six parts to the implementation: IPFS Storage, the insurance company, the pharmacist, the BN, the patient, and the doctor. A

Java prototype has been constructed using Geth, which is used to build BT. The source code for both programs is freely accessible online. Due to the need for on-chain storage space in the blockchain, the CID value (hash value) is kept in the blockchain after being extracted from IPFS version 4, and all of the reports are recorded in IPFS version 4. A network has been established up using IPFS version 4. The computers include Intel Core i5 7th Gen processors with (i) 8 GB RAM and 500 GB local storage based on Windows x64, and (ii) 6 GB RAM and 500 GB local storage based on Ubuntu 16 processors.

It is a well-known fact that the average block creation time of the chosen blockchain determines the computational efficiency of all blockchain-based schemes. For instance, a Bitcoin transaction typically takes ten minutes to execute. The EOS blockchain platform is selected by BSMPCS. BFTDPoS, the current EOS consensus process, can reliably produce a block every 0.5 seconds. All MPC Con- tract and Compute Contract activities in BSMPCS are carried out on a chain.
The primary time burden associated with off-chain execution in each round is the PVSS data distribution procedure, which involves sharing the Shamir's secret and carrying out several asymmetric encryption operations. For MPC nodes that choose to take part in the present compute work during the Compute Contract Init phase, their execution duration is mostly determined by the size of the quorum.

We may deduce that, for a given set of MPC nodes in Compute Contract, the cost of time for a BSMPCS round grows exponentially as the size of the quorum rises. This is so that additional asymmetric encryption computations may be performed during each round of computation as MPC nodes are added to a particular workload. Worse, in order to enable secret sharing, a higher power polynomial is required, which means that more bytes are used in the created shares, increasing the size and time required for the asymmetric encryption of the data. We may see that users choosing more MPC nodes to complete a compute work for greater privacy would result in a significant loss of efficiency when the quorum surpasses 40. This module is in charge of compiling their medical records and forwarding them

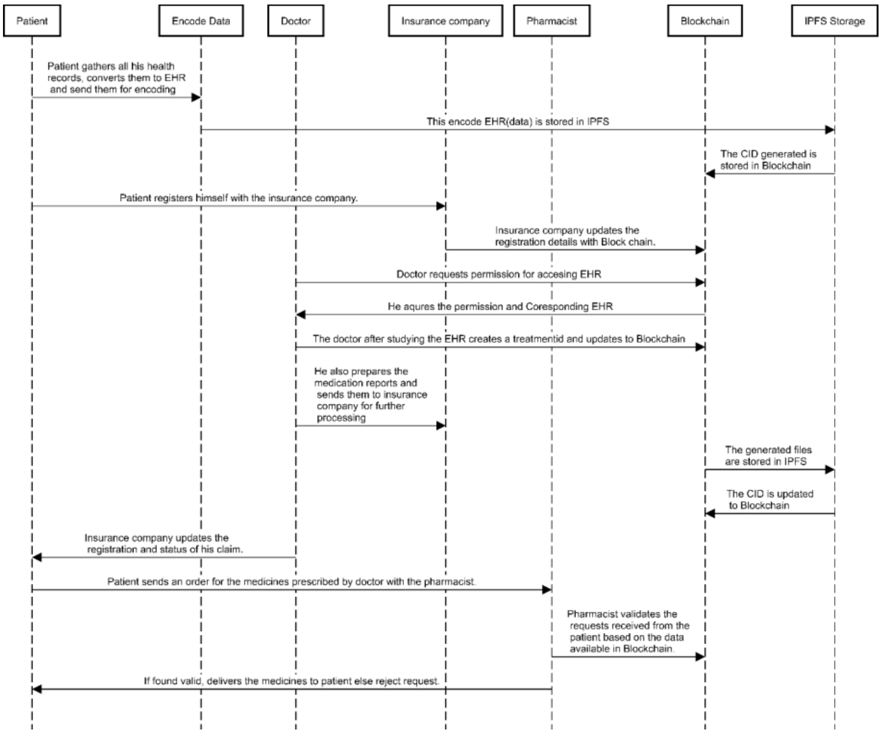

Patient
Encode Data
Doctor
Insurance company
Pharmacist
Blockchain
IPFS Storage
Patient gathers all his health records, converts them to EHR and send them for encoding
This encode EHR(data) is stored in IPFS
The CID generated is stored in Blockchain
Patient registers himself with the insurance company.
Insurance company updates the registration details with Block chain.
Doctor requests permission for accesing EHR
He aqures the permission and Coresponding EHR
The doctor after studying the EHR creates a treatmentid and updates to Blockchain
He also prepares the medication reports and sends them to insurance company for further processing
The generated files are stored in IPFS
The CID is updated to Blockchain
Insurance company updates the registration and status of his claim.
Patient sends an order for the medicines prescribed by doctor with the pharmacist.
Pharmacist validates the requests received from the patient based on the data available in Blockchain.
If found valid, delivers the medicines to patient else reject request.

Figure 5.4: Sequence diagram for EHR report in Healthcare System

to the data encoder so that the plain text may be changed to encoded language. These files will eventually be updated to the blockchain and transferred to the IPFS storage system. The upload and download times for various sizes are shown in Fig. 5. The graphs show that the computational cost of uploading a transaction is higher than that of downloading it.

Doctor: When a patient registers with the system, the request is sent to a related doctor. To access the data, he obtains authorization from the BN. In addition, he generates a treatment ID for the ongoing procedure. In addition to recommending certain medications and testing, the doctor uploads the information to the blockchain.

Insurance Company: The patients, hospital, and BN are all covered in this module. Depending on the kind of issue and emergency found, the patients register with the insurance provider. The hospital and the doctor confirm the information with the insurance company. If the request is determined to be legitimate, the patient's claim is rejected; otherwise, the information is processed and money is awarded to the patient.

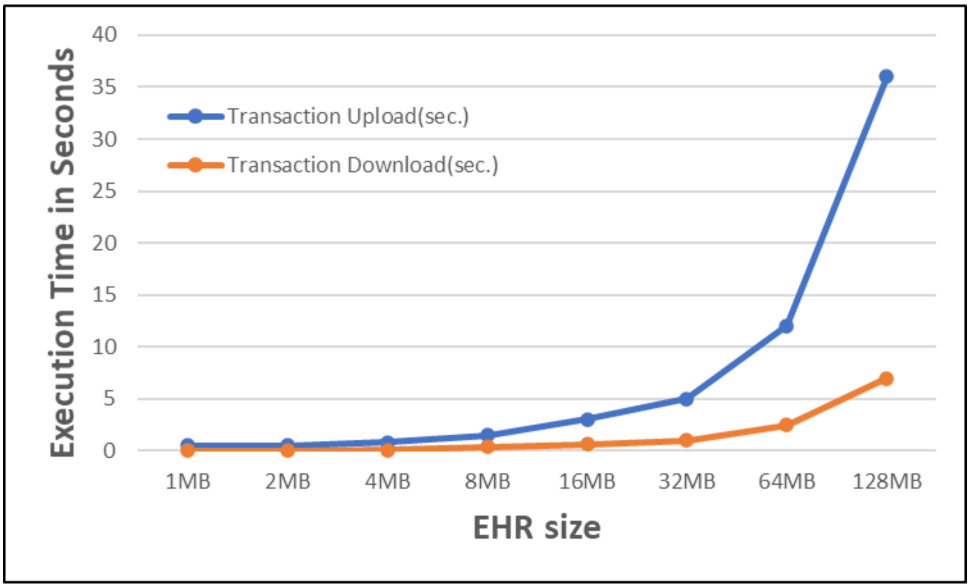


Figure 5.5: Transaction upload and download execution time

Pharmacist: Patients may place online orders for medications from the pharmacy after obtaining prescriptions from their doctors. The blockchain will be updated with the same.

IPFS Storage: The peers in the network store all of the reports in IPFS. Every file has a Content Identifier created for it when the reports are uploaded. This serves as a point of reference for network file access. In the blockchain, this produced Content Identifier value will be kept.

BN: To verify transactions submitted by different participating entities and to construct a block, this module really implements the consensus procedures. A number of blocks containing the data from the participating entities—such as patient and doctor IDs, treatment IDs, insurance company details, etc.—will be formed during the mining process. The observation is that the mining process takes longer than the block creation process. This may be seen in fig. 6.

Fig. 5.7 ,shows the time it takes peers to access (availability) a transaction for a range of report sizes. It seems sense that the access time would rise as the report's size rose. Furthermore, a transaction takes longer to complete the more peers participate.

