DESIGN AND ANALYSIS OF CLOUD CRYPTOGRAPHY BY COMBINING BLOCK-CHAIN MULTI AUTHORITY BOTNET

A

Thesis

Submitted for the Award of the Degree of

DOCTOR OF PHILOSOPHY

in

COMPUTER SCIENCE AND ENGINEERING

Submitted By

RAVIKUMAR CH

41900133

Supervised By

Dr Isha Batra

LOVELY PROFESSIONAL UNIVERSITY, PUNJAB

2024

CANDIDATE'S DECLARATION

I hereby declare that the thesis entitled, **"DESIGN AND ANALYSIS OF CLOUD CRYPTOGRAPHY BY COMBINING BLOCK-CHAIN MULTI AUTHORITY BOTNET",** submitted for the Degree of Doctor of Philosophy in Computer Science and Engineering is the result of my original and independent research work carried out under the guidance of Supervisor Dr. Isha Batra, Professor, School of Computer Science and Engineering, Lovely Professional University, Punjab. This work has not been submitted for the award of any degree, diploma, associateship, or fellowship of any University or Institution.

Date:

Investigator: Ravikumar Ch

School: Computer Science and Engineering
Lovely Professional University,
Punjab, India

CERTIFICATE

This is to certify that the thesis entitled *"Design and Analysis of Cloud Cryptography by Combining Block-chain Multi Authority Botnet",* submitted by **Ravikumar Ch** for the award of the degree of Doctor of Philosophy in Computer Science and Engineering, Lovely Professional University, is entirely based on the work carried out by her under my supervision and guidance. The work reported embodies the candidate's original work and has not been submitted to any other university or institution for the award of any degree or diploma, according to my knowledge.

Signature of Advisor **Date:**

Name: Dr. Isha Batra

Designation: Professor

Computer Science and Engineering

Lovely Professional University

ABSTRACT

The significance of addressing issues pertaining to cloud data security and the growing adoption of cloud storage solutions is on the rise. This study presents a robust approach utilizing blockchain technology to ensure data integrity within cloud environments. Beyond rectifying certain challenges associated with conventional central audit techniques, our objective is to leverage blockchain technology to enhance both the efficiency and security of the system. The integration of lattice-based authentication and cuckoo filters will effectively tackle processing power limitations while bolstering the identification verification process. We hold firm confidence in the effectiveness of our strategy to counter the threats posed by quantum computing. Rooted in the recognition of a Shortest Independent Subsequence problem (SIS), our chosen strategy provides a solid framework for our approach. While the efficiency of the proposed strategy has been evaluated, further elucidation of the assessment methodology and underlying hypothesis is warranted for clarity. A comprehensive investigation into integrity-based verification in conjunction with blockchain technology is deemed indispensable. Moreover, strict adherence to the more stringent guidelines outlined in the plan is imperative.

This research offers two key advancements for a resilient data sharing and retrieval model: the utility-assisted data protection approach and privacy measures. The former integrates blockchain-driven methods into cloud storage, reinforcing security and reducing single-point failure risk in conventional models. These enhancements fortify data security, improve throughput, and optimize cost-effectiveness, providing multifaceted benefits. Evaluation via responsiveness and accurate user detection metrics underscores the positive outcomes of these approaches.

Access control is the critical element of the cloud storage paradigm for boosting data security. However, traditional data sharing and access control approaches face significant challenges due to crucial misuse and privacy data leakage. Cloud computing data outsourcing has facilitated data sharing among various applications, while blockchain technology offers security through encryption mechanisms to confirm user identity. Despite enabling better management, cloud collaboration poses hazards to user privacy. Consequently, this research presents crucial advancements in cloud-based Blockchain's access control and privacy-based data sharing and retrieval processes. The first contribution identifies numerous threats to cloud and blockchain

security and utilizes machine learning models to mitigate risks and conduct a preliminary diagnosis of issues.

Subsequently, a cloud access control and data-sharing mechanism based on Blockchain are introduced. The access control and data-sharing processes based on blockchain technology effectively address the single-point failure created in cloud architecture. Data Users (DUs) initiate registration requests with their ID and password, which are then sent to Data Owners (DOs). A transactional blockchain is established using an encrypted master key and DO data, facilitating data encryption by DOs, with encrypted files being uploaded to IPFS. The transactional Blockchain contains ciphertext created by DOs through counting bloom filter information, including encrypted file locations and keys. Additionally, the research introduces a blockchain framework for efficient data retrieval and sharing on cloud systems, employing cuckoo routing architecture to ensure safe transmission. The cloud platform incorporates elements such as the Inter-Planetary File System (IPFS), transactional Blockchain, smart contracts, and mechanisms for data protection algorithms within DOs, thus ensuring secure information exchange and transmission.

Furthermore, to ensure data integrity within the cloud framework, the effectiveness of the proposed privacy and utility-assisted protection strategy is evaluated using responsiveness, actual user detection rate, privacy, and information loss as metrics. The novel approach for secure data sharing and retrieval in cloud structures demonstrates enhanced performance in this context. Notably, the response time is 21.33 seconds, information loss is curtailed to 3.4%, and a genuine user detection rate of 26.66% and a privacy rate of 93.87% are achieved for the Network traffic dataset. These findings underscore the potential of the privacy and utility-assisted protection strategy to enhance data sharing and retrieval models in cloud architectures. The methodologies developed address security concerns and establish the groundwork for more efficient and dependable cloud-based data management systems.

Overall, the Framework for combining cryptography, Blockchain, multi-authority, and Botnet technologies (BCMAB) stems from the need to address the limitations and challenges in secure, scalable, and trustworthy decentralized systems. By exploring the synergies among these technologies, researchers aim to develop innovative solutions that can advance the field of fast communication, privacy, and decentralized applications.

ACKNOWLEDGEMENT

I want to present my deepest gratitude to **Dr. Isha Batra** for her guidance, advice, understanding and supervision throughout the development of this thesis and study. Despite her busy schedule, he has been available at every step, devoting time and energy to providing much-needed counsel and advice. This enabled me to sail through the tough times and complete this enormous task.

I thank the **research project committee members** for their valuable comments and discussions. A special thanks to the management of **Lovely Professional University** for their support in academic concerns and for letting me get involved in my 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 have always motivated me in all the endeavours of my life, including this research work at LPU. I also thank my wife Swapna, for supporting my research work. My special thanks to my daughters Amuktha and Aaradhya for giving me joyful moments during the whole journey of my research work. Finally, I would like to thank every person who has directly and indirectly helped and motivated me in this journey.

RAVIKUMAR CH

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

LIST OF ABBREVIATIONS

Abbreviation	Description
SIS	Shortest Independent Subsequence
MAC	Mandatory access control
ABAC	Attribute-based access control
ABE	Attribute-based encryption
CSP	Cloud service provider
DAC	Discretionary access control
RBAC	Role-based access control
DHT	Distributed Hash table
IBAC	Identity-based Access Control
ACL	Access Control List
PoW	Proof of work
EVM	Ethereum Virtual Machine
AES	Advanced Encryption Standard
DES	Data Encryption Standard
RSA	Rivest-Shamir-Adleman
ECC	Elliptic Curve Cryptography
BCMAB	Block-Chain Multi Authority Botnet
EACMS	Emergency access control management system
BNA	Business Network Archive
IPFS	Interplanetary File System
EHR	Electronic Health Record
ACC	Access Control Contract
JC	Judge Contract
RC	Register Contract
BPDS	Blockchain-based privacy preserving data sharing model
EOS	Enterprise Operation System
CPVPA	Certificateless public verification mechanism against procrastinating auditors
PKG	Private key generator
WBAN	Wireless Body Area Network
KGA	Keyword Guessing Attack
SDI	Software Defined Infrastructure
POS	Proof of Stake
GDPR	General Data Protection Regulation
DBP	Distance-Bounding Protocol
EFADS	Efficient, Flexible, and Anonymous Data Sharing Model
QoS	Quality-of-Service
SAM	Security Access Managers
BDKMA	Blockchain-based Distributed Key Management Architecture
IoT	Internet of Things
DoS	Denial of service
PoA	Proof of Authority
RNN	Recurrent neural network
KDD	Knowledge Discovery Database
DO	Data Owner
DU	Data User
ECSA	Ensemble Cuckoo Search Algorithm
PDR	Presented Differ Ratio

PDP	Provable data Possession
TPA	Third-Party Auditor
CSO	Cuckoo search optimization
MHT	Merkle Hash Tree
BPMC	Blockchain and multi-party computing
TTP	Trustworthy third party
EOS	Enterprise Operation System
DBP	Distance-Bounding Protocol
SBIBD	Symmetric balanced incomplete block design
Tps	Transactions for second
IBE	Identity-based encryption
EACMS	Emergency access control and management system
PEP	Policy Enforcement Point

CHAPTER 1
INTRODUCTION

This section builds up the knowledge required to understand the problem statement of the research work by understanding the essential workings of Blockchain with decentralized data distribution over the cloud environment for better performance of the data transfer rate with data encryption models along with data traversing algorithms modified Cuckoo. Based on the existing set of problems, multiple research objectives have been framed to carry out this research work.

1.1 Introduction

A cloud storage system stores data that doesn't use local devices or conventional physical storage systems but relatively remote servers that can be accessed online. As long as they have an internet connection, it gives users the freedom to store, manage, and retrieve their data from any location. Systems for cloud storage are based on distributed computing, in which data is spread across numerous servers and places. Compared to conventional storage techniques, this strategy has significant benefits. The first benefit is scalability, which enables customers to expand or reduce their storage capacity based on their demands without physically changing their hardware. Because of its adaptability, cloud storage may be used by people and organizations with different storage needs.

Secondly, cloud storage provides high availability and reliability. Data is replicated and stored redundantly across multiple servers and data centres, guaranteeing accessibility and integrity even in server or location failures. This redundancy enhances data durability, supported by robust backup and disaster recovery mechanisms implemented by cloud storage providers. Additionally, cloud storage offers accessibility, allowing users to access their data from various devices like computers, Smartphone’s, or tablets using dedicated applications or web browsers. This fosters smooth collaboration and sharing among individuals or teams, enabling multiple users to work on duplicate files simultaneously [1].

Security is a critical aspect of cloud storage systems. Providers employ various measures to ensure data privacy and protection, including encryption, access controls, and regular security audits. However, users need to understand the security practices of their chosen cloud storage provider and take additional precautions to protect sensitive or confidential data.

Popular cloud storage platforms include the likes of Amazon S3, Microsoft OneDrive, Google Drive, and Dropbox. These services frequently provide a variety of storage plans, from free tiers with constrained storage capacity to premium subscriptions with higher storage limits and other features.

1.2 Cloud Storage System and Associated Challenges

The most crucial resource in today's world is information. Various electronic devices, including cameras, laptops, computers, and mobile phones, generate vast amounts of data daily, necessitating additional storage and resources. Cloud storage systems comprise distributed data centres or servers that cooperate and offer storage resources through virtualization technologies. The user-friendly nature of cloud storage systems has garnered significant attention from business organizations and individual users. Many consumers and businesses migrate their data to cloud storage systems to alleviate the burden of maintaining and safeguarding it on local storage systems. Cloud storage offers users and companies flexible, on-demand storage options by leveraging third-party services and the Internet. Service providers are responsible for maintaining cloud servers and delivering services for online data processing and storage to consumers [2].

Cloud storage users' system can access their data anytime from any place, allowing users with an on-demand, pay-per-use model. A cloud storage model allows users to lease and pay for computing and storage services according to their needs. Cloud users can use various benefits and features, including low-cost storage, automatic updating, adaptability, and catastrophe-proofing. But, since data could be lost when users save their data to the cloud, it's essential to protect the privacy of users as well as ensure the security of data. Furthermore, when consumers transfer their data to cloud storage, it is possible to lose control over their data, and the cloud storage might not be safe and could be vulnerable to various types of attacks [3]. Some disadvantages of current cloud storage systems are the need for trusted third-party providers, which can compromise server security, and centralized data storage, which can compromise users' privacy.

Distributed cloud storage systems are interconnected, and there is an increased risk of data breaches. Even though data is dispersed over several servers or data centres, a single breach has the potential to expose a significant amount of sensitive data, underscoring the vital necessity of strong security measures throughout the whole cloud infrastructure. For example, well-publicized events such as the illegal access to iCloud data are clear indicators of the pressing need for ongoing monitoring and improved security measures in cloud storage settings [4].

The challenges in the current cloud storage technology are described in the following manner:

a) **Security:** Central authority oversees the services provided through the current cloud system. However, this arrangement comes with a single-point failure, interfering with the availability of security and giving cloud users instant access.

b) **Privacy:** with the massive quantity of data about users collected and stored through cloud-based systems, the cloud storage platform offers its customers ease of use; however, it also poses serious privacy issues for data. So, even though customers do not know where their data goes and who accesses it, cloud users can trust cloud service providers with the data. In the same way, distributed cloud storage systems don't evenly distribute the storage data across the cloud servers. This raises privacy issues if one server is targeted, and the user's data could be disclosed.

c) **Integrity:** Due to the cloud's ability to store and retain user data, integrity problems might occur. The possibility of unapproved updates or deletions of outsourced data by other parties exists. For financial or political advantage, adversaries may alter cloud data resources, endangering the integrity of the data. These reasons have led to the development of several solutions based on third-party auditor-assisted public verification systems. They can also cause various issues, including inexperienced verification, leading to data integrity issues due to fraudsters who audit the data. Thus, we must develop new ways to address the data security issues the cloud storage platform demands.

d) **Data Breach:** Data breaches can result from accidental errors, security flaws, or intentional actions by attackers releasing data to the public. Depending on the sensitivity of the data, leaks can cause significant harm to individuals. Improper encryption methods in the cloud contribute to this problem, leading to the theft of sensitive user information. Implementing security measures such as cryptographic algorithms could help address data breach issues.

e) **Loss of Data Control:** Users that utilize the cloud trust the cloud service providers and entrust them with their sensitive or secret data since they know the data centres are safe. The place of storage for users' data isn't disclosed to cloud users. Therefore, users have no say over where the information is in the cloud or how it is processed. There should be more communication between cloud users and service providers while storing or processing data.

1.3 Blockchain Technology

Blockchain technology has emerged as a pervasive force, revolutionizing industries with its accessibility and security. In collaboration with IoT, exemplified by initiatives like Stuff's Network sponsored by Cloud Infrastructure and IoT Company, Blockchain offers transformative solutions addressing centralization, anonymity, and network stability issues in cloud-based systems. This combination, known as the BCoT prototype, holds promise under specific conditions, providing elasticity and usability to enhance Blockchain efficiency. This article presents a comprehensive analysis of BCoT implementation, delving into sensor data management, incentivization mechanisms, and technology integration. It offers strategic insights into use-case scenarios within and beyond 5G systems, demonstrating the potential of Blockchain and IoT integration in reshaping the technological landscape [5].

Blockchain, created by an anonymous developer named Nakamoto in 2008, is primarily regarded as the underlying technology of the Bitcoin cryptocurrency. Blockchain technology is a peer-to-peer system that serves as a shared and trusted public ledger. Its potential for creating blockchain-based software outside of Bitcoin cryptocurrency innovative technology is now an increasingly popular option for researchers and academics. The main goal of blockchain technology is decentralized governance, where the blockchain may be shared entirely among all of the network's nodes. Every node on the network can assess how other network nodes create, verify, sign, and secure new transactions. The decentralized blockchain architecture offers tamper-resistant and single point of failure-free, dependable, and secure operations. Public and private blockchain networks are the two main divisions of the blockchain. Everyone has access to the public blockchain, meaning anybody may join, create transactions, and participate in the consensus process (like the Bitcoin network). On the other hand, the private blockchain is a permissioned network where each member must first get permission from the authority to join or initiate a transaction [6].

Blockchain, a transformative digital innovation, redefines data storage, security, and transactions through its integral components—ledgers, transactions, blocks, consensus mechanisms, and smart contracts. Transactions, forming the foundation, are vessels for recording data within immutable blocks linked in an unbreakable chain through cryptographic hash values, ensuring security and chronological order. Decentralization sets blockchain apart, with the ledger shared and maintained collectively, promoting trust in a transparent, community-verified environment underpinned by consensus

mechanisms uniting multiple nodes to validate and secure transactions, fortifying the entire network's reliability. Moreover, blockchain innovation extends beyond its core components, as intelligent contracts automate processes, eliminate intermediaries, and reduce costs. At the same time, its tamper-resistant nature finds applications in provenance tracking, supply chain management, and voting systems, enhancing accountability and reducing fraud. In summary, blockchain revolutionizes data and transaction management, fostering decentralization, security, transparency, and automation, with far-reaching implications across various industries [7].