Comparing the performance of the proposed framework with seven other existing

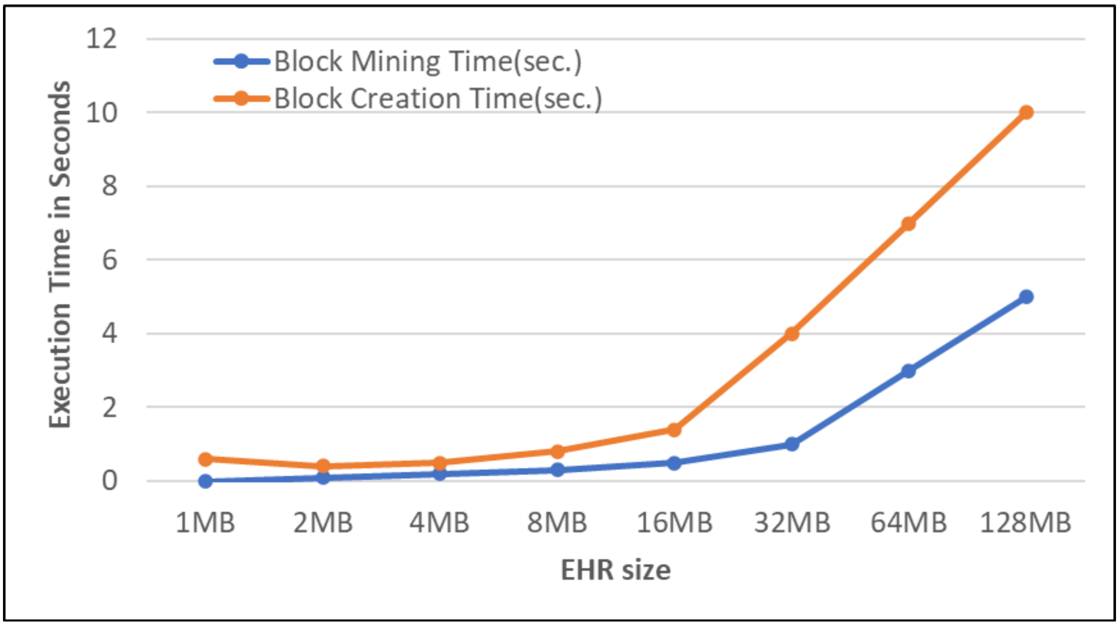


Figure 5.6: Execution time for block mining and block creation

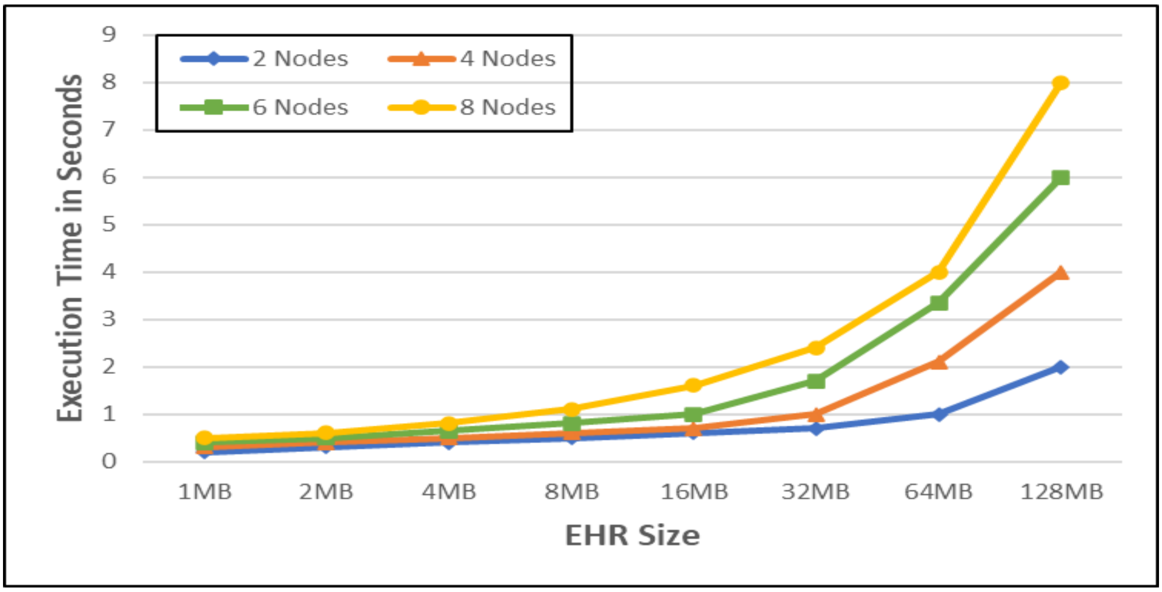


Figure 5.7: Running time for transaction access by number of nodes

schemes for protecting the privacy of Health Record Information systems is the focus of this section. The schemes include [103] [98] [99] [100] [104] [105] [120] .Seven benchmark privacy and security attributes are taken into consideration in our suggested framework, as shown in the table.

The chart indicates that our suggested architecture has succeeded in achieving both security and privacy features. Notably, our suggested architecture offers the best means of protecting patient privacy and HER security in terms of tamper- proofing, data privacy protection, patient privacy preservation, access control, non-repudiation, access revocation, and block search.

Table 5.1: Metrics

	Metrics	[J]	[F]	[G]	[K]	[L]	[M]	[N]	Proposed Scheme
1	Tamper – Proof	√	√	√	√	√	√	√	√
2	Privacy Preserving of Patient		√		√				√
3	Data Privacy(Confidentiality)		√						√
4	Access Control	√				√	√	√	√
5	Non – RepudiaTion	√	√	√	√	√	√	√	√
6	Access Revocation					√		√	√
7	Block Search	√			√	√	√	√	√

5.6.1 Evaluation

If Patients EHRs are securely and safely maintained by this application. It includes modules for every aspect of an electronic health care system, including those for physicians, patients, the research team, hospitals, and insurance providers. Ensuring the privacy of data collected and kept in the EHR system is the primary goal of this system. Additionally, the EHR Privacy Model in Blockchain is focused on avoiding data tampering, unauthorised change, and general support for an online electronic health care system. This system uses homomorphic encryption and a novel technology known as BT to provide data security and privacy. The smart contracts handle granting permission for data access, other modules,