Decentralization is the key feature of blockchain technology. It demonstrates that a centralized authority does not manage blockchain transactions. This extraordinary attribute reduces the potential for a single point of failure associated with centralized authority, thereby lowering operational costs and enhancing reliability. Additionally, blockchain enables transaction data to be immutable or unchangeable over time. The chain of blocks cannot be altered because the hash of each new block is always derived from the hash value of the preceding block. Once verified and uploaded to the blockchain network, it becomes difficult to modify, delete, or remove the data contained in a block. Transparency is another important characteristic of blockchain. Transaction information within the blockchain network is accessible to all users, ensuring complete accessibility, verification, and function tracking for everyone with identical rights. The blockchain achieves this transparency and verification by sharing an exact set of transaction data in the form of a ledger with all users on the network.

1.3.1 Blockchain-Based Cloud Storage System

A new storage system architecture integrating blockchain technology is essential to tackle security concerns arising from increasing data volume and cloud storage systems. By combining cloud storage with blockchain, this technology fusion enhances cloud services, efficiency, decentralization, transparency, and security and benefits both domains [10]. With a decentralized architecture facilitated by blockchain, there's no reliance on centralized authorities. This integration ensures resilience to data alterations and provides numerous potential benefits to cloud storage systems.

a) Decentralization: By eliminating the requirement for dependable third parties, decentralized structures based on blockchain technology may solve the single point of failure problem. Furthermore, the Blockchain’s peer-to-peer architecture guarantees immutability features and gives each network member an equal right to confirm the accuracy of the data [11].

b) Security: Through built-in network features, including confidentiality and availability, blockchain technology enhances the protection of the cloud storage system. The blockchain network keeps track of all transactions that are hash-encrypted and recorded. Network users also sign blockchain transactions to protect the privacy of user communications with cloud storage services.

c) Privacy: The Blockchain's integrity, immutability, and transparency properties provide the cloud storage system with high security. Each data block is stored in a linked chain on the blockchain network by being connected to the block before it. Therefore, altering or updating its content is impossible because blockchain is supported and governed by an immutable and secure consensus mechanism.

d) System difficulty: By combining blockchain technology with a cloud storage platform, the difficulty of implementation is significantly decreased. The cost of the required blockchain resources can be reduced using the cloud infrastructure to run the algorithms. Combining blockchain and the cloud opens up several quick and low-cost possibilities for the wide-scale implementation of blockchain-based cloud storage systems.

e) Feasibility: Several big organizations are actively deploying blockchain as a service project to test the viability of connecting blockchain with cloud technologies. Many businesses, including Amazon, IBM, Microsoft, and Oracle, have introduced the blockchain as a service platform on cloud computing. Additionally, combining blockchain with the cloud has tremendous advantages in several industries, including the Internet of Things, finance, healthcare, supply chain, and entertainment.

1.3.2 Access control-based data privacy

Access control in cloud computing is pivotal for maintaining the confidentiality and security of data, presenting a multifaceted challenge that demands robust solutions. Traditional access control mechanisms such as Mandatory Access Control (MAC), Attribute-based Access Control (ABAC), Usage Control (UCON), and Discretionary Access Control (DAC) form the foundation of security protocols within cloud frameworks [12]. However, the dynamic nature of cloud environments necessitates continual innovation in access control techniques to address evolving threats effectively. From confirming authoritative identification to implementing granular permission structures based on user roles and environmental conditions, access control mechanisms must adapt to the intricacies of cloud computing to thwart unauthorized access and safeguard essential data resources [13].

Mutual authentication between users and service providers is paramount in ensuring cloud security, requiring vigilant measures against channel attacks and other malicious tactics. While Cloud Service Providers (CSPs) leverage various access control measures and encryption technologies to bolster security, significant limitations persist, necessitating ongoing collaboration and innovation. By remaining proactive and responsive to emerging threats, stakeholders can work together to fortify access control mechanisms within cloud environments, ensuring the continued integrity and confidentiality of cloud-based systems and services [14].

1.3.3 Role-Based Access Control (RBAC)

Access control is a primary demand of any data device. Some general access control methods for services, namely ABAC and RBAC, are described. This RBAC system considers a cluster of roles that can be accessed to carry out some actions so that the users get access to operate at some essential parts. In general, the access control model considers the existence of a set of permissions P and a kind of user U [15].

1.3.4 Attribute-Based Access Control (ABAC)

The ABAC system consists of two requirements: the architecture model and the policy model. The policy model describes the characteristics of the ABAC schemes, whereas the architectural model considers the regulations of data access control [15].

1.3.5. Subject Attributes

A subject is a user who draws progress on a resource. Each subject comprises the related values that define the subject's characteristics and identity. These attributes include the subject's name, job title, organization, and subject identifier. On the other hand, a resource is a user that proceeds by a subject. Besides, the attributes in the resources are enlarged to authorize control decisions.

1.3.6 Environment Attributes

Environmental attributes play a pivotal role in shaping access control policies, as they dynamically adjust to varying contexts, such as network conditions and user locations. This adaptability ensures that access decisions remain aligned with evolving security requirements and compliance standards, fostering a robust and agile data governance framework. Additionally, the seamless integration of Attribute-Based Access Control (ABAC) necessitates a nuanced policy representation that accommodates diverse environmental factors, enabling fine-grained control over data access permissions across disparate systems and scenarios [16].

1.3.7. Multi-Clouds access control

Various methodologies have been developed to tackle permission control challenges in cloud environments. One notable approach involves creating a distributed access control infrastructure tailored to the cloud. This framework aligns with federated and loosely connected integration techniques, relying on the Role-Based Access Control (RBAC) system as its foundation. Access control rules are distributed like federated institutions within an XACML-enabled model called tenants [17]. The proxy multi-cloud computing model is also pivotal in facilitating the real-time integration of cloud-driven methodologies and dynamic incorporation.

1.4 Access management via blockchain

The work presented in this chapter offers a decentralized privacy solution for maintaining the privacy of information gathered and processed with the help of an outside party. This approach uses a blockchain as an access controller to protect the confidentiality of sensitive data. Pointers and an off-blockchain Distributed Hash Table (DHT) are also included, and the DHT maintains the encrypted data with the help of blockchain authorization. User and service login key pairs are combined to create a new composite identity each time a user checks in. Encrypting and decrypting the data both utilize an identification key. The blockchain is essential for authenticating the user and determining if the service is permitted access to the data. Additionally, it produces the hash code needed to retrieve the data from off-chain storage safely [18].

1.4.1 Block-chain based data sharing in the Cloud

Blockchain is a decentralized architectural concept that creates an immutable ledger for recording all transactions in a distributed manner. It serves as a secure data repository where events, referred to as blocks, are chronologically ordered. This transparent, distributed, and open ledger efficiently records every transaction between parties in an auditable way. Once data is placed into the blockchain, it cannot be changed unless a new record is added. Users in the cryptocurrency world maintain precise records on the network, ensuring consensus among all nodes in the blockchain currency [19].

1.4.2 Access control-based Blockchain in the Cloud

Ensuring confidence and reducing computing costs, the integration of blockchain technology presents a promising trend in cloud storage systems. This adoption enhances the trustworthiness, transparency, and decentralization of the system, enabling numerous connected devices to benefit from Blockchain’s confidence-building features.

By introducing a novel data management technique, blockchain empowers data owners to control and manage their data, thereby enhancing privacy protection for personal information. Moreover, the blockchain system paradigm addresses various challenges, including data privacy concerns. One notable aspect is the utilization of attribute-based encryption (ABE) in access control techniques, which enhances security measures.

The access control approach leveraging blockchain technology aims to bolster security measures. A crucial aspect of ensuring data privacy is through access restriction. Traditional access control models such as discretionary access control (DAC) and identity-based access control (IBAC) face limitations in establishing access control within the Internet of Things (IoT) system. All users can't create an Access Control List (ACL) in the IoT system due to its sheer volume of anonymous identities. However, by integrating delegation units that temporarily assign user-accessible privileges, the access control system simplifies management. Consequently, the system prioritizes the number of users over the total attributes, streamlining access control management [20].

1.5 Data Sharing Privacy in the Cloud

Privacy encompasses an individual's or group's ability to safeguard and control the disclosure of their data [21]. Its multifaceted nature includes how, when, and to what extent information is shared. Recent data holds more relevance than records, with users often preferring manual requests from friends over automatic alerts. Users may keep their information vague rather than pinpoint accuracy, reflecting varying comfort levels with data sharing.

In various commercial applications, the privacy and context of the user should be utilized and protected accurately, necessitating advanced encryption techniques, stringent access controls, and robust identity verification mechanisms to safeguard sensitive information. In institutions, security demands the application of laws, principles, and processes by which individually identifiable data is controlled, not only to comply with regulatory requirements but also to implant confidence among stakeholders, reinforcing the trustworthiness of data handling practices. Balancing these imperatives in the digital age presents an ongoing challenge, requiring continuous innovation and adaptation to ensure data security and privacy while enabling the seamless functioning of modern information systems.

In a cloud framework, security is defined as the services that secure the opponent from the deducing user's character model by the user's visit system if the individuals meet the sensitive information. Recently, numerous researchers have concentrated on Oblivious

RAM (ORAM) technology that meets diverse duplications of information to cover the authentic meeting objectives of users. ORAM has widespread applications in protecting the software and has been utilized as a promising mechanism in preserving the precautions in a cloud environment. There are various layers for securing data privacy in the cloud framework [22]. The first layer defines the likelihood of cloud resources for the user. The next layer is the authentication layer, which describes the valid authorization of users that helps sweep away the ease of access of illegal users, thereby protecting the information from intruders. The third layer is the confidentiality layer, which defines data protection; hence, the information is not supposed to be accessed by the public and must only be accessed by confidential users.

1.6 Data protection model

The data protection mechanisms are distinguished into four layers: the user layer, interface layer, platform layer, and management layer. This platform is more responsible for controlling the basic information storage process, while the interface layer is used for data encryption and categorization. The user layer validates the user's signature and offers significant information [23]. On the other hand, the control layer uses managing approaches to verify the effective mechanism of the overall process. The specific functionalities of every layer are illustrated as follows:

a) User layer

The user layer involves managing user applications and permissions, typically leveraging robust technologies like authentication and access control. These technologies facilitate user management and signature verification. Rigorous identity authentication ensures the continuity of characteristics and reveals authorization rights, effectively verifying privacy information in cloud computing platforms. To maintain the effectiveness of cloud computing, intricate authentication techniques are employed. Therefore, users should implement high-intensity authentication mechanisms to enhance security.

b) Interface layer

The interface layer is the gateway to cloud computing, classification, data evaluation, and equipment and data encryption technology. The data analysis and categorization model is a method introduced to encounter layer requirements. The advantage of this method is that it aids the users in managing the primary information but also enhances the potency of protecting the data security. The interface layer comprises programs and

devices and is mainly positioned at the gateway and outlet of the private cloud, which is used for encrypting, extracting, and categorizing user information. However, it validates the fundamental data of the user that will not move out to the public cloud. If primary information wants to be protected in public data, it should be encrypted to verify its privacy.

c) Platform Layer

The platform layer comprises both public and private. Data is categorized into core data that is protected in the private cloud. In the same way, the large-scale encrypted information is also saved in the public cloud. This mechanism depends on the hybrid cloud paradigm; the general users do not hold any private cloud. In addition, ordinary users can transform the private cloud into a user intranet, which also meets the security needs of this model.

d) Management Layer

The management layer usually includes safety audits, risk assessments, implementation of security strategies, and education. This layer typically supports the overall model's functioning and assures the working of the entire model. In terms of safety management, it also needs effective management to keep it, or else the most modern technology is very tough to play its part. Thus, user data can be secured in cloud computing by utilizing privacy management schemes based on the associated policies and regulations included with the enterprise's privacy security requirements.

1.7 Blockchain Technology and Cryptocurrencies

Online businesses and e-commerce are growing fast, and most online payments rely on trusted third parties to process the transactions. The Financial Institution serving as a third party has limitations and flaws like cost, time, storage, and security issues. Irreversibility of the transaction is not avoided to address mediating disputes. All these issues can be avoided if the transactions are done in person and using cash. Since that is fast changing, for the payments to be successful and fraud-free, there is a need for a new system without a central authority. The pandemic has accelerated the need for new technology that is advanced and secure at the same time. Similar electronic payment technology was presented in 2008[24]. A person, organization, or anonymous person named Satoshi Nakamoto suggested it. Satoshi proposed to use cryptographic-proof methods to create an electronic system enabling parties to conduct transactions without needing third parties. The innovation gave rise to a new technology known as

Blockchain technology. This technology's popularity, flexibility, functionality, and availability have made it more adaptable. This technology solves the double spending problem and the middleman in payments. It serves as a protocol for exchanging cryptocurrencies such as Bitcoins. The very first cryptocurrency to apply this for exchange was Bitcoin. It solves a very familiar computer science problem, The Byzantine Generals Problem, which questions the consensus of distributed systems by providing a probabilistic approach. Many other crypto coins came into existence and gained popularity [25].

1.7.1 Cryptocurrencies

a) **Bitcoin:** In the cryptocurrency community, it is referred to as the gold standard of the internet. Bitcoin is the first cryptocurrency on the market to trade assets between two people who are not under a single authority. It has the most robust brand recognition of any cryptocurrency on the market. Bitcoin cannot be faked or inflated in any way. Monitoring digital money ownership is the primary goal of the Bitcoin blockchain.

b) **Ether:** Quickly climbed to second place in terms of the market value of cryptocurrencies. Ethereum is predicted to surpass Bitcoin. The Ethereum Network, or computer code execution, is the main objective of the Ethereum Blockchain. Due to Ethereum's expansion, a single platform may now support thousands of apps [26].

c) **Litecoin:** Litecoin was introduced in 2011 to become the "silver" counterpart to Bitcoin. Developed to address Bitcoin's limitations, Litecoin boasts a shorter block creation time of around 2.5 minutes than Bitcoin's 10 minutes. Moreover, Litecoin can handle a higher number of transactions per second. Its shorter block times also help in avoiding double-spending.

Blockchain technology encompasses features such as a distributed database, decentralized networks, and digital ledgers, facilitating swift updating and storage of information. Peer-to-peer networks, constructed around nodes, can store and link with other assets using standard methods common in the financial industry. Data is safeguarded against alteration through cryptographic algorithms and encryption techniques. Each transaction is linked using hashes, time-stamped as a block, and securely preserved. Cryptography and hashing play crucial roles in Blockchain technology, with the Merkle tree concept employed to record transactional details [27].

1.7.2 Working of Blockchain Technology

A decentralized system is run by its users directly, without the involvement of any middlemen or external central authorities. It facilitates sending money to anyone on the network, making it easier for nodes or users. Blockchain enables speedy and efficient payments to everyone on the network. A cryptocurrency, like Bitcoin, consists of a network of peers all on its own. Every peer has a copy of the transactional history on file [28]. It demonstrates that sophisticated mathematical calculations, rather than trustworthy individuals, safeguard cryptocurrency. Blockchain doesn't care whether a cryptocurrency represents a certain number of dollars, cursors, or other units. Nodes are free to choose their coin unit. Blockchain technology allows for more transactions than financial and payment-related ones. Numerous assets, such as hundreds of barrels of oil, award credits, or an electoral vote, may be represented by a cryptocurrency. The transaction and the block construction are both started by the user. The nodes of the Blockchain network must validate the newly formed block. Only after confirmation is the block added to the Blockchain, and only then is the transaction completed at the receiving end. The completed transaction is then updated on the distributed network [29].

1.7.3 Necessary Requirements for Blockchain Technology

Before implementing Blockchain in traditional applications, it is necessary to determine whether the technology is compatible with all conventional systems and generates effective outcomes. As a result of the analysis, a decision tree was created to select this and apply it to the appropriate system. When deciding which application to choose, several qualities need to be considered. These qualities include the level of trust required, transaction speed, system security, authorization, and the ability to prevent reversibility. A decision tree can be employed to aid in this selection process. By following this tree, one can navigate the different factors and find a suitable method for their needs. However, suppose the preference is still inclined towards utilizing the rapidly advancing technology. In that case, there are two fundamental types of ledgers available: Permissioned Blockchain, also known as private Blockchain, and Permission-less Blockchain, often referred to as public Blockchain. These options present distinct characteristics and considerations that should be carefully evaluated before deciding [30].