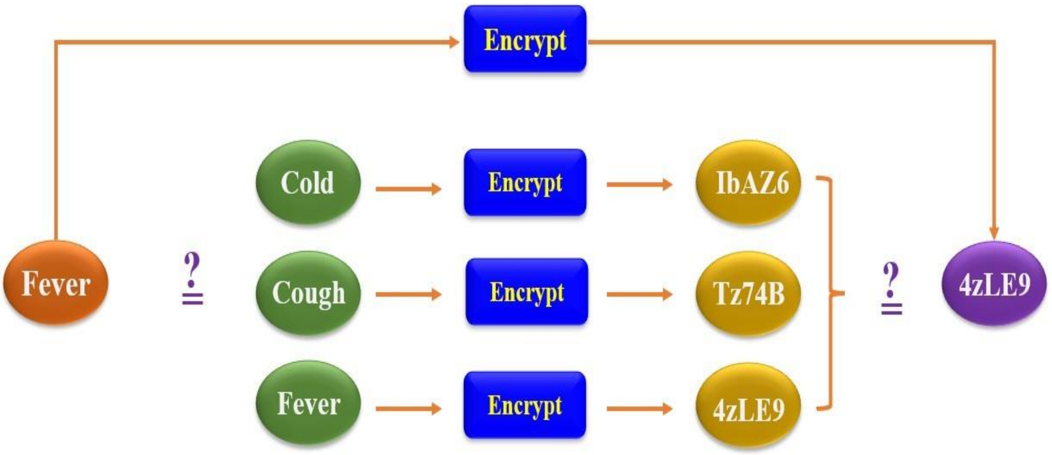
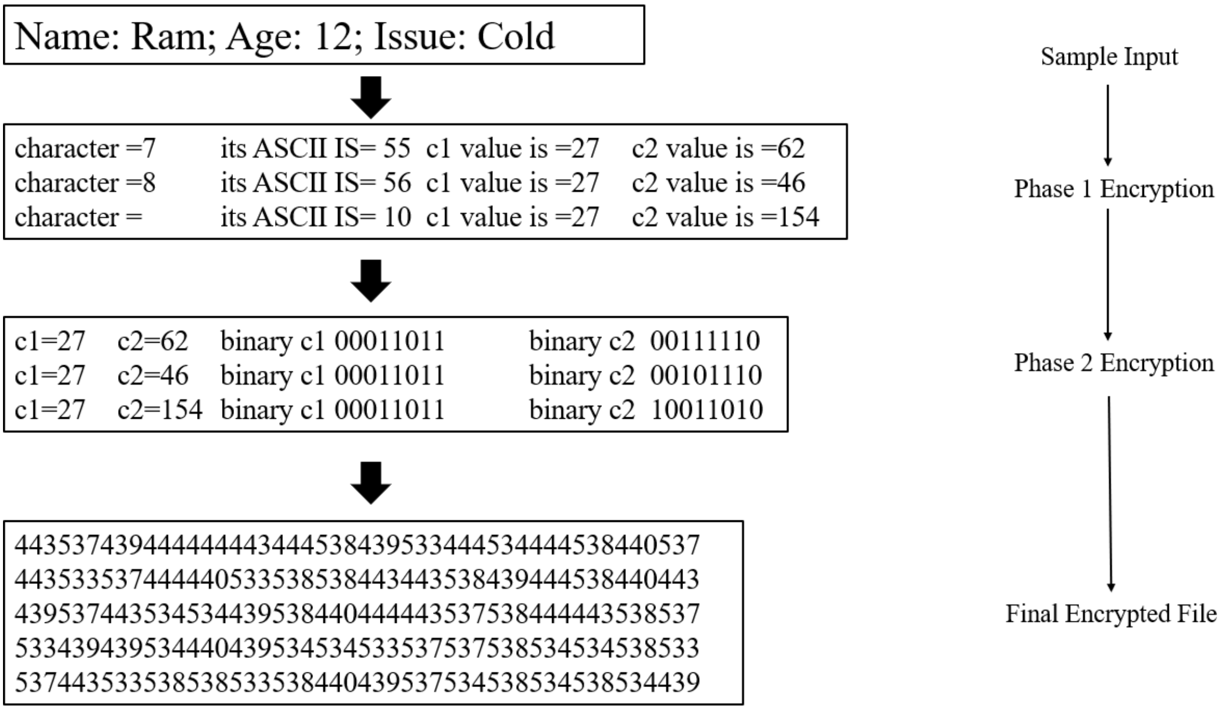


Figure 5.8: Working mechanism of Homomorphic Encryption

and collaborating entities.
A prototype of the intended system was put into place in order to assess the system’s functionality and the degree of privacy and security achieved for the data kept therein. We used the Ethereum blockchain platform, go-ethereum, version 7.5.4 of npm, and node version 15.8.0 to implement the prototype. Versions 5.1.66 and 6.12.2 of the Solidity Framework and IDE are used to deploy smart contracts, respectively, while version 0.8.1 of the Solidity scripting language is used to develop the contracts. The version of web3js that.

handles queries between Ethereum [2] nodes is v1.2.0.Six workstations were used to install the blockchain node each has an Intel CPU with a 2.30GHz core and 8 GB of main memory. A few nodes were set up in different settings, such as Windows 10 and Ubuntu 16. Version 13.2 of Java is utilised to implement the encryption and decryption modules of the HME process in the EHR-PP paradigm, and Notepad++ is the editor of choice.On receiving the search word ”Fever” the HME algorithm performs encryption and generates the code”4zLE9”.Now this encrypted keyword is searched and matched with the values that are already encrypted and stored in the database.



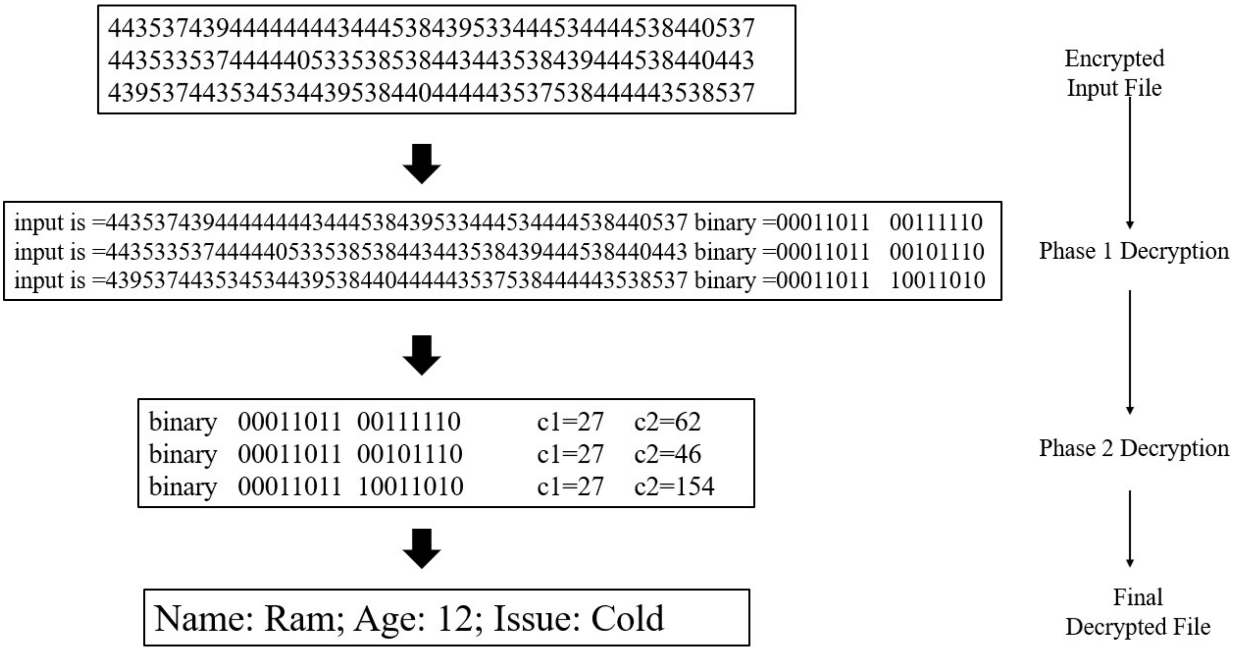
```
Name: Ram; Age: 12; Issue: Cold
```

```
character =7     its ASCII IS= 55  c1 value is =27   c2 value is =62
character =8     its ASCII IS= 56  c1 value is =27   c2 value is =46
character =      its ASCII IS= 10  c1 value is =27   c2 value is =154
```

```
c1=27   c2=62    binary c1 00011011       binary c2  00111110
c1=27   c2=46    binary c1 00011011       binary c2  00101110
c1=27   c2=154   binary c1 00011011       binary c2  10011010
```

```
4435374394444444443444538439533444534444538440537
4435335374444405335385384434435384394445384404443
4395374435345344395384404444435375384444443538537
5334394395344404395345345335375375385345345538533
5374435335385385335384404395375345385345538534439
```

Figure 5.9: Encryption process in ElGamal encryption algorithm



```
4435374394444444443444538439533444534444538440537
4435335374444405335385384434435384394445384404443
4395374435345344395384404444435375384444443538537
```

```
input is =4435374394444444443444538439533444534444538440537 binary =00011011   00111110
input is =4435335374444405335385384434435384394445384404443 binary =00011011   00101110
input is =4395374435345344395384404444435375384444443538537 binary =00011011   10011010
```

```
binary   00011011  00111110         c1=27    c2=62
binary   00011011  00101110         c1=27    c2=46
binary   00011011  10011010         c1=27    c2=154
```

```
Name: Ram; Age: 12; Issue: Cold
```

Figure 5.10: Decryption process in ElGamal decryption algorithm

Table 5.2: Transaction and execution cost

S.No	Operation Performed	Transaction cost		Execution-cost		Total cost (in ether)
		In gas units	In ethers	In gas units	In ethers	
1.	Contract Deployment	1955973	0.2621004	1444301	0.1935363	0.4556367
2.	Addchemist	166589	0.0223229	142821	0.019138	0.0414609
3.	Adddoctor	207754	0.027839	182834	0.0244998	0.0523388
4.	Addinsurance Company	126755	0.0169852	104651	0.0140232	0.0310084
5.	Addpatient	208706	0.0279666	184170	0.0246788	0.0526454
6.	Getpatient Information	29325	0.0039296	7797	0.0010448	0.0049744
7.	UpdatePrecautions	44111	0.0059109	21367	0.0028632	0.0087741
8.	Getchemist	25707	0.0034447	4243	0.0005686	0.0040133
9.	Getinsurance Company	26489	0.0035495	5089	0.0006819	0.0042314
10.	AddMedications notcoveredininsurance	65770	0.0088132	44114	0.0059113	0.0147245
11.	CreateTreatmentd	21857	0.0029288	329	0.0000441	0.0029729
12.	TreatPatient	189040	0.0253314	165144	0.0221293	0.0474607
13.	Gettreatment Details	27482	0.0036826	5890	0.0007893	0.0044719
14.	Medication Includedininsurance	53756	0.0072033	31780	0.0042585	0.0114618
15.	Getdoctordetails	24375	0.0032663	2911	0.0003901	0.0036564

Because this experiment involves the deployment or execution of a smart contract, its complexity is measured in terms of gas. The costs associated with each proce- dure carried out in the experiment are shown in Table 1. Gwei metrics are used. Total cost is equal to the number of gas units used times the cost per gas unit. To execute the framework, all of the activities in rows 1, 2, 3, 5, 7, 10, 11, 12, 14, and 16 must be completed. Therefore, 0.7274322 ethers are needed to execute this framework overall.