The determination of whether a blockchain will be private or the Functional Requirements govern the public. Known miners who are authorized are responsible for

mining the Permissioned Block, with the Permission Blockchain Network managed by an authorized miner. Every function can be configured based on the granted rights in a network with permissions. The primary duty of a block miner is to verify transactions, for which they receive compensation upon completing the verification process [31].

Every transaction in the ledger is identified using a transaction ID. Transaction details are based on the public key of the sender and the public key of the receiver. Input refers to the amount transferred to the beneficiary and the fees for verifying the transaction. The output here denotes the total balance available in the user's wallet.

1.7.4 Protocols in Blockchain Technology

In computer science, a protocol is a collection of guidelines or processes that control data transmission between devices. It is easier for computers to communicate and share information appropriately by following predefined standards. The protocol specifies the data format the parties will send and receive [32]. The most widely used internet protocols are DNS and TCP/IP. All participating computers (nodes) in this distributed system that attempt to connect have agreed upon a set of predetermined rules that govern how it operates. Networks need to adhere to a set of standard norms. Several procedures are listed below [33].

Bitcoin Protocol: Initially conceived for the virtual currency Bitcoin, this protocol serves as the governing framework for all Bitcoin transactions, aiming to establish a decentralized, trust-less monetary system, enabling secure peer-to-peer exchanges, and implementing a fixed supply issuance to counter inflation.

i. Anyone with private and public keys may join the Network since it is shared.

ii. This kind of network may be joined without permission.

iii. Each machine connected to this network will have full access to the data on the Bitcoin Blockchain.

iv. Because nodes may carry out irreversible transactions, trust can exist without the involvement of external parties.

v. The network incorporates technological elements such as proof-of-work (POW) consensus techniques, peer-to-peer (P2P) networks, digital signatures, encryption, and cryptographic hashing algorithms to ensure the integrity, security, and transparency of transactions.

1.7.5 Ethereum Protocol

The decentralized Blockchain platform Ethereum is open source, allowing developers to independently create and operate decentralized apps (DApps). The native programming language of Ethereum simplifies app development. The Ethereum main net was deployed on July 30, 2015. Ethereum employs general programming approaches (all-in-one blockchain) to implement its principles more broadly, a vision realized by Vitalik Buterin.

Additionally, it enables the communication between several of these resources, each of which has its state and running program using a message-passing framework. Anyone with access to the internet may use the Ethereum MainNet. Transactions may be created, verified, and added to the Ethereum production Blockchain by anybody with access to the Internet. Additionally, those connected to the leading network may hear the recorded transaction [34].

1.7.6 Smart Contracts

An agreement between unreliable parties is facilitated, carried out, and enforced via Blockchain-based software called a Smart Contract. Intelligent contracts are independent, self-verifying agents that operate on the Blockchain. The agreement is much more than a set of rules or requirements that may be expressed in terms of an IF-THEN logic structure. Smart contracts can be used with Ethereum, a Blockchain implementation, to expand its functionality. Located at a specific address on the Ethereum Platform, a contract is a comprehensive collection of Solidity-programmed code (modules) and data (context). Smart contracts are contracts that follow their conditions and carry them out. They are governed by the explicit terms and conditions included therein. Szabo asserts that traditional vending machines predate smart contracts. They accept coins and give the appropriate change by the stated price, along with a product [35].

Smart denotes quick thinking, and contract indicates something intended to be upheld by a court of law or other agreement. A smart contract is an automated, self-verifiable, intelligent agreement in JavaScript-based computer language. The Ethereum platform introduced smart contracts. Smart contracts are used as examples of deployed custom logic. The Ethereum Virtual Machine, or EVM, performs them. Smart contracts make it possible to write and move transactions across accounts. They resemble classes in object-oriented programming in many ways. Smart contracts may communicate with one another through calls. When an instance is created, specific functions may be

started, and the contract data can be modified along with a particular logic. For the Smart Contract, three significant research areas are made: Anonymity, Privacy, and Confidentiality selection. Anonymity is a concern as the technology shares all the data without checks and barriers. Users may create as many addresses as they like, which affects individuality. Zero Cash is a proposed cryptocurrency that meets privacy requirements by hiding all information except transactions [36]. Cryptocurrency privacy can also be attained by using coin-mixing methods compatible with Bitcoin to generate a whole new cryptocurrency. The author considered a variety of Sean and Cooper's proposed definitions of Smart Contracts, where the contract is constructed of computer code rather than plain English.

1.8 Cryptography

Cryptography in the cloud refers to securing data stored or utilized within cloud services. With encryption applied to all information cloud providers provide, users can safely and effectively use shared cloud services. The term 'cryptography,' dating back to the eighteenth century, primarily pertains to encryption, converting plaintext (standard data) into ciphertext (incomprehensible structure). Decryption, the reverse process, converts scrambled ciphertext back into plaintext. An algorithm and key determine the encryption process's specifics at any time [37]. Cryptographic keys were commonly used for encryption and decryption without additional processes like authenticity or verification. Generally, there are two types of cryptosystems:

1.8.1 Symmetric cryptography

In the field of symmetric cryptography, the goal is to develop innovative approaches such as homomorphism encryption. This type of encryption allows computations to be performed on encrypted data without the need for decryption, which can protect privacy while also enabling secure data processing. Additionally, developments in quantum-resistant symmetric encryption algorithms address emerging risks posed by quantum computing. It ensures that sensitive information will remain secure over the long term even though technical landscapes are always shifting. It is possible to increase the resilience of symmetric cryptography systems against both current and future adversaries by integrating these breakthroughs with strong key management methods. It will protect the confidentiality and integrity of data across a wide range of applications and situations.

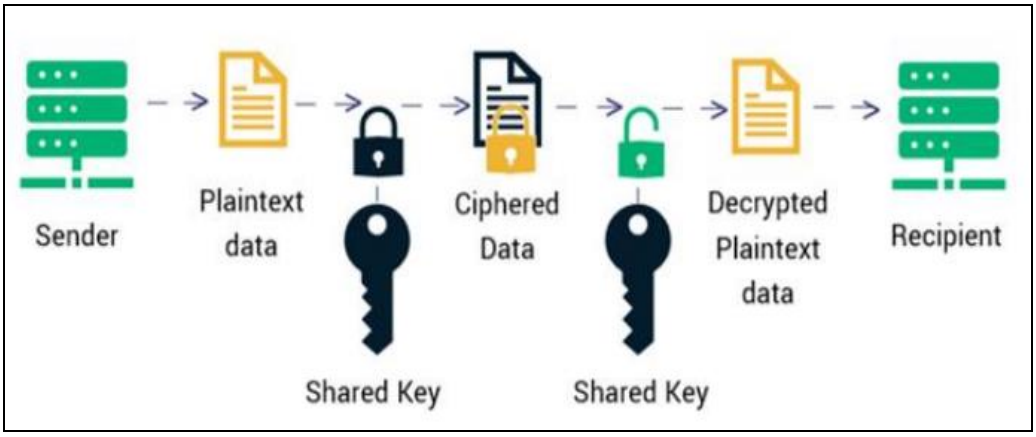


Figure 1.1: Symmetric Encryption

Applications, including secure communication protocols, data encryption, safe storage, and others, all rely significantly on symmetric cryptography. It is a cornerstone of contemporary cryptography and is frequently used to protect the secrecy and privacy of sensitive data. A cryptographic method called symmetric encryption, commonly called secret key encryption, uses the same key for encryption and decryption. The receiver recovers the original message by decrypting the ciphertext using the shared key that the sender used to encrypt the plaintext [38].

Ex: AES, DES. BLOWFISH and 3DES

1.8.2 Asymmetric Cryptography

Asymmetric cryptography, commonly called public-key cryptography, is a cryptographic method that encrypts and decrypts data using a pair of mathematically related keys. The public key is the key that is made available to the general public, while the private key is kept secret. Digital signatures, key exchange, and secure communication are all made possible by the potent toolkit that asymmetric cryptography offers.

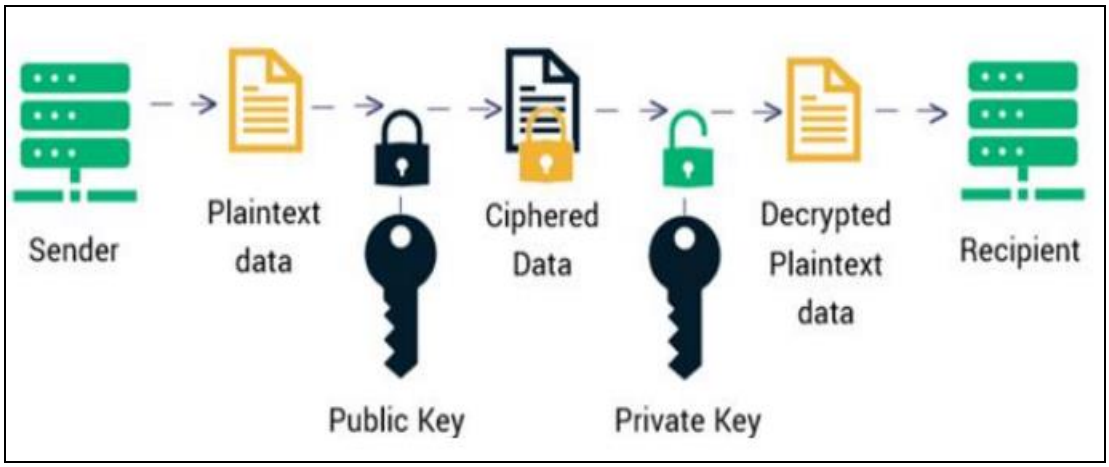


Figure 1.2: Asymmetric Encryption

Asymmetric encryption, commonly called public-key encryption, is a cryptographic technique that encrypts and decrypts data using a pair of mathematically related keys. The decryption key is kept secret, but the encryption key is disclosed. For achieving secrecy, integrity, and authenticity in various applications, asymmetric encryption offers a flexible and secure solution. It is a fundamental part of modern cryptography and is essential for secure email, web browsing, and other cryptographic applications [39]. This system improves communication security because it is so difficult to identify the relationship between the two keys. RSA (Rivest-Shamir-Adleman) and ECC (Elliptic Curve Cryptography) are two examples of asymmetric systems [40].

1.9 Problem statement

Blockchain technology's explosive growth has brought with it several new difficulties and complexities, especially when it comes to integrating it into the financial and industrial services sectors. To effectively address these challenges, the specific problems encountered must be recognised and expressed. The following quotes highlight important topics related to blockchain and cloud computing:

Problem statement 1: The lack of clear authorization processes exposes Blockchain systems to security vulnerabilities.

Problem statement 2: Inadequacies in ensuring the complete removal of digital signatures present risks to data integrity within Blockchain frameworks.

Problem statement 3: Susceptibility to malicious interference underscores vulnerabilities in the information security protocols of Blockchain systems.

Problem statement 4: Compromised credibility and potential loss of digital currency result from cyber attacks on transaction ledgers within Blockchain-based cloud frameworks.

Problem statement 5: The absence of robust residual data security measures raises concerns regarding the complete elimination of digital assets, posing risks to both data privacy and integrity.

Problem statement 6: Insufficient measures to ensure confidentiality and accessibility in advanced Blockchain scenarios may compromise data security and integrity, particularly concerning the complete removal of digital assets.

Therefore, a framework for The Block-Chain Multi Authority Botnet Framework (BCMAB) emerges as an innovative solution, enhancing privacy safeguards, evaluating communication trustworthiness, and fortifying cloud security measures.

1.10 Motivations

The motivation for combining cryptography, blockchain, multi-authority, and Botnet technologies lies in addressing several critical challenges in secure communication, privacy, and trust in a decentralized environment. Cloud computing has revolutionized how businesses and individuals store, process, and access data in recent years. However, this paradigm shift has also brought about various security challenges. Traditional approaches to cloud security, particularly centralized audit techniques, have proven inadequate in the face of sophisticated cyber threats such as data breaches, ransomware attacks, and insider threats.

Central audit techniques often have inherent limitations, including single points of failure and vulnerability to manipulation or compromise. Moreover, cloud environments' dynamic and distributed nature exacerbates these challenges, making it increasingly difficult to ensure data confidentiality, integrity, and availability.

The thesis identifies these shortcomings and addresses the urgent need for innovative solutions to strengthen cloud security and accommodate the dynamic nature of cloud computing ecosystems. The thesis aims to establish a robust foundation for securing cloud infrastructure by leveraging blockchain technology's decentralized and tamper-resistant properties. Blockchain technology, renowned for its immutable ledger and cryptographic security mechanisms, offers advantages for enhancing data integrity and access control in cloud environments. Blockchain-based solutions can mitigate much vulnerability associated with traditional centralized approaches by decentralizing trust and eliminating single points of failure. Furthermore, integrating lattice-based authentication and cuckoo filters introduces novel methods for overcoming processing power constraints, particularly pertinent in resource-constrained cloud environments. These techniques enhance security and optimize the identification verification process, improving system efficiency and performance.

The thesis presents a proactive strategy to tackle evolving threats in cloud computing by integrating blockchain with complementary techniques, aiming for robust protection against cyber threats. It enhances cloud security through rigorous analysis, design, and evaluation, fostering more dependable cloud environments. Combining cryptography, blockchain, multi-authority, and Botnet technologies addresses decentralized system limitations. Researchers strive to innovate solutions for improved communication speed, privacy, and decentralized applications, driven by the necessity to overcome security, scalability, and trust challenges.

1.11 Research objectives

- To analyze the effect of cyber attacks in the traditional cyber framework and study the blockchain cryptocurrency architecture to assess shortcomings and safety performance.

- Implement Blockchain technologies to establish a fast and safe distributed access control system in the cloud platform.

- To create a cloud blockchain multi-authority Botnet that uses the credit-dependent crypto method to detect the functionality of attacks and identify the activity within a computer network or information to ensure a secure information control system.

- The experimental template is used to evaluate the device output in various quality conditions, including processing times and capacity, and to detect consumption rate.

1.12 Research methodology

We advocate for developing an enhanced cloud cryptography blockchain system that integrates visual techniques into consumer and cloud frameworks. This adaptive architecture incorporates Blockchain technology functionalities and strengthens security measures at user endpoints, aiming to bolster security and ensure access protection while enabling a comprehensive evaluation of threat functionalities. To assess the efficiency of this methodology, we will employ network and data attack features to evaluate factors such as network latency, detection rate, processing time, and security breach prevention. Furthermore, the adaptive architecture incorporates botnet functionality to identify data and network threats by assessing attacker functionality coordinating with Blockchain technology to evaluate identifiers and block fraudulent activities. By integrating attacker signatures and identification mechanisms, we aim to determine assault functionality, utilizing machine learning access control methods compared to existing secured and data-sharing models.

Combining cloud computing with consumer-centric strategies offers a dynamic and innovative approach to security challenges in the digital realm. Our proposal advocates for an upgraded cloud blockchain system, leveraging advanced cryptographic techniques to fortify data security, privacy protections, and access controls. By empowering users to customize security measures through blockchain technology, we enable proactive safeguarding of cloud-hosted data and applications. The structured flowchart in Figure 1.3 provides a roadmap for implementing this approach, aligning each step with corresponding research methodologies. Through this holistic strategy, we aim to deliver practical solutions that address current security challenges while

anticipating and adapting to future threats in the digital landscape. Extensive testing and evaluation will validate the effectiveness of our proposed methodology, ensuring its readiness to meet the evolving demands of cybersecurity in an increasingly interconnected world.

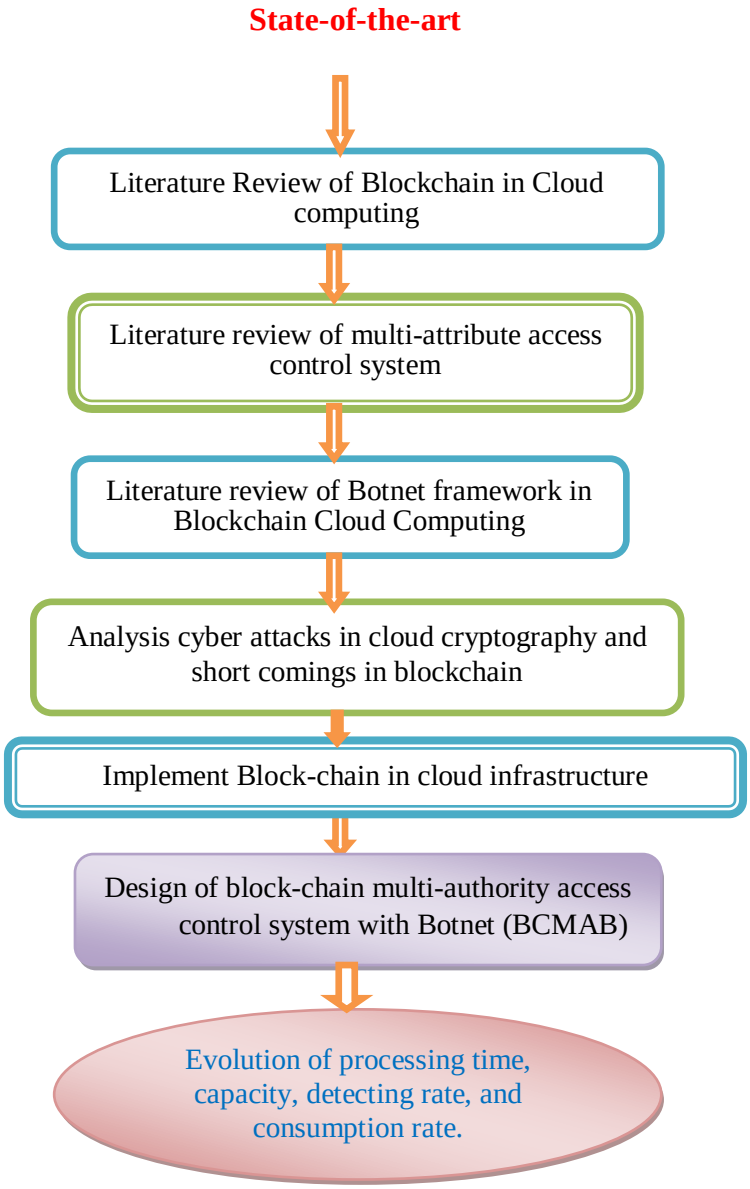


Figure 1.3: Research methodology flowchart

In the research's working model, an adaptive architecture is demonstrated, showcasing the innovative integration of a security system within user areas, coupled with the robust design functionality of Blockchain technology. This pioneering approach comprehensively evaluates the threat landscape, bolsters security measures, and ensures foolproof access protection. The BCMAB framework also addresses the challenge of computation delay in cloud services, a persistent issue that can hinder overall performance. By harnessing the processing power of the multi-authority Botnet and the efficiency of blockchain technology, the framework optimizes resource allocation,

ensures streamlined task execution, and minimizes latency. These results in improved response times, enhanced user experience, and increased operational efficiency for cloud services.

This groundbreaking decentralized integrity service achieves its objectives by streamlining and strengthening security measures while incorporating anonymous authentication systems and implementing role-based access control. Blockchain technology drives this transformation, fundamentally altering the data security landscape. This service establishes an environment that exhibits resilience, transparency, and tamper-proof qualities by eliminating the vulnerabilities associated with centralized systems and eradicating single points of failure. The consensus mechanism, involving multiple network participants, ensures data integrity, rendering it virtually impervious to unauthorized modifications.

Furthermore, this service showcases robust security features and embraces state-of-the-art anonymous authentication systems. This innovative approach empowers users to interact with the blockchain while safeguarding their identities, creating a solid shield for sensitive information and effectively thwarting potential security breaches. Additionally, the system seamlessly integrates role-based access control, providing precise control over data access and modifications. It means that only authorized individuals or entities are granted permission to access specific data, significantly reducing the risk of malicious activities and unauthorized alterations. This multifaceted approach marks a significant leap forward in data security and privacy. In summary, combining these streamlined and robust security measures and the inherent decentralization of the service establishes a trustworthy and resilient solution for safeguarding data integrity across a diverse spectrum of applications and industries. In turn, it reinforces the reliability and security of critical systems, marking a significant advancement in data protection [41].

In Figure 1.4, the research presents an adaptive architecture that seamlessly integrates a security system within user domains, leveraging Blockchain technology's transformative potential. The Block-Chain Multi Authority Botnet Framework (BCMAB) emerges as an innovative solution, enhancing privacy safeguards, evaluating communication trustworthiness, and fortifying cloud security measures. This comprehensive framework aims to mitigate computational latency, ensuring a secure, efficient, and reliable cloud computing ecosystem adaptable to the demands of the digital age.

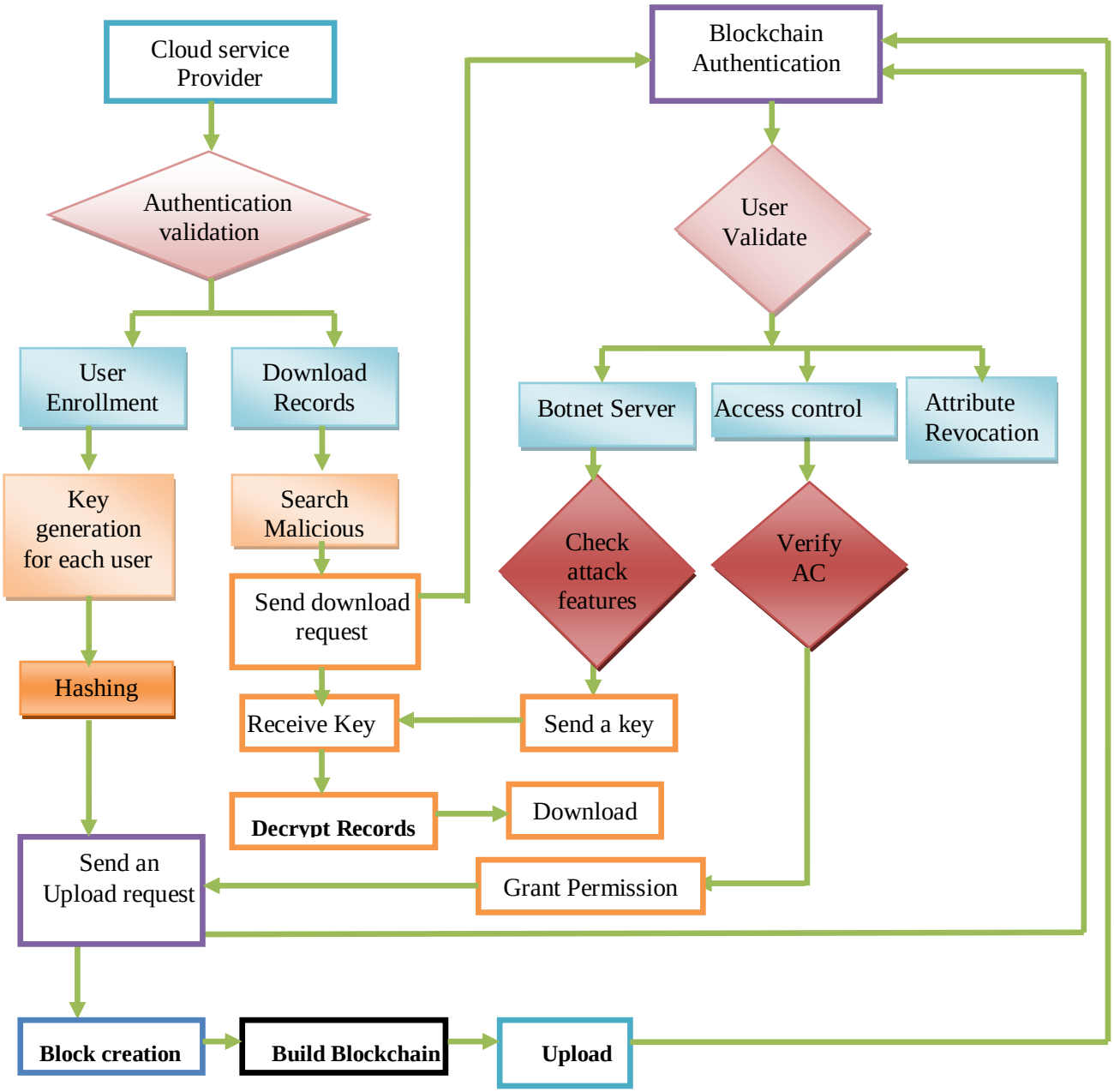


Figure 1.4: Working Model for the Research Work

1.13 Major Contribution of Thesis

This research endeavour seeks to pioneer a groundbreaking approach by synergizing Blockchain, multi-authority authentication, and Botnet detection, ultimately elevating cloud computing security to unprecedented levels. Through this innovative strategy, we aim to bolster data protection and optimize operational efficiency, setting new standards for safeguarding sensitive information in cloud environments.

A trusted and reputed cloud system adopting blockchain and Botnet mechanisms will improve the communication overhead by minimizing the security computation features and maximizing the system efficiency while computing large amounts of data for hybrid cloud service models. In addition, the research model ensures cloud privacy and

enriches the cloud application for assisting different cloud services. Moreover, the cloud system minimizes the latency and avoids data leakage with the help of attribute revocation.

Overall, this research work carried out on the design and analysis of Cloud Cryptography by combining Blockchain, Multi-Authority, and Botnet can make significant contributions to the field of secure cloud computing by proposing a novel approach to secure cloud computing, designing a closed architecture, evaluating performance, conducting a security analysis, comparing with existing methods, and presenting use case scenarios.

1.14 Research Assumptions

Preserving the integrity of cloud-based data is a paramount concern, given the widespread adoption of cloud storage solutions. While various methodologies have been proposed to address this issue, they often have limitations. Our study introduces a novel approach to cloud-based data integrity verification, leveraging blockchain technology to overcome the shortcomings of existing techniques. Specifically, we have implemented a quantum-resistant anomaly, cuckoo, and bloom filter technique, integrating the cuckoo algorithm to alleviate the computational burden associated with user verification. By utilizing blockchain as a decentralized network for releasing and validating verification results, we enhance the security and transparency of the system, moving away from traditional centralized audit mechanisms.

The research outcomes demonstrate our system's remarkable efficiency, particularly in user authentication, while our security analysis showcases the algorithm's resilience against potential hacker threats. By adopting a decentralized blockchain-based integrity service, our approach redefines the conventional centralized model for data integrity verification. Unlike traditional centralized services reliant on a single authority, our decentralized system leverages the collective power of a distributed network of nodes to achieve consensus and ensure data immutability, thus enhancing overall security and reliability.

Furthermore, integrating blockchain technology promotes transparency and trust within the system, mitigating risks associated with single points of failure and offering a robust solution for ensuring the integrity of cloud-based data. As the digital landscape evolves, our innovative methodology provides resilience against emerging threats, ensuring the confidentiality and authenticity of cloud-hosted information.

1.15 Organization of the Thesis

The thesis entitled **"DESIGN AND ANALYSIS OF CLOUD CRYPTOGRAPHY BY COMBINING BLOCK-CHAIN MULTI AUTHORITY BOTNET"** deliberates on Cloud security by addressing a few problems encountered with the traditional central audit technique and approaches. Blockchain technology is employed to improve the system's effectiveness and security. Lattice-based authentication and cuckoo filters are also combined to address the issue of processing power constraints while enhancing the identification verification procedure.

The chapter-wise contribution of the thesis is as follows.

Chapter 1 is an introductory chapter that discusses Cloud Storage System and Associated Challenges, the basics of Blockchain Technology, Access management via blockchain, Data sharing privacy, Data protection, and the basics of Cryptography. The motivation, Research objectives, and the contribution of the work done are also part of this chapter.

Chapter 2 contains the literature survey on the problem addressed in this research work. It presents the literature review on the state of the art for the chosen problem statement. It also contains the research gaps identified in the review of the existing literature.

Chapter 3 analyses cyber-attacks targeting the Cloud and proposes a cryptography model for encrypting blockchain data.

Chapter 4 proposes implementing Blockchain technologies to build a quick and safe distributed access control network in a Cloud platform. The proposed scheme has been thoroughly examined by its simulation, and the results are presented and analyzed well.

Chapter 5 implements a new and innovative design that reduces the consumption of energy as well as the number of nodes crossing in blockchains over the cloud with a group cuckoo model. Again, the proposed method was simulated, and the results were presented and analyzed.

Chapter 6 presents the data transmission for a decentralized approach on the blockchain with efficient capability-based access control (DCapBAC).

Chapter 7 is the concluding chapter of the thesis, which summarizes the significant contributions and considers their ramifications. It also outlines the potential directions for future research work.

1.16 Summary

The chapter summarizes the work on the design and analysis of cloud cryptography by combining blockchain, multi-authority, and Botnet which can have several significant contributions, required technologies, methods, and algorithm procedures. The Existing works and limitations have been proposed, and proposed methods with perfect objectives have been designed with the latest solutions. The next chapter defines the existing works implemented by the different authors.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The cloud storage model plays an essential role in the daily life of business areas during growing internet technology. The cloud storage model plays a significant role and affords more convenience in humans' day-to-day lives because the cloud affords several types of storage services for business persons and enterprise domains for accessing cloud resources and sharing information anywhere. The existing data storage model in the cloud has a single failure mark, and it can be resolved based on a decentralized data storage method so that it obtains more advantages than a centralized scheme [42]. Generally, the decentralized network has more scalability, reliability, and secrecy. In addition, single-point failure is more challenging for a centralized network. The decentralized network is highly utilized for the business model and Bitcoin for overcoming the single point failure, such that this model is fully secured and, thus, enhanced efficiency.

Furthermore, trust and scalability in the data-sharing mechanism are improved. In the decentralized model, the information is accumulated in a single peer, and no user can make any alternations. Moreover, Blockchain is also known as a decentralized structure, so it generates an immutable ledger as a distributed method for recording every transaction [43]. Therefore, cloud computing is the smart structure in contrast to cost and services in cloud computing.

2.2 Classification of several works relating to access control using blockchain

This section delves into access control and privacy-based data sharing and retrieval methodologies within blockchain-based cloud models, offering insights into the diverse approaches adopted in research chapters. Techniques are meticulously analyzed and categorized into ledger-based blockchain methods, encryption-based approaches, smart contract-based models, and Ethereum-based blockchain frameworks. This comprehensive categorization sheds light on the myriad strategies employed for access control and privacy-based data sharing and retrieval schemes. Such exploration underscores the dynamic nature of blockchain technology and its pivotal role in tackling pressing security and privacy concerns within cloud computing, showcasing its ongoing evolution and adaptability.

2.2.1 Blockchain-based ledger-based model

The current work is focused on using blockchain-based ledger technologies to create an emergency access control management system (EACMS) for medical records. This system was put into place by a team under the direction of A.R. Rajput, and it includes several rules governed by smart contracts to deal with emergencies and establish the length of such periods. The Business Network Archive (BNA), which describes the system's capabilities, was created by the architecture using Hyperledger Composer. The smart contracts on the ledger allow data retrieval and authorization verification for any transaction within the system. This architecture ensures that the system for handling health records is effective, safe, and auditable by depending on ledger smart contracts [44].

Qin, X, and associates presented an access control approach based on the blockchain with several attribute authorities for a secure cloud data-sharing architecture. This innovative model addresses the security and privacy challenges associated with cloud data sharing by leveraging decentralized and transparent blockchain technology. In their proposed architecture, the access control model utilizes smart contracts on the blockchain to enforce fine-grained access policies based on the attributes of users and data. Multiple attribute authorities are introduced to manage and validate different characteristics, such as user roles, credentials, or data sensitivity levels. These attribute authorities play a vital role in ensuring access requests align with the predefined policies and criteria [45].

Ali, S. et al. created a blockchain-based decentralized data storage paradigm. Blockchain was used to gather file information, while Distributed Hash Tables (DHT) were used to accumulate actual files at different locations based on a peer-to-peer network [46]. The developed off-chain storage model also achieves high throughput and low latency. This algorithm effectively reduces the project's need for centralized processing, uptime, and accumulating resources.

Thwin's model integrates blockchain to bolster tamper resistance, ensuring data integrity and security. Additionally, cryptographic and proxy re-encryption algorithms safeguard privacy, enhancing user confidentiality. Furthermore, tamper resistance, revocability consent, and audibility improve system performance and reliability. Moreover, the proxy re-encryption model enables secure sharing of decryption capabilities, enhancing security and facilitating collaborative data access [47].