Performance comparison Analysis: In this section, we address the performance assessment of proposed framework with other existing schemes related to privacy preserving of Health Record Information system schemes.

Table 5.3: Performance comparision analysis

Reference	Access Controll	Access Revocation	Privacy Preserving	Access to Patients	Predictive Model	Decision Making
Al-Sumaidaee et al. (2023)	Yes	Yes	No	No	NO	Yes
Egala et al. (2023)	Yes	No	No	Yes	No	No
Abou El Houda et al. (2022)	Yes	No	Yes	Yes	No	No
Proposed Model	Yes	Yes	Yes	Yes	Yes	Yes

5.7 Summary

MPC scheme to address the needs of robustness and fairness in multi-party computing. The suggested approach maintains a public reputation system in which probability of being chosen. The significance of electronic health information in terms of numerous security and privacy issues is covered in this study. After meticulously noting a number of issues, we established a novel architecture to protect and preserve the confidentiality of healthcare data. This is why data is sent and stored in an encrypted manner. With this innovative kind of encryption, users may safely work with encrypted text, ensuring that their data remains private. Consequently, it also reduced the time required to finish several encryption and decryption procedures for every obtained query. We also integrated it with BT to make it impenetrable. Results from our tests showed that the technology outperformed more traditional forms of encryption and storage. The Smart Contract needs to check the values of the intermediate and final stages of each cycle. When the timer goes off, the smart contract will know that either a message was sent or none was sent. Furthermore, an incentive structure promotes teamwork by all parties involved; those who are truthful will gain more and more, while those who are dishonest will suffer more severe repercussions. Concerns about privacy stem from the fact that blockchain maintains an immutable public record; MPC was developed to tackle this very problem. In future studies, we will look at the potential privacy protection advantages that MPC offers blockchain.

Chapter 6

CONCLUSION AND FUTURE SCOPE

6.1 Conclusion

Bitcoin provides a sophisticated method for storing medical data, executing medical transactions, and fostering trust in the integration and interchange of medical information within a decentralized global healthcare network. The healthcare sector has demonstrated considerable interest in Bitcoin yet, privacy and security issues persist as the primary points of contention about its application for medical data exchange. This article examines a study on the privacy and security of BT within the healthcare sector, spanning the years 2017 to 2023. This critical review evaluates the present situation by analyzing the existing body of research, with particular emphasis on studies that investigate challenges and practical applications. This study offers significant insights into potential future research avenues and advancements through a rigorous assessment. The findings indicate that blockchain is employed to develop advanced and innovative therapies that enhance the standard methods for managing, transferring. Blockchain utilization in the healthcare sector is fundamentally advancing, significantly enhancing data management process security, efficiency, access control, technical innovation, and privacy protection. The results also imply that the majority of the present limits are related to the model's functionality, as well as the expenses and restrictions that come with putting it into practice. A comprehensive framework is shown to encompass potential domains, including regulatory compliance, system design, and data security, where future scholars may make significant contributions. Last but not least, the Systematic Literature Review indicates that more study may make it easier for blockchain applications to be widely used to solve important problems in medical diagnosis, legal compliance, fraud prevention, and the enhancement of patient care in emergency situations or during remote monitoring.

FHE is used by the Machine Learning Privacy-Preserving Model (MLPPM) to protect data security and privacy during machine learning activities. Completely homomorphic encryption maintains secrecy by enabling calculations on encrypted material without the need to decode it. This study focuses on advancing MLPPM models by utilizing the Cheon-Kim-Kim-Song-Residue-Number-System (CKKS-RNS) FHE scheme and bootstrapping to address the limitations of traditional FHE methods. Existing models like CryptoNet, SEALion, and CryptoDL primarily cater to basic or nonstandard machine learning models and have demonstrated limited effectiveness with more sophisticated datasets. These methods typically replace non-arithmetic activation functions with approximations before bootstrapping, restricting the model's depth and complexity. By integrating CKKS-RNS and employing advanced approximation techniques for non-arithmetic functions such as ReLU and Softmax, this study presents a robust approach for deep learn- ing on encrypted data. Our model, based on ResNet-50, was validated using the MNIST dataset and demonstrated high accuracy and performance. The proposed MLPPM model achieved a classification accuracy of 92.43% ± 2.65%, closely aligning with the original ResNet-50 model's accuracy of 91.89%. Inference was performed in 20 minutes on a dual Intel Core i7 CPU with 8 GB RAM, showcasing the feasibility of applying FHE to complex machine learning models.

Privacy protection for EHRs is becoming an issue that the general public is becoming more and more interested in. The increasing use of virtual currencies like bitcoin has led to the development of BT, which possesses the qualities of ”decentralization” and ”immutability”. Current EHR management systems prioritize safeguarding user privacy information above the security risks that occur when patients engage with several roles. As of right now, there is no sufficient solution to the problem of insurance companies accessing confidential patient information and violating their privacy. As the number of reported data breaches that threaten the current system rises, users' privacy is called into question because of personal data that third parties manage and obtain in large amounts. This study offers a block chain-based solution to all of the aforementioned problems.The paper proposes a blockchain-based framework to address privacy concerns in electronic health record systems. It specifically applies the decentralized, immutable qualities of blockchain to secure data against unauthorized access. The use of smart contracts for EHR management is relatively novel, as it allows interactions with insurance companies without exposing sensitive data. This contribution should highlight why smart contracts are better suited for this use case compared to existing mechanisms. The application of homomorphic encryption ensures that the system can process encrypted data without decrypting it. This allows computations (such as insurance claim verifications) to be performed on encrypted data, preserving privacy. The BSMPCS system is a new framework that could potentially combine these technologies into a unified solution. The paper should emphasize how this is different from existing EHR management systems and what makes it more secure and privacy-preserving.Using Bitcoin smart contract technology and homomorphic encryption, we create the feature with BSMPCS that allows the insurance company to decide whether to execute insurance requests even in the absence of a way to get the ID and the plain text of the EHR. As a consequence, during communication, no private patient information would be revealed to uninvited parties, improving user data privacy and security.

6.2 Future Scope

Blockchain-inspired privacy-preserving and auditable EHR models could improve healthcare data management. Healthcare systems generate massive volumes of numerical, classified, and unstructured data like photos, videos, and audio. Privacy and the integrity of multidimensional data are essential. Decentralization, immutability, and transparency make blockchain technology a possible solution. Healthcare organizations need customized solutions to improve blockchain-based EHR security, efficiency, and accessibility. Advanced anonymization and cryptography to secure healthcare data across formats are significant future goals. This connection would protect data privacy and meet strict legal standards. AI-driven methods can automate quasi-identifier identification in healthcare datasets. This breakthrough would make privacy protection frameworks more scalable and precise, especially for high-dimensional and sensitive datasets, by eliminating manual intervention. AI and blockchain can improve healthcare data management security and efficiency to fulfill modern healthcare ecosystem needs Healthcare blockchain adoption presents particular problems, such as limited storage capacity, the necessity for privacy-preserving techniques for on-chain data, and the complexity of implementing revocable access control. To maximize blockchain technology for EHR systems, these issues must be addressed. This paper presents a blockchain-inspired access control mechanism using private blockchain technology and cryptographic primitives to overcome these challenges. This technique addresses major challenges while keeping the model realistic, secure, and auditable. Tamper-resistant storage and revocable access control make electronic health record management secure and efficient. The model's privacy and security are tested against tampering, collusion, replay attacks, and malicious access attempts to prove its resilience. These studies verify the system meets healthcare application qualitative and functional requirements. Performance comparisons with existing healthcare data management solutions show blockchain-based solutions' efficiency and scalability, indicating their real-world potential. This research develops a blockchain-inspired, privacy-preserving, auditable EHR framework. The concept addresses present constraints and anticipates future issues, ushering in an exciting era in healthcare data management. This framework protects sensitive patient data and ensures stakeholder confidence, transparency, and auditability. Future blockchain research in other healthcare fields could lead to revolutionary electronic health record management solutions that prioritize privacy, security, and efficiency. In future,it is intended to extend the research work for multiple sensitive attributes and high-dimensional data. Nowadays, healthcare data not only consists of numerical and categorical attributes but consists of image, video, and audio kind of data. Privacy preserving approaches to protect such data should be identified. Anonymization approaches can be merged with crypto graphical approaches to protect healthcare data of different formats. An AI based model can be proposed to identify the quasi attributes of healthcare data without human intervention.