2.3 Encryption-based techniques

A variety of encryption-based techniques for access control and data-sharing processes were looked at in the literature review. Among these, Ma et al. developed an Internet of Things (IoT) paradigm for access control using their technology, which used a fog computing structure, and many blockchains ran in the cloud to provide a cross-domain access mechanism. It was adopted to address the demands for blockchain technology because of its extensibility, fine-grained audibility, decentralization, high scalability, and privacy protection in access control. Multiple authorization assignment nodes and group access models were established. The duration of the dynamic transaction collection varies. This approach effectively enhances system performance and scalability by the network's size [48].

Lin et al. Security and privacy are safeguarded by the attribute signature and message authentication code designed for the blockchain-based system. Attribute signatures and blockchain were integrated to authenticate terminals, gateways, and message authentication codes. Furthermore, the multi-receiver encryption process was used to offer confidentiality. Meanwhile, smart contracts were utilized to ensure scalability, and the request process was done by interaction with smart contracts [49].

Sun, J. and Fang, Y. devised a model to facilitate cross-domain data sharing in electronic health records. This method integrates a cryptographic model to ensure safe data sharing while safeguarding patient privacy. Employing delegation architecture for access control, the strategy combines on-demand revocation and fine-grained access control. Both proxy signature-based and role-based models incorporate the delegation process. A fine-grained access control model was also developed to address more delicate and stringent control requirements [50].

Gao, Het al. Introduced Blockchain-Based Security Sharing technique, termed BSSPD, used to encrypt data sharing and accumulate the data on IPFS for increasing scheme decentralization. Furthermore, the decryption key and address of shared data were encrypted using the CP-ABE model [51]. Here, encryption was performed depending on particular access policies, and the data owner utilized blockchain for publishing information and distributing keys. The ciphertext keyword search model was employed to protect data user privacy during retrieval.

Ma, X et al. Designed an effectual data-sharing approach based on blockchain. At first, the data owner shares the data with multiple users who fulfil the access policies. After that, a searchable encryption approach was employed to solve the complexity of the

cipher text query. Moreover, data sharing was performed without the interaction of data owners with data queries [52]. Here, the CP-ABE algorithm was introduced for the data encryption process. In addition, the CP-ABE approach effectively increases data security during the data-sharing process.

2.3.1 Ethereum-based blockchain approach

This section overviews various research endeavours focusing on Ethereum-based methods for access control and data sharing and retrieval processes.

Dagher, G. et al. introduced a privacy-preserving model for enhancing the interoperability of Electronic Health Records (EHR) using blockchain technology. Advanced cryptographic techniques were employed to bolster security measures, including the accumulation of hashes of data references during the transfer of query link information within a private contract. Additionally, a proxy re-encryption method was utilized to aggregate small encrypted records and store keys on the blockchain, ensuring data confidentiality and integrity. Subsequently, smart contracts were leveraged for access control, facilitating role changes for providers, patients, and third parties on the blockchain. This approach resulted in an elevated level of decentralization, enhancing access control and contributing to a more decentralized system overall. Through dynamic role management, access control was improved, and the system also achieved a higher degree of decentralization, bolstering its resilience and security [53].

Wang, Set, et al. devised a robust sharing mechanism facilitating efficient and secure data sharing among users within a decentralized storage structure. Through smart contracts and access control mechanisms, data owners can precisely define conditions and permissions for sharing their data, thereby enhancing privacy by enabling data sharing on a need-to-know basis with transparent and audible access control. This technique harnesses the Ethereum blockchain, a decentralized storage system like interplanetary files, and Attribute-Based Encryption (ABE) to ensure robust security measures. Furthermore, data owners can allocate secret keys to encrypt shared data and data users based on a signify success policy, enhancing data protection. The implementation includes a keyword search operation on ciphertext within the decentralized storage model via a smart contract on the Ethereum blockchain, effectively addressing cloud server issues. Additionally, it generates an encrypted keyword index for shared files, storing it on the Ethereum blockchain for accessibility and transparency. Following smart contract deployment, accurate search results are retrieved, ensuring efficient data retrieval and security maintenance [54].

2.4 Blockchain techniques based on smart contracts

The following is an explanation of the literature review of previous research projects using blockchain technologies based on smart contracts:

Ali and several others started BACI. This paradigm's creation was driven by IoT models' delegation and access control requirements, which primarily rely on query- and event-based permission allocation. Then, using the blockchain architecture, a decentralized, delegation-based, reliable, secure, and verifiable structure was created. The node with the most minor permission occasionally received the most important and the least permission altogether. The major components of this architecture are an application manager, a smart contract, a user device, an IoT device, a blockchain manager, and a blockchain manager. Access control for a small number of devices is effectively managed by this architecture [55].

A secure and effective solution for data sharing in the IoT ecosystem is provided by Truong et al.'s data-sharing methodology and access control strategy, which depend on IoT smart contracts implemented on the blockchain. The proposed approach improves data security, privacy, and accountability in IoT-based data-sharing contexts by exploiting the decentralized and transparent properties of the blockchain and enforcing access control through smart contracts. This technique was primarily developed to address several issues with trust and authentication for IoT access management. The Judge Contract (JC), the Access Control Contract (ACC), and the Register Contract (RC) were employed in this case to enable efficient access control management. The Register Contract (RC) was utilized to establish user authentication in the system, and the Access Control Contract (ACC) also governs the access system [56]. Additionally, JC identified the offender using a behaviour evaluation methodology. Each subject's penalty was determined after the misbehavior detection process was finished.

Chen, Y. et al. introduced an innovative blockchain-based medical data-sharing model, integrating attribute-enabled access control and privacy safeguards. This approach combines K-anonymity and searchable encryption techniques to enable secure sharing of medical data. Users can search encrypted medical data records using Hyperledger Fabric and consortium blockchains. Attribute-based access control ensures users are granted access based on their attributes [57]. Combining searchable encryption and K-anonymity provides seamless data sharing while preserving privacy. A prototype model was implemented using chain codes within the Hyperledger Fabric framework.

Jaiman, V. and Urovi, V [58], the smart contract represents individual consent for enabling data requesters in this model. Then, the dynamic consent approach was extended by two schemes, such as ADA-M defining the queries from data requests. The Ethereum blockchain was applied, and various data-sharing circumstances were estimated.

Liu Jet al. [59] presented a blockchain-based privacy preserving data sharing model used for EHR electronic medical records, named BPDS. The electronic medical record was also accumulated securely in the cloud, and indexes were reserved in the Interfroof Consortium blockchain. Furthermore, the complexity of medical data leakage was highly decreased, and the indexes of blockchain guarantee that the electronic medical record was modified. Moreover, secure data sharing was automatically accomplished by the smart contract for pre-defined access permission of patients. In addition, a joint design of an access control model and a content extraction signature model was applied to afford privacy preservation in the data-sharing model.

Zhang Y et al. [60] modelled blockchain structure for data sharing with fine-grained structure in IoT. The consensus technique was considered a Byzantine fault tolerance model in the model. Originally, IoT data was encrypted. After that, the smart contract model was incorporated with an attribute encryption model for realizing fine-grained sharing. Moreover, access strategies were placed on the encrypted key, such that the encrypted key was encrypted via attributes to decrypt the cipher text. After that, the smart contract was employed to ensure the scalability of the access control table. Here, every data-sharing request interacted with smart contracts by transactions.

First proposed by Xu, Het al. [61], the hierarchical attribute-based encryption model used the hierarchical attribute model and the multi-level authorization centre. This solution offered flexible and fine-grained access control by assigning user attributes to several authorization centres. After that, this model was integrated with a fabric blockchain approach for resolving the significant decryption cost issues for users in IoT. Additionally, smart contracts in the blockchain performed complicated partial decryption models to decrease user decryption overhead. Here, blockchain was utilized to realize the traceability of historical functions to satisfy data restriction security needs.

Yang C et al. [62] created a blockchain-based access control system that includes privacy security in the cloud systems, dubbed AuthPrivacyChain. Initially, the account number of the node was used to develop the blockchain to ensure uniqueness and limit access control of information, which was encrypted before being stored in the

blockchain. Then, access control process authorization revocation, as well as authorization, was devised. Here, this model was developed depending on the Enterprise Operation System (EOS), and it protects authorized privacy. This approach encrypts and accumulates the blockchain model's access control rights, safeguarding user privacy. Additionally, this model ensures availability, resource accountability, integrity, confidentiality, and resource accountability and resists several internal and external attacks.

A blockchain-enabled concept for data sharing and privacy protection in smart cities called Private Sharing was presented by Makhdoom, I.et. al [63]. The parties in smart contracts were made aware of this algorithm's guarantee of user data confidentiality. Data owners were then encouraged to share their information with stakeholders or third parties. Several requirements are outlined in the EU GDPR, such as accessibility, sharing, and data owner deletion.

Nguyen, D. Cet al. [64] devised a blockchain for electronic health data sharing of mobile cloud-enabled E-health systems. Finally, peer-to-peer IPFS and blockchain were combined for decentralized data sharing and storage. Essential safeguards are included to increase the trustworthiness of blockchains. Following a breach affecting 51% of the transaction ledger, the 51% stage of the attack comprises issues with just violated credibility and a lack of transaction availability. However, residual identity lacks security since it cannot guarantee that the payment information will be erased.

A private PDP program with a Blockchain emphasis was recommended by Huaqun Wang et al. [65]. According to a debate on anonymity, the approach may even detect the customer's security. The certificate authentication procedure must be eliminated. Therefore, the identification-focused PDP algorithm based on blockchain is vital in research. If further strengthening of private keys is needed, examining the constantly evolving keys technology of the blockchain PDP system is essential.

Sujatha et al. [66] introduced CPVPA, a credentials public authentication system designed to address the threat of dozing auditors. In traditional authentication setups, auditors play a vital role in verifying user credentials. However, the risk of a dozing auditor, who may neglect their verification duties, compromises security. CPVPA integrates on-chain blockchain currency into transactions, ensuring auditor-led authentication. Security research confirms CPVPA's efficacy in providing crucial protection compared to existing schemes. Future studies should explore integrating CPVPA with other blockchain technologies.

Jiawen Kang, among others, and ZehuiXiong et al. [67], to study connections within public blockchains that can be verified as evidence of cloud-edge providers and miners-working systems study employed a theoretical framework to play a tri-leader game with three followers. The best results in a distributed system can be achieved mainly using the ADMM method to use miners and sips. Yet we shall strive to enhance the application, e.g., utility definition. The ADMM algorithm cannot be applied easily.

Jamal Bentahar, Mona Taghavi, and others [68], a multi-agent data analysis platform traditional cloud vendor's federations as well as what impact this has on the quality of service. With this proposal, an integrated strategy has been developed in which an oracle functions as a verification agent when the engine matching agents are built using the blockchain to assess the level of the service.

In this chapter, Yinghui Zhang and Robert H. Deng [69] suggested program architecture, philosophy, antagonistic paradigm, design objectives, and specific implementation specifics for BPay. Regarding the issue of activity savings in more nuanced data centre situations, such as transferring blockchain-driven attribute-based health information, our protection report showed that while the hashing is detonation-resistant, BPay achieves objectivity and efficient justice, and ECDSA cannot be accused for data.

Xiaojun Zhang and JieZhao [70] implemented an innovative conditional heritage-preserving health verification system of biomedical data daily for the victims. In fact, with dependent identification, our system retains confidentiality; even the PKG can trace and relinquish the true self of patients misbehaving. The software is much more practical for cloud-based WBANs, having done a comprehensive efficiency review as opposed to current programs.

Bobo Huang, Li Jin, et al. [71] investigated the new model of BaaS bottleneck for the current Bitcoin blockchain. According to our research chapter, the agreement is the challenge in prior crypto-currencies, such as Bitcoin and Ethereum. As one of the pioneering cryptocurrencies, the Bitcoin blockchain has faced its fair share of challenges over the years, with scalability being a prominent issue. Scalability concerns refer to the Blockchain’s ability to handle a growing number of transactions efficiently. These challenges are not unique to Bitcoin but also extend to other cryptocurrencies like Ethereum, which operate on similar principles.

Yuan Zhang, Chunxiang Xu, et al. [72] described a secure and efficient PEKS platform called SEPSE for off-line KGA resistance, where different simultaneous servers were

also used to support keyword encrypted data to free SEPSE from another failure point. On every wide server where protected server manager shares are exchanged annually to bypass the core agreement, SEPSE offers regular renewals. We also indicated SEPSE protection and finalized an output assessment. SEPSE has proven successful regarding networking and transmission costs. The authors would discuss opportunities for improving the stability, efficiency, and accessibility of data outsourcing frameworks for future study.

Yuan Zhang, Chunxiang Xu, et al. [73] discussed the possible consequences of the outsourced responsive tests. Chronos+ is a blockchain-based, safe time-stamping system for cloud data management, in which a web-accessible Chronos+ log repository endorses both management and time-stamping services. More diverse capabilities in Chronos+ need to be analyzed for current projects. Other activities conducted by either cloud vendors or customers on outsourced information, especially in cloud storage systems, need to be time-stamped for comment demand.

Peilong Li, Chen Xu, et al. [74] sought to respond to the challenges encountered by creating SDIs to incorporate technology into regulatory compliance and healthcare applications. Given the significant change in data centres and challenging drive framework, Going well past experiments, our potential study should concentrate on adapting the same example in a natural home environment linked to online networks to an operating CORD system.

According to toRuonan Chen, YannanLi, et al. [75], an external provider blockchain-based storage protocol was portrayed to autonomous vehicles, which allow continuous updating but rather public verification. The multi-replica domain strategy was also used to boost durability by using blockchain. We demonstrate their stability in the random Oracle model and apply the file storage protocols to our protocol.

Mauro Conti, Sandeep Kumar, et al. [76] proposed an external service provider blockchain-based power generation protocol that was portrayed as a new technology that enables efficient updating and public verification. The methodology of multi-replica storage is to boost security, utilizing blockchain to archive all peer-to-peer interactions. Studies showed their security in the adversary model and implemented file storage strategies for our protocols.

Blockchain applications for data storage in P2P networks were pioneered by Simanta Shekhar Sarmah [77]. These applications revolutionize the utilization of computational resources by enabling efficient and secure data storage. Transactions within blockchain

networks utilize two prominent algorithms, namely proof-of-stake and actual evidence-of-job, to ensure the reliability and stability of the system. Currently, extensive research is underway to explore the potential of blockchain applications in cloud storage environments.

According to Hui Huang, Xiaofeng Chen et al. [78], the Cloud infrastructure should be defined as a cloud storage solution that allows payments and services at the edge devices. The cloud user (outsourcer) can download untrusted edge devices (workers) with resource-constrained devices in mobile cloud concepts and pay for the distributed computing tasks. Both new implementations use the standard E-cash methodology to create payment tokens, which need a reputable organization (in this case, a bank) to prevent duplicate spending.

Marie Vasek and Tyler Moore [79] defined the direct damage done as never to be used by the victims, who allowed the passing of money over to the fraudsters. Furthermore, and even more critically, all consumers, even those who are not fraud perpetrators, incur indirect harm. Such harm hurts the reputation of legal practices and the rising confidence of customers, who become more reluctant to pursue new services. The analyst finds that 60 percent of overall sales accounted for a pre-date Bitcoin scam, Bridge HYIPs.

YongYu, YannanLi, et al. [80] defined the IoT in both academia and business to determine the IoT faces of various security bugs, and data security and privacy are increasing in blockchain digital encrypted blockchain, which offers IoT security which may influence several industries such as infrastructure, finance, which trade. Discussed common issues relating to IoT security and safety, put up a program to combine blockchain with IoT, have great faith in IoT data and diverse plug-ins, and offer approval and enticing robustness.

Satoshi Nakamoto [81] did something different and unexpected by organizing an online auction that didn't care much about the people involved. Even though it had the same level of security for ownership, it wasn't very good at ensuring people didn't accidentally pay more than once. To fix this issue, we devised a clever way for people to work together directly. This solution uses proof of work to track how things should work. It helps stop anyone trying to cheat the system by changing how things are calculated. It is important because trust is essential when many different ways of processing things are involved.

Giuseppe Ateniese, Roberto Di Pietro, et al. [82] proposed and developed a step-by-step design of a tested PDP framework that was very lightweight. It exceeds several counts of prior work like overhead duration, data collection, and performance and enables complex research. It is ineffective for identity verification by the public (third party), as it is based on symmetric cryptography. One workable alternative would be a hybrid scheme, which includes our scheme components.

According to David Cash, Alptekin et al. [83], to ensure that evidence is stored correctly and can be recovered from the computer, a client should keep their data on a distant server (such as in the cloud) and periodically conduct an assessment committee process. During an examination procedure, the burden and communication on servers and clients would be considerably lower for output than for reading or transferring the data. All corporate data will be fully aware and able to be sent when the device is required by a request to cover any storage regions.

According to Ayad F. Barsoum and M. Anwar Hasan et al. [84], the CSP provides charged storage capacity on its network to collect customer data. A greater degree of scalability, performance, and robustness is accomplished by replicating data on several computers in separate data centres. The greater the payment customers charge, the more copies the CSP will carry. Customers must then be fully assured that CSP has clearly defined all duplicates of the data consented to in the separate contract and inquires about accessing information gathered from shoppers on all remotely stored copies.

You can also offer an RSA key or trapdoor (let's say, for example, an RSA code) with the group of users and permit them to come back together to determine the encoder with the secure trapdoor technology Suggested [85]. We should know the sizable corpus of distributed signature and RSA key generation chapters for the coding protocol. The optimal method for the mechanism remains for further studies.

Shawn Wilkinson, Tome Boshevski, et al. [86] presented a peer-to-peer FTP server network that utilizes end-to-end encrypted messages, allowing users to access and share the information without depending on third-party service providers. Research teams also discussed issues, including network attacks and parent disconnections, an assessment that continually scans reliability, including thoroughness, and uses identical recurrent versions of encryption. Operating a robust and fault-tolerant system on reputable service suppliers dramatically increases privacy and security.

Shawn Wilkinson, Jim Lowry, et al. [87] have created a theoretical paradigm through which the MetaDisk. Blockchain could serve as the foundation for a software

component. It serves as a peer-to-peer node that runs flexible information technology. We provided a simple introduction to a particular form of data network, but on the Store platform, we left unanswered concerns regarding conflict settlement, session hijacking, and security models.

Here, Ralph C. Merkle [88] has provided a list of several verification methods. Although they are not the only feasible, they are crucial tools for device design engineering since they show what is possible and provide workable answers to common issues. Modern protocols that use various Shared Key features in blockchain systems are being developed.

Xiwei Xu, Cesare Pautasso, et al. [89] addressed their experiences with the blockchain. The blockchain provides synchronization and networking services via transactions, security oracles, and cryptographic protocols, as well as particular facilitation capabilities such as permit management, safe cryptographic transfer, merchant services, mining, and incentives, which contrast the blockchain with related network nodes such as shared data store modifying state machine. We also perfected critical design decisions that rely on the project's practical expertise, suggested by integrating a blockchain into the layout.

Blockchains' use in creating a new decentralized digital computer network has been studied as a possibility by Doriane Perard, Lucas Gicquel, and many others [90]. The initialization for the device day-audits and closing of the device comprises the three primary parts of the Blockhouses method. The company focuses on proof of retrievability that authenticates communication, allowing contracts to ensure that the server protects the data. The main problem that the network faces could be that its dimensions are so large that it's challenging to manage. Erasure codes help solve the problem by stopping production.

Shrestha created a new blockchain model, A. et al. [91]. Blockchain technology is utilized to facilitate user modeling. Blockchain technology enables people to share information without giving up any control or ownership of the data. Here, user data from the repository was converted into an open data structure via a shared stream onto the blockchain, allowing other nodes to process and use the data. The addition of smart contracts allows for the verification and execution of data agreements and the conversion of digital tokens into user incentives. Smart contracts also carry out a twofold deposit security procedure to ensure privacy.

Guo Y et al. [92] introduced a blockchain-based structure for secure and reliable data sharing in distributed systems. Data owners permit outsourcing their data to the distributed model in an encrypted structure. The data owner allocates the secret key for authorized users without an extra round interface for creating acceptable search tokens by influencing blockchain smart contracts. In addition, this approach effectively resolves the trust problems of query authorization. Finally, a secure local index structure was designed to support encrypted keyword search and forward privacy, and blockhead overhead was moderated.

2.5 Other access and data sharing techniques

This section presents the various other access control and data sharing and retrieval methods for blockchain-enabled cloud techniques, which are explained as follows:

Ding et al. [93] presented a novel attribute-based access control approach for the Internet of Things structure. In this method, blockchain methodology was employed for recording attribute allocation to avoid lightweight computation and better effectiveness for the IoT model. This model simplified the access control structure and two parties by hash functions and signatures. A few consortium nodes were utilized here to construct this system and resist several attacks.

Ouaddah et al. [94] devised a privacy-preserving access control method using blockchain technology in the Internet of Things. Here, a new decentralized pseudonymous and privacy-preserving authorization management model exists for controlling the constancy of blockchain and access control of controlled devices. Moreover, authorization tokens were selected as an access control model delivered by an emergency cryptocurrency solution.

Liu X. et al. [95] developed a blockchain-based medical data sharing and protection paradigm to enhance the electronic health system. At first, several security properties were satisfied, including openness, decentralization, and tamper resistance. A reliable model was also generated for accumulating medical data and accessing historical data while considering privacy preservation. After that, the symptom matching model was provided among each patient, which permits the conduct of mutual authentication and production session keys. Besides, an enhanced consensus model was included by enhancing conventional delegated proof of stake, which was more reliable, secure, and proficient.

Eltayieb Net al. [96] enabled the encryption model for safe data sharing in the cloud model. This approach satisfies various security needs of cloud computing, including enforceability and confidentiality. Additionally, smart contracts were introduced in this technique for solving cloud storage issues. Here, this algorithm was integrated with the benefits of encryption and signature for obtaining confidentiality. This algorithm mainly depends on an access structure tree for enforcing user access policy in various functions, like encryption and decryption.

Zheng, X et al. [97] modelled blockchain-based personal health care data distribution in the cloud as a theoretical framework for securely and openly distributing private continuous dynamic health data among individuals. In addition, a data quality inspection approach using machine learning approaches was employed to control data quality. The General Data Protection Regulation (GDPR) manner was developed to enable users to share health data securely. In addition, high-quality personal health data was gathered for the data-sharing process. Then, various solutions were employed for sharing massive dimensional incessant dynamic data hast pointers for the storage location. After that, there are restrictions on continuous dynamic health data by incorporating cloud storage and blockchain. The massive dimension of health regarding data was accumulated in an encrypted format on the cloud. Then, the data quality validation model was considered in this model for controlling data quality in both software and hardware by machine learning models.

Zhang, Z et al. [98] designed the new position verification model, Ears, to prevent lengthening and shortening distance fraud. Furthermore, it can tolerate the lengthening distance attack. In addition, Ears were included on a higher network layer of wireless communication, the existing Distance-Bounding Protocol (DBP). This approach effectively avoids strict time synchronization.

Zhang, X et al. [99] This approach enables the user to authorize and assist in managing complicated encrypted diagnostic data-sharing processes. In addition, the data-sharing method was performed utilizing an enabled encryption model with a keyword search process. Meanwhile, patients can recover medical data by submitting the trapdoor of related keywords. Besides the security system for cipher text authorization, enforceability and trapdoor privacy were considered for the data sharing.

Sundareswaran et al. [100] modelled a novel, highly decentralized information accountability structure for data sharing in the cloud. Here, an object-centred model was developed, which enables the closing logging model with user data. The Java Archives

(JAR) file was included for generating travelling and dynamic objects and guarantees access to user data. In addition, a distributed auditing model was implemented to strengthen user control. This model was highly decentralized and platform independent, without a dedicated storage system. The log record structure was updated to provide more authenticity and integrity assurance.

Liu, X et al. [101], the approved users were directly decrypting the data files without communicating with data owners. In this technique, encryption computation and storage overhead were independent of the quantity of revoked users. Moreover, user revocation was obtained by revocation loss exclusive of updating secret keys of residual users. Furthermore, privacy preservation and secure access control to the user were afforded, assuring any group member to use cloud resources.

Wu et al. [102] presented a systematic access control approach to secure electronic health data sharing in the cloud. This approach effectively supports the selective sharing technique for composite electronic health records. In addition, privacy concerns were accommodated to process the access request in healthcare data to ensure privacy. The comprehensive access control model was applied to assist the selective sharing of compound electronic health data from numerous healthcare providers in the cloud. The electronic health data model and the cross-domain aggregation method were developed for access control. Finally, a proof of concept model was employed in the cloud structure.

Shen J et al. [103] devised a blockchain-based key agreement for group data sharing in a cloud structure. The group data-sharing process was introduced using the symmetric balanced incomplete block design (SBIBD), which was employed to identify participant communication. Moreover, this model executes fault detection to ensure a general conference key for every participant. After that, the volunteer replaced malicious participants to support fault tolerance properties in the fault detection stage. Besides, volunteers enable the system to resist various vital attacks.

Wei, G. et al. [104], through proxy re-encryption, a cloud computing Efficient, Flexible, and Anonymous Data Sharing Model (EFADS) is described. The system and algorithm levels are this methodology's two key phases. These models efficiently represent the four system setup, upload, user grant, and download stages. The data files were encrypted using symmetric key encryption, and the primary keys were directly encoded using proxy re-encryption architecture.

Chu, C.K. et al. [105] developed a key aggregate cryptosystem for a scalable data-sharing process. The public key cryptosystem was developed, which creates constant-size cipher text for any group of cipher text. Here, various groups of secret keys were gathered as a single key. Moreover, the private key owner can discharge the continual size aggregate key used for flexible selections of cipher text groups in the cloud. Furthermore, the condensed, collected key was quickly transferred to other accumulated smart cards with restricted secure storage.

Xia, Q.I et al. [106] introduced a trust-less structure for medical data sharing through the MeDShare model. This model offers improved auditing, data provenance, and control in sharing medical data within a cloud environment. The primary focus of this approach is to identify and prevent evil utilization of the data by entities accessing it through a custodian model. The MeDShare model ensures the transparency and integrity of the data-sharing process by recording all data transitions and sharing activities in a tamper-proof manner. This recording mechanism serves as an immutable record of the entire task, providing a reliable source of information for auditing purposes.

2.6 Research gaps

1) According to the various authors' contributions and research, the blockchain still has different security breaches due to the lack of trust. Generally, the cloud system is organized with various auditing and assessment tools to audit the various kinds of data, but unauthorized users are still stealing data.

2) The role-based access control system defined an attribute-based hierarchical system to determine accessibility by combining the cryptography techniques. The computation of the cryptography hash function needs a different attribute set, which leads to a more complicated computation problem.

3) They break down exclusively crude data, or, in other words, data should be dissected at a few layers. The data broke down at the lowest layer overburdens cloud security frameworks, overpowers human chiefs, and may not contain enough proof about the expectations of an aggressor.

4) Existing security systems can't socially dissect data. Fundamentally, data about the connections of occasions is not accessible at prediction time.

In [92], the development of EACMS for access control in blockchain systems represents a notable effort. However, it is observed that this model failed to yield substantial improvements in system performance while maintaining simplicity. It suggests a gap in

optimizing access control mechanisms within blockchain systems, particularly balancing performance enhancements with complexity. Similarly, in [75], an approach integrating blockchain-enabled access control with multiple attribute authorities was proposed for a secure cloud data-sharing model. Despite its aim to enhance security, the algorithm encountered difficulties in effectively balancing efficiency and security considerations. It highlights a significant research gap concerning developing access control mechanisms to manage multi-authority environments while maintaining robust security measures efficiently.

Furthermore, introducing a blockchain-based decentralized data storage approach in [81] represents a step forward in addressing data management challenges. However, the identified gap lies in the model's inability to consistently maintain the required Quality-of-Service (quality of service) standards. It underscores the need for novel strategies and protocols that can ensure reliable quality of service levels in decentralized data storage environments leveraging blockchain technology. Therefore, while existing literature has made strides in exploring access control and data-sharing techniques within blockchain-based systems, there remains a clear need for further research to address the identified gaps. Future endeavours should focus on refining access control mechanisms to optimize performance, enhancing the efficiency-security balance in multi-authority environments, and devising strategies to consistently uphold the quality of service standards in decentralized data storage systems.

2.6.1 The challenges experienced by existing encryption-based methods are illustrated below:

In [8], BDKMA was devised for access control in the IoT structure. However, this approach was not discovered, and a feedback model was developed for Security Access Managers (SAMs) and cloud managers to assist the persistence of blockchain-based IoT. The BSeIn model was designed in [62] for a fine-grained access control model, although this model has not estimated the performance based on collaboration and hardware implementation. The cross-domain data sharing model was developed in [86], although this model failed to identify the attacks for ensuring resilience. In [88], BSSPD was created for the fine-grained access control process, even though an effective ciphertext searchable approach was not included for optimizing this system. A blockchain-based data-sharing algorithm was developed in [90], but this model still failed to decrease time complexity during crucial generation, matching, encryption, and decryption processes. The blockchain-driven access control model was devised in [87]

to preserve personal health record system privacy. This model effectively reduced the computational cost of the system, although it failed to reduce the time complexity.

The challenges faced by Ethereum-based blockchain techniques are explained as follows. The privacy-preserving approach for interoperability of EHR utilizing blockchain structure was developed in [61]. However, this method failed to meet the legislative standards in medical data for improved performance. The decentralized storage model's data storage and sharing technique was introduced in [37]. However, this model did not implement user attribute revocation functions and access policy updates for enhanced performance. The blockchain structure for data sharing with the fine-grained model in IoT is devised in [69]. However, this model does not include encryption algorithms for better performance. In [70], a blockchain-based data security sharing approach with fine-grained access control was designed, but the polynomial time of this model was not improved. In [40], the AuthPrivacyChain model was introduced, even though the processing time of this model was not reduced. In [73], the Privy Sharing technique was designed, although this model did not include a fog system for a secure combination of IoT devices with a blockchain structure. The blockchain model was designed for electronic health data sharing of mobile cloud-based E-health systems [76]. However, this approach did not obtain better performance with less complexity.

In [34], an attribute-based access control approach for IoT was introduced; however, it encountered challenges due to the lack of integration with a consensus algorithm, which is essential for ensuring efficient performance in dynamic IoT environments. Despite the potential benefits of attribute-based access control in enhancing the security and granularity of access policies, the absence of a consensus mechanism limits its applicability in large-scale IoT deployments where real-time decision-making is crucial.

The privacy-preserving access control approach utilizing blockchain in IoT, as proposed in [32], faced limitations in its implementation. While leveraging blockchain technology for preserving privacy in IoT data sharing is promising, the model's failure to incorporate the Raspberry IoT device and utilize the Bitcoin blockchain structure hindered its potential for achieving better performance and scalability. Integrating these components could have enhanced the efficiency and robustness of the access control system, ensuring secure and seamless communication in IoT environments while preserving user privacy. Thus, addressing these challenges is essential for realizing the full potential of blockchain-enabled access control and data sharing in IoT ecosystems.

While the blockchain-based attribute-enabled encryption technique proposed in [72] aimed to enhance data-sharing security within cloud infrastructures, it faced limitations in integrating with smart contracts on Ethereum, hindering its performance optimization potential. Similarly, the blockchain-based method for distributing personal healthcare data, as presented in [54], failed to effectively reduce computational complexity, highlighting the need for further refinement to streamline data processing within healthcare systems. Furthermore, despite the introduction of a secure and location-sensitive data-sharing algorithm for cloud systems [77], challenges persisted in reducing time complexity, underscoring the importance of addressing efficiency concerns alongside security measures.

Moreover, in [78], an identity-driven, authorized, encrypted diagnostic data-sharing approach was proposed; however, it overlooked the incorporation of a mobile-assisted health system, which could have bolstered both security and performance aspects. Additionally, [79] introduced a novel and highly decentralized information accountability structure for cloud data sharing, offering a promising model for the autonomous defence of shared content. Nevertheless, its incomplete implementation suggests the need for further development to realize its potential benefits fully. Lastly, [80] developed the Mona model for dynamic cloud groups yet struggled to ensure adequate confidentiality, indicating the ongoing challenge of balancing flexibility and security in cloud environments.

Table 2.1: Work comparisons based on methodology and Limitations

References	Methodology	Algorithms	Limitations
[44]	Develop an emergency access control and management system (EACMS) using blockchain technology.	Hyperledger Composer	This model leverages smart contracts within the ledger, ensuring efficiency, security, and audibility. Smart contracts automatically enforce access control, privacy policies, and transaction validation, enhancing data sharing effectiveness and system integrity.