References

[1] H. O. Alanazi, A. Zaidan, B. Zaidan, M. M. Kiah, and S. Al-Bakri, "Meeting the security requirements of electronic medical records in the era of high- speed computing," *Journal of medical systems*, vol. 39, pp. 1–13, 2015.

[2] E. Ahmed, R. A. El Khoribi, G. Darwish, A. Muzy, and G. Bernot, "Modeling of the development of the fetus cognitive map from the sensorimotor system," *Egyptian Informatics Journal*, vol. 21, no. 4, pp. 191–199, 2020.

[3] E. Lee, S. Han, and S. H. Jo, "Consumer choice of on-demand mhealth app services: Context and contents values using structural equation modeling," *International journal of medical informatics*, vol. 97, pp. 229–238, 2017.

[4] E. K. Achampong, "Electronic health record (ehr) and cloud security: the current issues," *International Journal of Cloud Computing and Services Science*, vol. 2, no. 6, p. 417, 2013.

[5] P. Matsudaira, "High-end biological imaging generates very large 3d+ and dynamic datasets," *Proceedings of the VLDB Endowment*, vol. 3, no. 1-2, pp. 3–3, 2010.

[6] T. Dehling and A. Sunyaev, "Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the german nationwide health information technology infrastructure," *Electronic Markets*, vol. 24, pp. 89–99, 2014.

[7] O. Dorgham, B. Al-Rahamneh, A. Almomani, K. F. Khatatneh *et al.*, "Enhancing the security of exchanging and storing dicom medical images on the

cloud," *International Journal of Cloud Applications and Computing (IJ-CAC)*, vol. 8, no. 1, pp. 154–172, 2018.

[8] T. K. Teoh and M. M. Hannan, "Ventricular assist device–associated infection," *Infectious Disease Clinics*, vol. 32, no. 4, pp. 827–841, 2018.

[9] E. Urtnasan, J.-U. Park, E.-Y. Joo, and K.-J. Lee, "Automated detection of obstructive sleep apnea events from a single-lead electrocardiogram using a convolutional neural network," *Journal of medical systems*, vol. 42, pp. 1–8, 2018.

[10] M. Christodorescu, R. Sailer, D. L. Schales, D. Sgandurra, and D. Zamboni, "Cloud security is not (just) virtualization security: a short paper," in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 97–102.

[11] J. Lemke, "Storage and security of personal health information," *OOHNA J*, vol. 32, no. 1, pp. 25–26, 2013.

[12] C.-L. Chen, P.-T. Huang, Y.-Y. Deng, H.-C. Chen, and Y.-C. Wang, "A secure electronic medical record authorization system for smart device ap- plication in cloud computing environments," *Human-centric Computing and Information Sciences*, vol. 10, pp. 1–31, 2020.

[13] C. S. Kruse, B. Smith, H. Vanderlinden, and A. Nealand, "Security tech- niques for the electronic health records," *Journal of medical systems*, vol. 41, pp. 1–9, 2017.

[14] S. Kaushik, "Blockchain and 5g-enabled internet of things: Background and preliminaries," *Blockchain for 5G-Enabled IoT: The new wave for Industrial Automation*, pp. 3–31, 2021.

[15] V. Liu, M. A. Musen, and T. Chou, "Data breaches of protected health information in the united states," *Jama*, vol. 313, no. 14, pp. 1471–1473, 2015.

[16] J. S. Ancker, M. Silver, M. C. Miller, and R. Kaushal, “Consumer experi- ence with and attitudes toward health information technology: a nationwide survey,” *Journal of the American Medical Informatics Association*, vol. 20, no. 1, pp. 152–156, 2013.

[17] R. Collier, “Us health information breaches up 137%,” 2014.

[18] R. Haque, H. Sarwar, S. R. Kabir, R. Forhat, M. J. Sadeq, M. Akhtaruzzaman, and N. Haque, “Blockchain-based information security of electronic medical records (emr) in a healthcare communication system,” in *Intelligent Computing and Innovation on Data Science: Proceedings of ICTIDS 2019*. Springer, 2021, pp. 641–650.

[19] K. Hameed, A. Ali, M. H. Naqvi, M. Jabbar, M. Junaid, and A. Haider, “Resource management in operating systems-a survey of scheduling algorithms,” in *Proceedings of the International Conference on Innovative Computing (ICIC), Lanzhou, China*, 2016, pp. 2–5.

[20] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, “A decentralized privacy-preserving healthcare blockchain for iot,” *Sensors*, vol. 19, no. 2, p. 326, 2019.

[21] E.-Y. Daraghmi, Y.-A. Daraghmi, and S.-M. Yuan, “Medchain: A design of blockchain-based system for medical records access and permissions management,” *IEEE access*, vol. 7, pp. 164 595–164 613, 2019.

[22] C. W. Choo, *Information management for the intelligent organization: the art of scanning the environment*. Information Today, Inc., 2002.

[23] L. Hang and D.-H. Kim, “Design and implementation of an integrated iot blockchain platform for sensing data integrity,” *sensors*, vol. 19, no. 10, p. 2228, 2019.

[24] B. Yu, S. K. Kermanshahi, A. Sakzad, and S. Nepal, “Chameleon hash time-lock contract for privacy preserving payment channel networks,” in

Provable Security: 13th International Conference, ProvSec 2019, Cairns, QLD, Australia, October 1–4, 2019, Proceedings 13. Springer, 2019, pp. 303–318.

[25] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" *IEEE cloud computing*, vol. 5, no. 1, pp. 31–37, 2018.

[26] S. Kasra Kermanshahi, J. K. Liu, and R. Steinfeld, "Multi-user cloud-based secure keyword search," in *Australasian conference on information security and privacy*. Springer, 2017, pp. 227–247.

[27] S. Kasra Kermanshahi, J. K. Liu, R. Steinfeld, and S. Nepal, "Generic multi-keyword ranked search on encrypted cloud data," in *Computer Security–ESORICS 2019: 24th European Symposium on Research in Computer Security, Luxembourg, September 23–27, 2019, Proceedings, Part II 24*. Springer, 2019, pp. 322–343.

[28] D. Li, Z. Luo, and B. Cao, "Blockchain-based federated learning methodologies in smart environments," *Cluster Computing*, vol. 25, no. 4, pp. 2585–2599, 2022.

[29] V. K. Rathi, V. Chaudhary, N. K. Rajput, B. Ahuja, A. K. Jaiswal, D. Gupta, M. Elhoseny, and M. Hammoudeh, "A blockchain-enabled multi domain edge computing orchestrator," *IEEE Internet of Things Magazine*, vol. 3, no. 2, pp. 30–36, 2020.

[30] L. Nkenyereye, B. Adhi Tama, M. K. Shahzad, and Y.-H. Choi, "Secure and blockchain-based emergency driven message protocol for 5g enabled vehicular edge computing," *Sensors*, vol. 20, no. 1, p. 154, 2019.

[31] I. Mistry, S. Tanwar, S. Tyagi, and N. Kumar, "Blockchain for 5g-enabled iot for industrial automation: A systematic review, solutions, and challenges," *Mechanical systems and signal processing*, vol. 135, p. 106382, 2020.

[32] I. Budhiraja, S. Tyagi, S. Tanwar, N. Kumar, and M. Guizani, “Cr-noma based interference mitigation scheme for 5g femtocells users,” in *2018 IEEE Global Communications Conference (GLOBECOM)*. IEEE, 2018, pp. 1–6.

[33] P. N. Srinivasu, A. K. Bhoi, S. R. Nayak, M. R. Bhutta, and M. Woźniak, “Blockchain technology for secured healthcare data communication among the non-terminal nodes in iot architecture in 5g network,” *Electronics*, vol. 10, no. 12, p. 1437, 2021.

[34] C. Feng, K. Yu, A. K. Bashir, Y. D. Al-Otaibi, Y. Lu, S. Chen, and D. Zhang, “Efficient and secure data sharing for 5g flying drones: A blockchain-enabled approach,” *IEEE Network*, vol. 35, no. 1, pp. 130–137, 2021.

[35] K. Khujamatov, E. Reypnazarov, N. Akhmedov, and D. Khasanov, “Blockchain for 5g healthcare architecture,” in *2020 international conference on information science and communications technologies (ICISCT)*. IEEE, 2020, pp. 1–5.

[36] M. Vivekanandan, S. VN, and S. R. U, “Bidapsca5g: Blockchain based internet of things (iot) device to device authentication protocol for smart city applications using 5g technology,” *Peer-to-Peer networking and applications*, vol. 14, no. 1, pp. 403–419, 2021.

[37] J. Gao, K. O.-B. O. Agyekum, E. B. Sifah, K. N. Acheampong, Q. Xia, X. Du, M. Guizani, and H. Xia, “A blockchain-sdn-enabled internet of vehicles environment for fog computing and 5g networks,” *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 2019.

[38] S. Zhou, H. Huang, W. Chen, P. Zhou, Z. Zheng, and S. Guo, “Pirate: A blockchain-based secure framework of distributed machine learning in 5g networks,” *IEEE Network*, vol. 34, no. 6, pp. 84–91, 2020.

[39] Y. Zhang, K. Wang, H. Moustafa, S. Wang, and K. Zhang, “Guest editorial: Blockchain and ai for beyond 5g networks,” *IEEE Network*, vol. 34, no. 6, pp. 22–23, 2020.

[40] T. Allard, N. Anciaux, L. Bouganim, Y. Guo, L. Le Folgoc, B. Nguyen, P. Pucheral, I. Ray, I. Ray, and S. Yin, “Secure personal data servers: a vision paper,” *The VLDB Journal*, vol. 3, no. 1-2, pp. 25–35, 2010.

[41] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient controlled encryption: ensuring privacy of electronic medical records,” in *Proceedings of the 2009 ACM workshop on Cloud computing security*, 2009, pp. 103–114.

[42] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, “Security and privacy-preserving challenges of e-health solutions in cloud computing,” *IEEE access*, vol. 7, pp. 74 361–74 382, 2019.

[43] C. Dainton and C. H. Chu, “A review of electronic medical record keeping on mobile medical service trips in austere settings,” *International journal of medical informatics*, vol. 98, pp. 33–40, 2017.

[44] P. F. Edemekong, P. Annamaraju, and M. J. Haydel, “Health insurance portability and accountability act,” 2018.

[45] F. Gao, S. Thiebes, and A. Sunyaev, “Rethinking the meaning of cloud computing for health care: a taxonomic perspective and future research directions,” *Journal of medical Internet research*, vol. 20, no. 7, p. e10041, 2018.

[46] K. Geetha, “Impact of cloud database in medical healthcare records based on secure access,” *Int. J. Eng. Adv. Technol. Regular*, no. 8, p. 6, 2019.

[47] I. Keshta and A. Odeh, “Security and privacy of electronic health records: Concerns and challenges,” *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 177–183, 2021.

[48] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, “Ubehealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities,” *IEEE Access*, vol. 6, pp. 32 258–32 285, 2018.

[49] N. M. Deshmukh, S. Kumar, and R. Shirsath, “Secure fine-grained data access control over multiple cloud server based healthcare applications,” in *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*. IEEE, 2019, pp. 1–6.

[50] M. A. Sarwar, T. Bashir, O. Shahzad, and A. Abbas, “Cloud-based architecture to implement electronic health record (ehr) system in pakistan,” *IT Professional*, vol. 21, no. 3, pp. 49–54, 2019.

[51] S. Thavamani and M. Rajakumar, “Privacy preserving healthcare data us- ing cloud computing,” *International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075*, vol. 8, no. 10S, 2019.

[52] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, “Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control,” *Journal of medical systems*, vol. 40, pp. 1–8, 2016.

[53] Z. Xia, N. N. Xiong, A. V. Vasilakos, and X. Sun, “Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing,” *Information Sciences*, vol. 387, pp. 195–204, 2017.

[54] R. Ch, I. Batra, and A. Malik, “A novel design to minimise the energy consumption and node traversing in blockchain over cloud using ensemble cuckoo model,” *International Journal on Recent and Innovation Trends in Computing and Communication*, 2022.

[55] C. Ravikumar, I. Batra, and A. Malik, “A comparative analysis on blockchain technology considering security breeches,” in *Proceedings of Trends in Electronics and Health Informatics: TEHI 2021*. Springer, 2022, pp. 555–565.

[56] S. Paul, M. Riffat, A. Yasir, M. N. Mahim, B. Y. Sharnali, I. T. Na- heen, A. Rahman, and A. Kulkarni, “Industry 4.0 applications for medical/healthcare services,” *Journal of Sensor and Actuator Networks*, vol. 10, no. 3, p. 43, 2021.

[57] S. M. H. Bamakan, S. G. Moghaddam, and S. D. Manshadi, "Blockchain-enabled pharmaceutical cold chain: Applications, key challenges, and future trends," *Journal of Cleaner Production*, vol. 302, p. 127021, 2021.

[58] J. Fan and F. Vercauteren, "Somewhat practical fully homomorphic encryption," *Cryptology ePrint Archive*, 2012.

[59] J. H. Cheon, A. Kim, M. Kim, and Y. Song, "Homomorphic encryp- tion for arithmetic of approximate numbers," in *Advances in Cryptology–ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I 23*. Springer, 2017, pp. 409–437.

[60] L. Soltanisehat, R. Alizadeh, H. Hao, and K.-K. R. Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review," *IEEE Transactions on Engineering Management*, vol. 70, no. 1, pp. 353–368, 2020.

[61] A. Saha, R. Amin, S. Kunal, S. Vollala, and S. K. Dwivedi, "Review on "blockchain technology based medical healthcare system with privacy issues"," *Security and Privacy*, vol. 2, no. 5, p. e83, 2019.

[62] F. Bourse, M. Minelli, M. Minihold, and P. Paillier, "Fast homomorphic evaluation of deep discretized neural networks," in *Advances in Cryptology–CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III 38*. Springer, 2018, pp. 483–512.

[63] J. H. Cheon, K. Han, A. Kim, M. Kim, and Y. Song, "A full rns variant of approximate homomorphic encryption," in *Selected Areas in Cryptography–SAC 2018: 25th International Conference, Calgary, AB, Canada, August 15–17, 2018, Revised Selected Papers 25*. Springer, 2019, pp. 347–368.

[64] C. Gentry, “Fully homomorphic encryption using ideal lattices,” in *Proceed- ings of the forty-first annual ACM symposium on Theory of computing*, 2009, pp. 169–178.

[65] J. H. Cheon, K. Han, A. Kim, M. Kim, and Y. Song, “Bootstrapping for approximate homomorphic encryption,” in *Advances in Cryptology–EUROCRYPT 2018: 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29-May 3, 2018 Proceedings, Part I 37*. Springer, 2018, pp. 360–384.

[66] H. Jin, Y. Luo, P. Li, and J. Mathew, “A review of secure and privacy-preserving medical data sharing,” *IEEE access*, vol. 7, pp. 61 656–61 669, 2019.

[67] J. Lee, E. Lee, J.-W. Lee, Y. Kim, Y.-S. Kim, and J.-S. No, “Precise approximation of convolutional neural networks for homomorphically encrypted data,” *IEEE Access*, vol. 11, pp. 62 062–62 076, 2023.

[68] Q. Lou and L. Jiang, “She: A fast and accurate deep neural network for encrypted data,” *Advances in neural information processing systems*, vol. 32, 2019.

[69] W. Jung, S. Kim, J. H. Ahn, J. H. Cheon, and Y. Lee, “Over 100x faster bootstrapping in fully homomorphic encryption through memory-centric optimization with gpus,” *IACR Transactions on Cryptographic Hardware and Embedded Systems*, pp. 114–148, 2021.