[45]	Establishing trust between multiple parties and developing smart contracts for estimating tokens for attributes, decreasing computation and communication overhead for data users.	Secret Sharing and Hyperledger Fabric	The model assists in recording the access control method, but scalability and efficiency in larger networks may pose challenges.
[46]	Devised blockchain-based decentralized data storage model.	Distributed Hash Tables (DHT), an off-chain storage model,	The proxy re-encryption model enables users to share their decryption abilities with others for security purposes. However, managing complex access controls can be challenging.
[48]	Access control standards should be audibility, decentralized, highly scalable, and privacy-preserving. Additionally, system expansion was supported by developing system operation models, different authorization assignment nodes, and group access models.	Blockchain-based Distributed Key Management Architecture (BDKMA)	Scalability concerning network size: The system experiences a 25% increase in latency and a 15% drop in throughput when network size doubles, impacting overall system efficiency and responsiveness.
[50]	A cryptographic model was included to secure data sharing and patient data privacy.	Integrates fine-grained access control, on-demand revocation, and access control	Stringent control needs may limit flexibility and adaptability: Implementing fine-grained access controls and on-demand revocation incurs a 20% increase in management overhead, potentially limiting the system's ability to adapt to new requirements or integrate with other systems.
[51]	The data on IPFS for increasing scheme decentralization, decryption key, and address of shared data was encrypted using the CP-ABE model.	Blockchain-Based Security Sharing technique, termed BSSPD	Preserving user data privacy during data retrieval: Ensuring user privacy during data retrieval increases processing time by 30% and requires additional computational resources, leading to potential performance bottlenecks.

[52]	An encryption approach was employed to solve the complexity of the cipher text query.	CP-ABE algorithm	Data security and data sharing process complexities: The complexity of encrypting and querying ciphertext results in a 40% increase in query processing time and a 25% reduction in system throughput, making real-time data access challenging.
[53]	Cipher text of the decentralized storage model was applied using a smart contract on the Ethereum blockchain, encrypted keyword index.	Attribute-Based Encryption (ABE)	Smart contract retrieves the accurate search result, but efficient keyword search and indexing can be challenging: Encrypted keyword indexes lead to a 35% increase in search latency and a 20% rise in computational overhead, affecting search performance and efficiency.

2.7 Summary

The existing research works related to access control and data sharing for blockchain-driven cloud techniques are explained in this chapter. The various methods implemented for efficient access control and data sharing models are categorized into four categories: ledger-based blockchain techniques, encryption-based approach, smart contract-based blockchain model, and Ethereum-based blockchain, which are elaborated in the above section. Furthermore, the above sections also include the research gap and issues experienced in access control and data sharing for blockchain-enabled cloud techniques.

CHAPTER 3
Study and Analysis of Cryptocurrency Architecture

3.1 Introduction

As technology has advanced, businesses have begun to digitalize various aspects of their operations. The dangerous environment for cyber-attacks is evolving quickly. Because there aren't practical measurements, methods, or frameworks to describe and assess the damage that cyber-attacks bring to industries, it's impossible to predict what could happen due to these assaults. IoT cyber-attacks have been around for a while; however, since IoT has become a part of our everyday lives and communities, it's essential to consider cyber security as a serious matter. Thus, there is an urgent need to safeguard IoT, necessitating a thorough understanding of the warning signs and threats against IoT infrastructure. The study's primary goals are to examine how cyber-attacks affect the general cyber framework and assess the strengths and safety of the blockchain cryptocurrency architecture. It provides the quality assurance of cloud service providers, which use computing resources shared by the Internet of Things (IoT) and is currently experiencing rapid expansion. The ability to provide certain services has made it the most rapidly developing technology that significantly impacts both the commercial and social spheres. They are a part of every aspect of our modern living, such as education, health, and businesses. It includes gathering private information on individuals and organizations and developing products, financial transactions, and marketing. As a result of the increasing demands connected to applications worldwide, the comprehensive creation of related devices inside the Internet of Things has started to set high standards for adequate security [107]. Every day, there are more dangers, and the extent and sophistication of the assaults are growing. The expanding scale of the network and the number of possible attackers make it impractical. However, the tools at the disposal of prospective attackers have likewise improved in sophistication, effectiveness, and strength [108]. The Internet of Things must thus be protected against threats and vulnerabilities to realize its full potential. Security has been defined as preventing physical injury, unauthorized access, theft, or loss of an object by preserving strict confidentiality and integrity of the item's facts and proving those facts at any moment it is essential.

The word cryptocurrency is now widely used in academic and commercial contexts. Bitcoin, a leading cryptocurrency with high capital market compliance, generated $10 billion in 2016 [109]. Formality introduces a novel approach to enhance the integrity

and reliability of digital records. This innovative data storage solution leverages blockchain technology and immutable data structures, such as Merkle trees or content-addressable storage. The blockchain initially presented in 2008 and implemented in 2009, is the primary generation used to create Bitcoin [110]. The block list of the blockchain contains all authorized transactions, which might exist as a public record. As more blocks are continuously added to it, this category is expanding. Distributed consensus techniques and asymmetric encryption have been used for user security and public ledger interoperability. The crucial characteristics of decentralization, resolution, anonymity, and audibility are usually present in the blockchain era. These developments will dramatically reduce transaction costs and boost the efficiency of the blockchain.

The potential applications of blockchain extend beyond finance, with the technology poised to revolutionize various industries such as transportation, online transactions, and virtual property management. By leveraging smart contracts, harnessing the capabilities of the Internet of Things (IoT), and facilitating public contributions, blockchain stands to enhance transparency, efficiency, and security across diverse domains. Its decentralized nature and cryptographic features offer innovative solutions to longstanding challenges, paving the way for transformative advancements in sectors ranging from supply chain management to healthcare and beyond [111].

Once the transaction is carried out on the blockchain, it may be completed utilizing automated miners for smart contracts. Blockchain technology can significantly enhance specific Internet networks but is subject to several complex technological limitations. Scalability is a significant difficulty to start. The capacity of a Bitcoin block has been reduced to no more than 1 megabyte. The block is mined every 10-15 minutes or more. The Bitcoin network can process seven transactions simultaneously following an hour's worth of charge; therefore, it cannot manage frequent, excessive trading. More excellent blocks, on the other hand, suggest a more significant storage space and a slower network spread [112].

As the evolution of blockchain technology continues at a rapid pace, achieving a delicate equilibrium between robust security protocols and optimal block length becomes increasingly critical. Adaptable adjustments are essential to sustain network performance while effectively countering emerging threats. Additionally, the proliferation of self-serving mining tactics within the mining community underscores the persistent requirement for diligent monitoring and governance of blockchain operations. To fortify the resilience of the blockchain ecosystem and in still trust among

stakeholders, proactive initiatives to mitigate these challenges are indispensable. By proactively addressing these issues, we can propel the technology forward, fostering its widespread adoption across diverse industries and ensuring its sustained progress.

ARCHITECTURE PROPOSED FOR BLOCKCHAIN

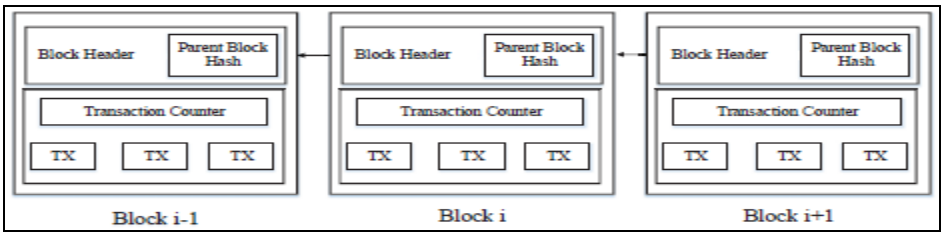


Figure.3.1 A good instance of Blockchain is an ongoing sequence of blocks.

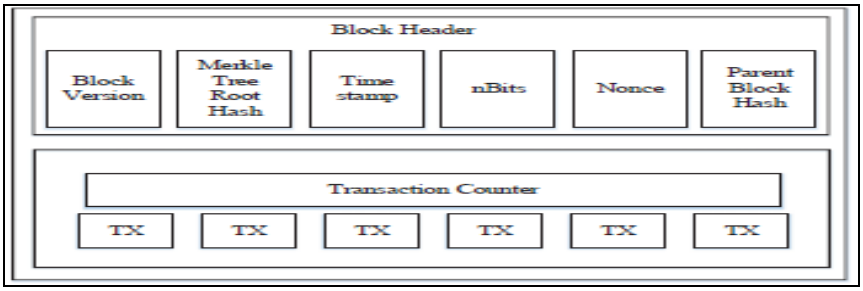


Figure.3.2 Block structure

A blockchain serves as a conventional public ledger, resembling a sequential collection of blocks, meticulously recording a comprehensive history of transactions. As illustrated in Figure 3.2, a blockchain in action is a testament to its sequential structure, where each block's header contains a cryptographic hash identical to that of the preceding block, cementing its connection in a continuous chain. However, it's worth noting that within the Ethereum blockchain, you may also encounter hashes from uncle blocks, descendants of the ancestor blocks associated with the main chain. These nuances in blockchain architecture underscore the sophistication and versatility of these distributed ledgers in accommodating various data structures and maintaining the integrity of the transaction history.

The following is a summary of these chapters' significant contributions:

a) To show safety, we advise using a distributed consensus process based on Proof of Authority (PoA).

b) For more reliable and secure cloud storage for individuals or businesses, we suggested a distributed cloud storage system based on blockchain technology.

c) In cloud-based distributed storage, we utilize a genetic algorithm to detect the replicating of a file that affects multiple users and data centres.

3.2. Types of Cyberattacks in cloud cryptography

The majority of vulnerabilities and flaws discovered in the fundamental structural components of the cloud are often produced by cyber assaults in cloud computing. These flaws and openings have drawn interest from various attack profiles, from APT to script kiddies. Many cloud systems have had several hacks that use flaws with cloud extensions and incorrect settings in the cloud extension based on the design samples. Each of these attacks violates, at the very least, one of the fundamentals of the Trinity doctrines of the CIA. The majority of assaults target cloud components that are located in a specific layer or that span many tiers. As a result, the assaults we evaluate moving forward are multi-stage attacks inside and across layers. They increase the assault using a kind of pivot node bye. A particular assault has a different goal than the alternative.

The following list includes a variety of cyber-attacks related to cloud cryptography.

a) Hyper-jacking: A hypervisor that generates a virtual environment within a virtual machine (VM) host is subjected to an attack in which a hacker seizes control maliciously.

b) Sincere yet Inquisitive Server: Cloud servers are honest but weird; they will conduct searches faithfully while deducing and analyzing encrypted data based on the supplied logs and looking for traps.

c) Link Aggregation Attack (DoS type attack): A denial of service (DoS) incident is a cyber attack in the world of computing in which the attacker attempts to prevent an item or community service from being accessed by the supposed users by quickly or permanently turning off services for the Internet-connected entity.

d) Sidechain assessment: The primary issue with cloud computing is the side channels created by shared resident virtual machines or processes on shared computers. Most cloud proof-of-concept channel assaults deduce strategies based on changes to shared device caches.

e) Attack on Network during VM Migration: A relay attack occurs while a virtual machine moves from one location to another. The kinetics of virtual simulation are being taken advantage of in this assault. Due to the smooth movement of VM images between physical machines across a network, stores often migrate VMs to different places, mainly depending on their consumption.

f) VM Escape Attack: A network attack during the migration of a virtual machine from one location to another. The kinetics of virtual simulation are being taken advantage of

in this assault. Due to the smooth movement of VM images between physical machines across a network, stores often migrate VMs to different places, mainly depending on their consumption.

g) MITC Attack: MITC attacks provide hackers access to data and files in well-known file sync services like Google Drive. Hackers can steal data and interfere with users' acceptance of fully used Google storage.

h) XML - HTTP DOS: XML DoS attacks are very asymmetric: the attacker wants to use a tiny amount of processing power or bandwidth more manually to preserve the attack payload.

3.3 Various Shortcomings in Cryptocurrency

The following list of crypto currency's drawbacks is provided.

a) Scalability

The volume concerns that might occur are perhaps the most significant problems with cryptocurrency. The volumes of transactions that come in every day that are so expensive that they need a VISA are dwarfed by the wide variety and popularity of virtual currencies, which is surprisingly growing. Additionally, unless the infrastructure that supports this technology is considerably extended, cryptocurrencies cannot compete with businesses like VISA and MasterCard in the same market for transaction rates.

b) Cybersecurity concerns

Cryptocurrencies may pose a risk for cybersecurity breaches due to their virtual nature and vulnerability to hacking, as demonstrated by ICOs compromised this past summer alone, resulting in substantial losses for customers totalling tens of millions of dollars and a $473 million loss overall. Maintaining a robust security architecture could be imperative to mitigate these risks. However, numerous entities are already taking proactive measures, swiftly implementing more secure cybersecurity software compared to traditional banks.

c) Price swings and a lack of intrinsic value

Buffett highlighted price volatility as a critical concern in cryptocurrency, attributing it to the lack of intrinsic value. Addressing this issue could involve tethering the currency's value to tangible or intangible assets, as some recent players have attempted with energy futures or diamonds. A higher adoption rate could bolster consumer confidence and mitigate fluctuation risks.

d) High volatility and the possibility of substantial losses

Over the past five years, the monthly volatility of Bitcoin's price in US dollars has been determined to be 90%, contrasting significantly with the annual rates of 15.3% for S&P Gold and 13.4% for the S&P 500. Examining the diverse returns offers a clearer insight into the magnitude of fluctuation experienced by Bitcoin investors. Notably, within the sixty months leading up to December 31, 2020, Bitcoin has shown monthly returns ranging from a high of 76.1% to a low of -37.6%.

e) An infinite potential supply

Even while the total amount of bitcoins that may be created will eventually be limited to 21 million, following a predetermined supply as stated in its protocol, the state of affairs at the moment indicates that new cryptocurrencies are being created constantly. The market's dynamic nature, where creativity and innovation continue to produce a wide range of digital assets, is highlighted by this proliferation of digital assets. As a result, it looks like there will always be a supply of cryptocurrencies—no end in sight. The continuous growth of this ecosystem not only showcases the adaptability of blockchain technology but also poses potential advantages and difficulties for regulators, developers, and investors navigating it. It also emphasizes the necessity of flexible tactics and close supervision to traverse the constantly shifting terrain of cryptocurrencies successfully.

f) Limited acceptance and poor storage of value

While Bitcoin and others are covered with various fee structures, there are still relatively few locations where you can exchange cryptocurrencies for genuine goods or services. For similar reasons, cryptocurrencies are a lousy store of value due to their intrinsic volatility. The pricing of cryptocurrencies will change significantly when translated into a base currency for a person, even within the day.

g) Unsupported and unregulated

Cryptocurrency, renowned for its decentralized nature and empowerment of individuals, faces scrutiny due to findings from a 2019 academic study revealing that 46% of Bitcoin transactions were linked to criminal activities. This revelation has raised investor apprehension, with 25% expressing genuine concerns about crypto's association with illicit practices. Hence, there's increasing demand for robust regulatory frameworks and enhanced security measures in the cryptocurrency sector to tackle these issues effectively.

3.4 Methodology

Consensus Method for Proof of Authority

A consensus technique known as Proof of Authority (PoA) primarily focuses on the reputation or trustworthiness of affiliated parties within a blockchain network. It is a novel approach to implementing consensus algorithms that offer excellent efficiency and fault tolerance. In PoA, nodes that have established their authority are granted the privilege of generating new blocks. A node must first undergo pre-authentication to attain this authority and receive sufficient validations to add additional blocks.

PoA is an established set of rules for blockchain consensus that provides an efficient and effective solution for protecting information on blockchain networks. By personally authenticating nodes configured to be trusted, the PoA method exploits the value of identities to impose security. The Proof of Authority, a set of rules, is surprisingly scalable since it uses a variety of block validators—preapproved peers who serve as device administrators may inspect blocks and transactions. Organizations may use blockchain technology while maintaining their privacy thanks to the proof of authority approach. Microsoft Azure is one situation where PoA is employed. The Azure platform offers private blockchain network solutions without using ether as a local currency fuel because it has no mining needs. Smart contracts on the blockchain are pieces of code or software managed by a peer-to-peer network of computers. Using smart contracts, human rights monitoring teams can coordinate and uphold agreements amongst community members without using traditional criminal contracts. They can create agreements between parties, corporate policies, or simple tokens. Smart contracts are a boundary between public and private within the blockchain in the context of the technology. They can operate as an unchanging component and be able to accept transactions or make them executable under a variety of circumstances (transactions may be denied or require a particular input to perform the intended purpose). Smart contracts are made.