[70] J.-W. Lee, E. Lee, Y. Lee, Y.-S. Kim, and J.-S. No, “High-precision bootstrapping of rns-ckks homomorphic encryption using optimal minimax polynomial approximation and inverse sine function,” in *Advances in Cryptology–EUROCRYPT 2021: 40th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, October 17– 21, 2021, Proceedings, Part I 40*. Springer, 2021, pp. 618–647.

[71] K. Han and D. Ki, “Better bootstrapping for approximate homomorphic encryption,” in *Cryptographers’ Track at the RSA Conference*. Springer, 2020, pp. 364–390.

[72] J.-P. Bossuat, C. Mouchet, J. Troncoso-Pastoriza, and J.-P. Hubaux, “Efficient bootstrapping for approximate homomorphic encryption with non-sparse keys,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2021, pp. 587–617.

[73] E. Hesamifard, H. Takabi, and M. Ghasemi, “Cryptodl: Deep neural networks over encrypted data,” *arXiv preprint arXiv:1711.05189*, 2017.

[74] C. Juvekar, V. Vaikuntanathan, and A. Chandrakasan, “{GAZELLE}: A low latency framework for secure neural network inference,” in *27th USENIX security symposium (USENIX security 18)*, 2018, pp. 1651–1669.

[75] B. Reagen, W.-S. Choi, Y. Ko, V. T. Lee, H.-H. S. Lee, G.-Y. Wei, and D. Brooks, “Cheetah: Optimizing and accelerating homomorphic encryption for private inference,” in *2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA)*. IEEE, 2021, pp. 26–39.

[76] F. Boemer, Y. Lao, and C. N.-H. Wierzynski, “A graph compiler for deep learning on homomorphically encrypted data. arxiv 2018,” *arXiv preprint arXiv:1810.10121*.

[77] F. Boemer, A. Costache, R. Cammarota, and C. Wierzynski, “ngraph-he2: A high-throughput framework for neural network inference on encrypted data,” in *Proceedings of the 7th ACM workshop on encrypted computing & applied homomorphic cryptography*, 2019, pp. 45–56.

[78] R. Gilad-Bachrach, N. Dowlin, K. Laine, K. Lauter, M. Naehrig, and J. Wernsing, “Cryptonets: Applying neural networks to encrypted data with high throughput and accuracy,” in *International conference on machine learning*. PMLR, 2016, pp. 201–210.

[79] H. Chen, I. Chillotti, and Y. Song, “Improved bootstrapping for approxi- mate homomorphic encryption,” in *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, 2019, pp. 34–54.

[80] J.-W. Lee, E. Lee, Y. Lee, Y.-S. Kim, and J.-S. No, “Optimal minimax polynomial approximation of modular reduction for bootstrapping of approxi- mate homomorphic encryption.” *IACR Cryptol. ePrint Arch.*, vol. 2020, p. 552, 2020.

[81] A. Kim, A. Papadimitriou, and Y. Polyakov, “Approximate homomorphic encryption with reduced approximation error,” in *Cryptographers’ Track at the RSA Conference*. Springer, 2022, pp. 120–144.

[82] J. Halpern and V. Teague, “Rational secret sharing and multiparty computation,” in *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*, 2004, pp. 623–632.

[83] A. Lysyanskaya and N. Triandopoulos, “Rationality and adversarial behav- ior in multi-party computation,” in *Annual International Cryptology Conference*. Springer, 2006, pp. 180–197.

[84] A. Beimel, A. Groce, J. Katz, and I. Orlov, “Fair computation with rational players,” *Cryptology ePrint Archive*, 2011.

[85] M. Nojoumian and D. R. Stinson, “Socio-rational secret sharing as a new direction in rational cryptography,” in *Decision and Game Theory for Security: Third International Conference, GameSec 2012, Budapest, Hungary, November 5-6, 2012. Proceedings 3*. Springer, 2012, pp. 18–37.

[86] G. Asharov, R. Canetti, and C. Hazay, “Toward a game theoretic view of secure computation,” *Journal of Cryptology*, vol. 29, no. 4, pp. 879–926, 2016.

[87] S. Nakamoto and A. Bitcoin, “A peer-to-peer electronic cash system,” *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf*, vol. 4, no. 2, p. 15, 2008.

[88] M. Andrychowicz, S. Dziembowski, D. Malinowski, and Ł . Mazurek, "Fair two-party computations via bitcoin deposits," in *Financial Cryptography and Data Security: FC 2014 Workshops, BITCOIN and WAHC 2014, Christ Church, Barbados, March 7, 2014, Revised Selected Papers 18*. Springer, 2014, pp. 105–121.

[89] ——, "Secure multiparty computations on bitcoin," *Communications of the ACM*, vol. 59, no. 4, pp. 76–84, 2016.

[90] I. Bentov and R. Kumaresan, "How to use bitcoin to design fair protocols," in *Annual Cryptology Conference*. Springer, 2014, pp. 421–439.

[91] R. Kumaresan and I. Bentov, "How to use bitcoin to incentivize correct computations," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 30–41.

[92] A. Kiayias, H.-S. Zhou, and V. Zikas, "Fair and robust multi-party computation using a global transaction ledger," in *Advances in Cryptology–EUROCRYPT 2016: 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Vienna, Austria, May 8-12, 2016, Proceedings, Part II 35*. Springer, 2016, pp. 705–734.

[93] L. Sweeney, "k-anonymity: A model for protecting privacy," *International journal of uncertainty, fuzziness and knowledge-based systems*, vol. 10, no. 05, pp. 557–570, 2002.

[94] N. Li, T. Li, and S. Venkatasubramanian, "t-closeness: Privacy beyond k-anonymity and l-diversity," in *2007 IEEE 23rd international conference on data engineering*. IEEE, 2006, pp. 106–115.

[95] A. Narayanan and V. Shmatikov, "How to break anonymity of the netflix prize dataset," *arXiv preprint cs/0610105*, 2006.

[96] Y.-A. De Montjoye, C. A. Hidalgo, M. Verleysen, and V. D. Blondel, "Unique in the crowd: The privacy bounds of human mobility," *Scientific reports*, vol. 3, no. 1, pp. 1–5, 2013.

[97] C. Dwork, "Differential privacy," in *International colloquium on automata, languages, and programming*. Springer, 2006, pp. 1–12.

[98] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd international conference on open and big data (OBD)*. IEEE, 2016, pp. 25–30.

[99] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Y. MedBlock, "Efficient and secure medical data sharing via blockchain., 2018, 42," *DOI: https://doi. org/10.1007/s10916-018-0993-7*, p. 136.

[100] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain," *Journal of medical systems*, vol. 42, no. 8, p. 140, 2018.

[101] D. Soujanya and K. Venkata Ramana, "Secured surveillance storage model using blockchain," in *Evolving Technologies for Computing, Communication and Smart World: Proceedings of ETCCS 2020*. Springer, 2021, pp. 249– 263.

[102] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in *Security, Privacy, and Anonymity in Computation, Communication, and Stor- age: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10*. Springer, 2017, pp. 534–543.

[103] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, and S. Liu, "Blockchain-based data preservation system for medical data," *Journal of medical systems*, vol. 42, pp. 1–13, 2018.

[104] B. Shen, J. Guo, and Y. Yang, "Medchain: Efficient healthcare data sharing via blockchain," *Applied sciences*, vol. 9, no. 6, p. 1207, 2019.

[105] M. Uddin, M. Memon, I. Memon, I. Ali, J. Memon, M. Abdelhaq, and R. Alsaqour, "Hyperledger fabric blockchain: Secure and efficient solution

for electronic health records," *Computers, Materials & Continua*, vol. 68, no. 2, pp. 2377–2397, 2021.

[106] R. Kumaresan, T. Moran, and I. Bentov, "How to use bitcoin to play decentralized poker," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 195–206.

[107] R. Kumaresan, V. Vaikuntanathan, and P. N. Vasudevan, "Improvements to secure computation with penalties," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016, pp. 406–417.

[108] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "l-diversity: Privacy beyond k-anonymity," *Acm transactions on knowledge discovery from data (tkdd)*, vol. 1, no. 1, pp. 3–es, 2007.

[109] N. Alrebdi, A. Alabdulatif, C. Iwendi, and Z. Lian, "Svbe: Searchable and verifiable blockchain-based electronic medical records system," *Scientific Reports*, vol. 12, no. 1, p. 266, 2022.

[110] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, and E. Oropallo, "Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem," *Technovation*, vol. 120, p. 102480, 2023.

[111] A. Chatterjee, N. Pahari, and A. Prinz, "Hl7 fhir with snomed-ct to achieve semantic and structural interoperability in personal health data: a proof-of-concept study," *Sensors*, vol. 22, no. 10, p. 3756, 2022.

[112] J. Jayabalan and N. Jeyanthi, "Scalable blockchain model using off-chain ipfs storage for healthcare data security and privacy," *Journal of Parallel and distributed computing*, vol. 164, pp. 152–167, 2022.

[113] P. Ruan, T. T. Anh Dinh, Q. Lin, M. Zhang, G. Chen, and B. Chin Ooi, "Revealing every story of data in blockchain systems," *ACM Sigmod Record*, vol. 49, no. 1, pp. 70–77, 2020.

[114] D. Tith, J.-S. Lee, H. Suzuki, W. Wijesundara, N. Taira, T. Obi, and N. Ohyama, “Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability,” *Healthcare informatics research*, vol. 26, no. 1, pp. 3–12, 2020.

[115] M. Prokofieva, S. J. Miah *et al.*, “Blockchain in healthcare,” *Australasian Journal of Information Systems*, vol. 23, 2019.

[116] V. Mani, P. Manickam, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, “Hyperledger healthchain: patient-centric ipfs-based storage of health records,” *Electronics*, vol. 10, no. 23, p. 3003, 2021.

[117] S. Chenthara, K. Ahmed, H. Wang, F. Whittaker, and Z. Chen, “Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology,” *Plos one*, vol. 15, no. 12, p. e0243043, 2020.

[118] M. Verdonck and G. Poels, “Decentralized data access with ipfs and smart contract permission management for electronic health records,” in *Business Process Management Workshops: BPM 2020 International Workshops, Seville, Spain, September 13–18, 2020, Revised Selected Papers 18*. Springer, 2020, pp. 5–16.

[119] N. Ashizawa, N. Yanai, J. P. Cruz, and S. Okamura, “Eth2vec: learning contract-wide code representations for vulnerability detection on ethereum smart contracts,” in *Proceedings of the 3rd ACM international symposium on blockchain and secure critical infrastructure*, 2021, pp. 47–59.

[120] Z. Peng, C. Xu, H. Wang, J. Huang, J. Xu, and X. Chu, “P2b-trace: Privacy-preserving blockchain-based contact tracing to combat pandemics,” in *Proceedings of the 2021 international conference on management of data*, 2021, pp. 2389–2393.

Publications

- Survey On Electronic Health Records (EHRS): Challenges And Solutions , Proceedings of the Sixth International Conference on Computing Methodologies and Communication (ICCMC 2022) IEEE Xplore Part Number: CFP22K25-ART; ISBN:978-1-6654-1028- (Published -Scopus indexed)

- Blockchain in Healthcare:An Evaluation of Literature,Frameworks and Recommendations,proceedings in the 2nd Internatioanl Conference on Networks ,Intelligence Computing (ICONIC 2024) (Accepted and Proceedings started for Publication)

- The Network MLPPM :Machine Learning Privacy -Preserving Model with Fully Homomorphic Encryption for Deep Neural Network ,proceedings in the Internatioanl Journal of Systematic Innovation (IJOSI) Scopus Free Journal (Accepted)(SJR Value: 0.15)

- Blockchain -Based Secure Multiple Computation Scheme (Bsmpcs) For Preserving And Extraction Of Healthcare Data ,Published in International of Information Systems Engineering and Management,2025, 10(18s) e-ISSN: 2468-4376.

- Blockchain-Based Smart Medical Privacy-Preserving Contract System for Secure Electronic Health Records Management" has been accepted for publication in International Journal of Environmental Sciences, ISSN: 2229-7359, Volume 11, No. 6.

Appendix A

Appendix

Implmentation Algorithms

Privacy in Healthcare

BT is a viable solution for enhancing healthcare privacy due to its numerous advantages.

Data is disseminated over multiple network nodes. Consequently, the likelihood of encountering
a singular site susceptible to failure or attack is diminished.

Step 1: Planning

1. Identified Research gaps need for our requirement
2. Research questions & Objectives delineated
3. Specifying appropriate database & Selection criteria

Step 2: Execution

1. Database Search
2. Article Screening
3. Select articles curated for the present study

Step 3: Assimilation

1. Information Extraction & Structuring
2. Synthesis of focal areas
3. Proposition of future research issues

The Cheon-Kim-Kim-Song (CKKS) scheme, along with the Brakerski-Fan-Vercauteren (BFV) scheme, represents a category of word-wise FHE systems. The CKKS

scheme, in
particular, is well-suited for handling encrypted real data and has been widely adopted for MLPPM applications

ResNet-50 ON CKKS-RNS SCHEME

This framework includes convolution (Conv), fully connected layer (FC), and Softmax. With the exception of the addition of bootstrapping processes, This device and the original ResNet-50 model are almost identical. FHE techniques and implementations could contribute to faster processing times. By leveraging these accelerators, it may be possible to reduce the runtime substantially, making FHE more viable for deep learning applications. Moreover, applying the MLPPM model to individual images rather than batches and optimizing the CKKS-RNS scheme's packing mechanism could further reduce execution time. This approach will be explored in subsequent research to optimize batch processing and enhance overall performance.

Homomorphic encryption:

The algorithm used for performing homomorphic encryption is If the public key is (G, q, g, h), where = gx, and x is the secret key, then the encryption of a message is m (m) = (gr, m, r) for any random r$\{0, . . . , q - 1\}$ in the ElGamal cryptosystem, which is a cyclic group G of rank q with generator g.

Register: To become an MPS node, a participant must first register once this is done will the participant be eligible services in exchange for money.

Reputation System: According to this contract, every MPS node has a rep- utation value. The reputation value of the MPS node will rise if it cooperates and does the calculation work successfully; if not, it will fall. The MPS nodes' long-term usefulness is determined by their reputation value.

Incentive Mechanism: The MPS node receives revenue from two sources: the price charged to users who use the service, and the penalty imposed on dishonest MPS nodes. The allocation of rewards after the completion of each service is a reflection of the real usefulness of MPS nodes, as determined by the Incentive Mechanism.

Choose Quorum: In order to complete the present calculation work, users may choose. A low reputation does not guarantee selection, but the likelihood will drop very rapidly as the reputation value drops. The poor players should be given another opportunity to make up for their previous actions. We must also take a newbie into account. This is in line with what is really true

Setup Phase: Each participant's reputation value is publicly maintained by the ledger based on their previous actions. To make selection easier, individuals must build up their reputation values over an extended period of time

Phase of Input: When submitting the input, users must charge for the current job. The accuracy of the user's input will. The service fee will be charged to the truthful Users if they fail to provide the accurate input within the allotted period. The service price will allow the programme to withstand denial-of-service assaults from users

Compute Phase: The Smart Contract also detects the MPS node's intermediate value. In conclusion, the Smart Contract will identify any BSMPSS participant who violates the protocol and will prevent them from taking part in the subsequent task. The plan makes use of a (t, n)-theshold secret share, which provides some fault tolerance as long as an appropriate t is specified. Users may choose a new subset to resume the agreement even in the event that the protocol is terminated. As a result, BSMPSS is resilient

Doctor: When a patient registers with the system, the request is sent to a related doctor. To access the data, he obtains authorization from the BN. In addition, he generates a treatment ID for the ongoing procedure. In addition to recommending certain medications and testing, the doctor uploads the information to the blockchain.

Insurance Company: The patients, hospital, and BN are all covered in this module. Depending on the kind of issue and emergency found, the patients register with the insurance provider. The hospital and the doctor confirm the information with the insurance company. If the request is determined to be legitimate, the patient's claim is rejected; otherwise, the information is processed and money is awarded to the patient.

Pharmacist: Patients may place online orders for medications from the pharmacy after obtaining prescriptions from their doctors. The blockchain will be updated with the same.

IPFS Storage: The peers in the network store all of the reports in IPFS. Every file has a Content Identifier created for it when the reports are uploaded. This serves as a point of reference for network file access. In the blockchain, this produced Content Identifier value will be kept. To verify transactions submitted by different participating entities and to construct a block, this module really implements the consensus procedures.

The significance of electronic health information in terms of numerous security and privacy issues is covered in this study. After meticulously noting a number of issues, we established a novel architecture to protect and preserve the confidentiality of healthcare data. This is why data is sent and stored in an encrypted