The Proof of Authority protocol is based on the Proof of Stake and Proof of Work security protocols, comprising the decentralized cryptocurrency network. Proof-of-work protocols give decision-making ability to individuals who perform computing functions. In contrast, completely Proof-of-Stake-based protocols grant the authority to make choices for entities that are parts of the system.

Governance is a group of N trustworthy nodes built on PoA methods. Each authority is uniquely identified and most considered reliable, especially if N = 2 + 1. The decision is made by the authorities to direct clients to do outbound transactions. The mining rotation scheme, a popular method of distributing responsibility for the appearance of blocks across authorities, provides the foundation for the agreement on activity program algorithms. The period is broken up into stages, and the mining leader for each step is a professional.

Gavin Wood, a co-founder of Ethereum and a former CTO, assisted in its development in 2017. It is an environmentally friendly method for personal blockchains. Auditors gamble on their identities and reputations, not assets, using the PoA consensus system, and their decisions are founded on the costs of identities among the group and other devices. In the end, the validation nodes of PoA Blockchain networks may be accessible to select as reliable instances.

Since a group of accepted community members verifies transactions, The PoA consensus rules can be used to verify packets comprising exchange networks and delivery chains because the nodes' identities will be considered while using the rules.

3.4.1 PoA consensus algorithm

Step 1: Every miner attempts to generate an unfilled block header at the beginning by using the hash power here.

Step 2: If the miner can make blocks with no information, this occurs when the hash value for the block's header is less than her target difficulty.

Step 3: All network nodes consider the block header's hash a trustworthy information source. N random stakeholder.

Step 4: The miner aired an empty block header, and each stakeholder on the internet can confirm that the header is authentic. This implies that it has the prior block's hash and matches the current difficulty level.

Step 5: The block is acknowledged as a valid component of the blockchain when the Nth stakeholder has communicated the block wrap to the network, and all other nodes accept that it is an exemplary block following the preceding procedure.

Step 6: the mining company and the lucky stakeholders divided the transaction fees for the stakeholder who earned the number N.

Because network nodes are pre-authenticated, block generation rights are granted to nodes capable of surviving DoS attacks. PoA system allows users to defend against attacks.

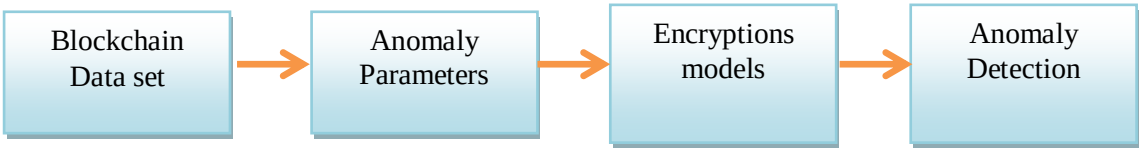


Figure 3.1: Work Flow Diagram

3.4.2 Use of Cryptography in Blockchain

Asymmetric key algorithms, hash functions, and encryption techniques are integral to blockchain technology. They ensure data integrity, confidentiality, and authentication within the network. Hash functions, including the widely used SHA-256 algorithm, enable participants to consistently view and validate the blockchain. These cryptographic mechanisms collectively contribute to the security and reliability of blockchain networks.

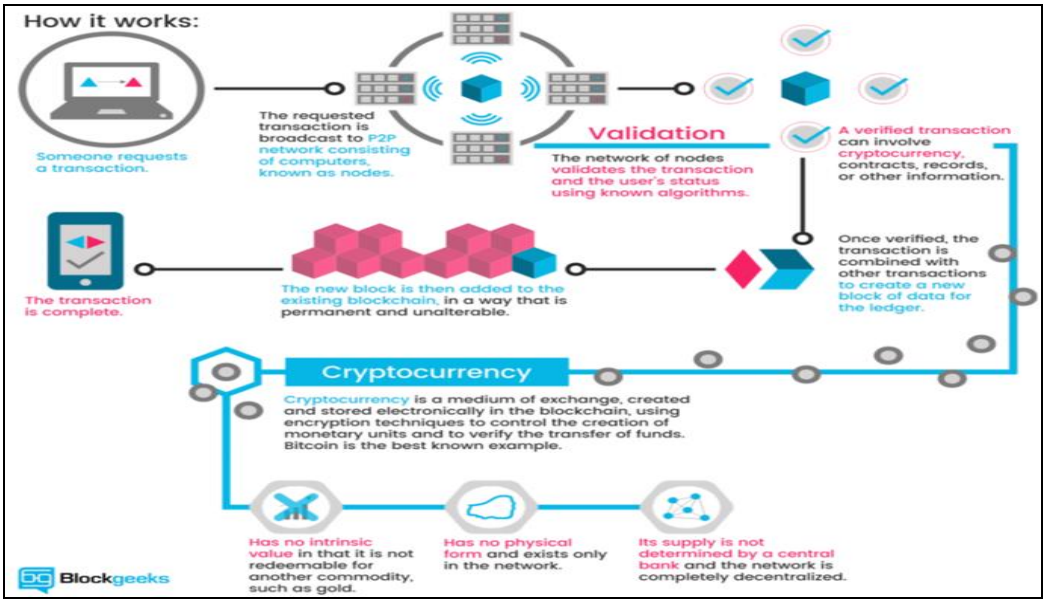


Figure 3.2 Architecture of cryptocurrency

3.5 Results and Discussions

Our goal in this part is to investigate the prior method used to detect cyberattacks on blockchain incursion. Experiments are carried out on the previously proposed recurrent neural network (RNN) based on deep learning using Python programming. Here, the Windows operating system is utilized with the Python 3.7 version, and many libraries,

including Numpy, Pandas, and Matplotlib, are imported. We must direct the interpreter toward our Python code to execute a script.

The KDD dataset, consisting of five rows and 42 columns and coming in the .csv form, has been used to evaluate the effectiveness of the method used during this research.

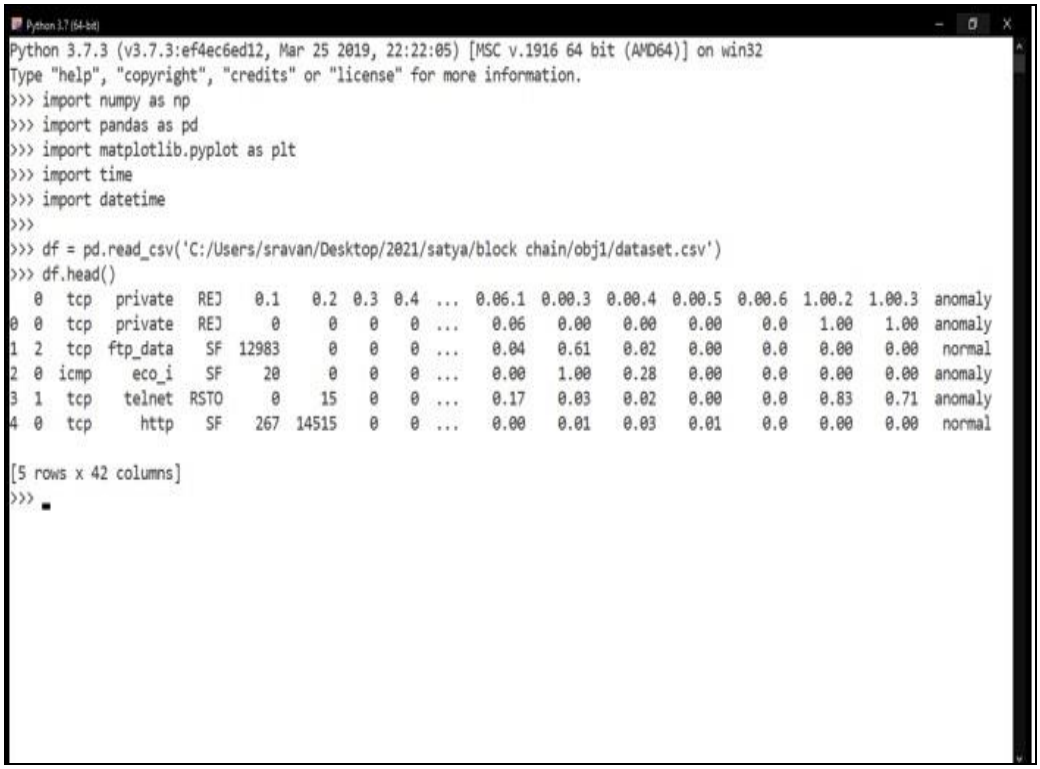


Figure 3.3 Detecting blockchain intrusion cyberattacks using the earlier RNN approach.

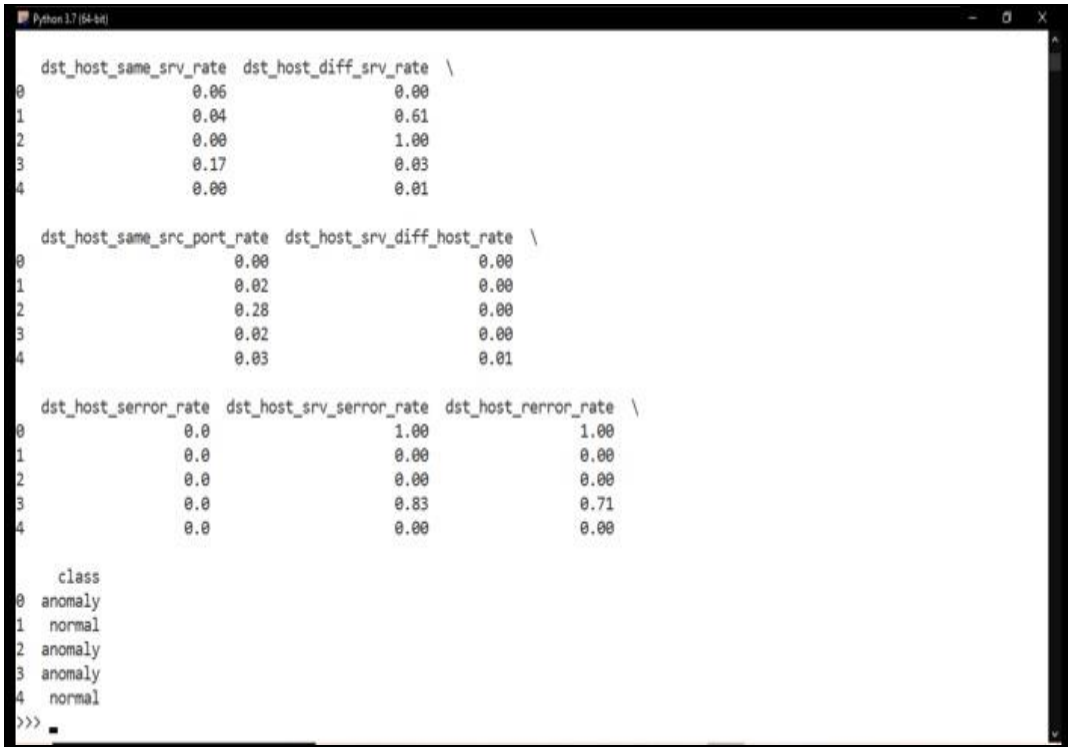
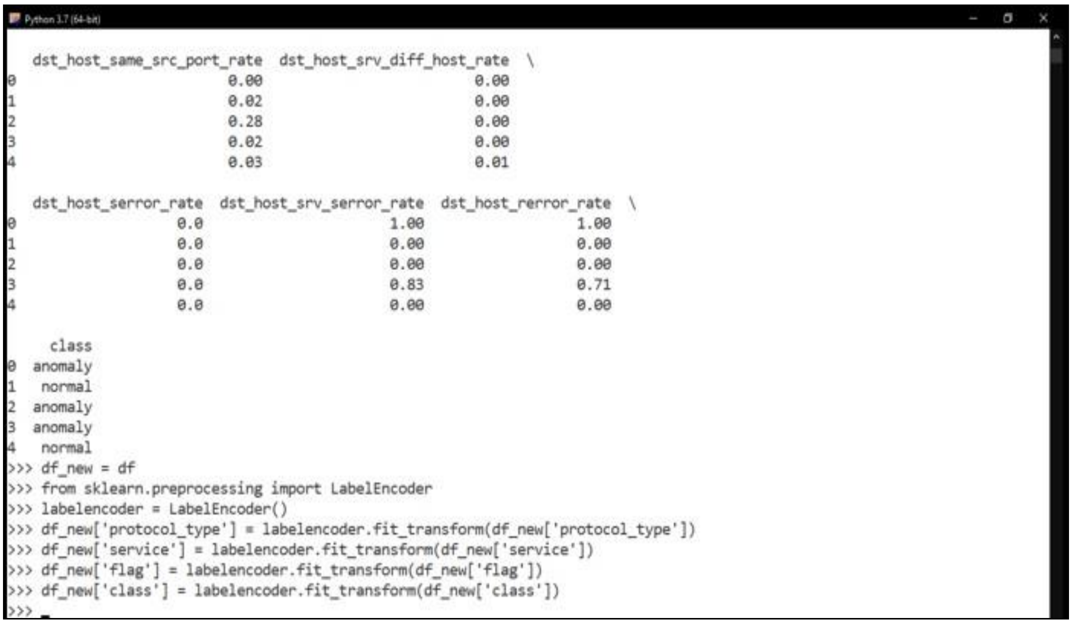


Figure 3.3: Dealing with the data's class labels


```
   dst_host_same_src_port_rate  dst_host_srv_diff_host_rate  \
0                         0.00                         0.00
1                         0.02                         0.00
2                         0.28                         0.00
3                         0.02                         0.00
4                         0.03                         0.01

   dst_host_serror_rate  dst_host_srv_serror_rate  dst_host_rerror_rate  \
0                   0.0                      1.00                  1.00
1                   0.0                      0.00                  0.00
2                   0.0                      0.00                  0.00
3                   0.0                      0.83                  0.71
4                   0.0                      0.00                  0.00

     class
0  anomaly
1   normal
2  anomaly
3  anomaly
4   normal
>>> df_new = df
>>> from sklearn.preprocessing import LabelEncoder
>>> labelencoder = LabelEncoder()
>>> df_new['protocol_type'] = labelencoder.fit_transform(df_new['protocol_type'])
>>> df_new['service'] = labelencoder.fit_transform(df_new['service'])
>>> df_new['flag'] = labelencoder.fit_transform(df_new['flag'])
>>> df_new['class'] = labelencoder.fit_transform(df_new['class'])
>>>
```

Figure 3.5 A Label encoder that works to encrypt the infiltration process's classified label

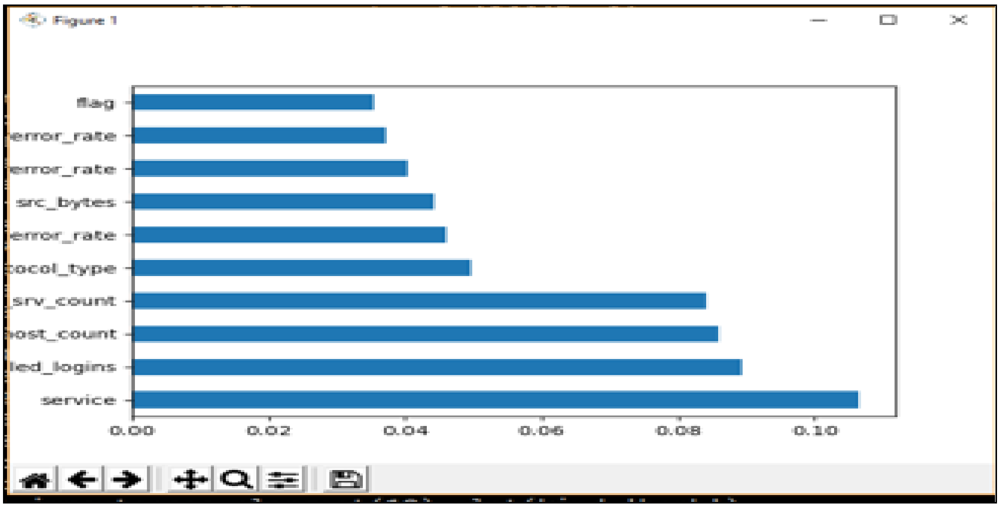
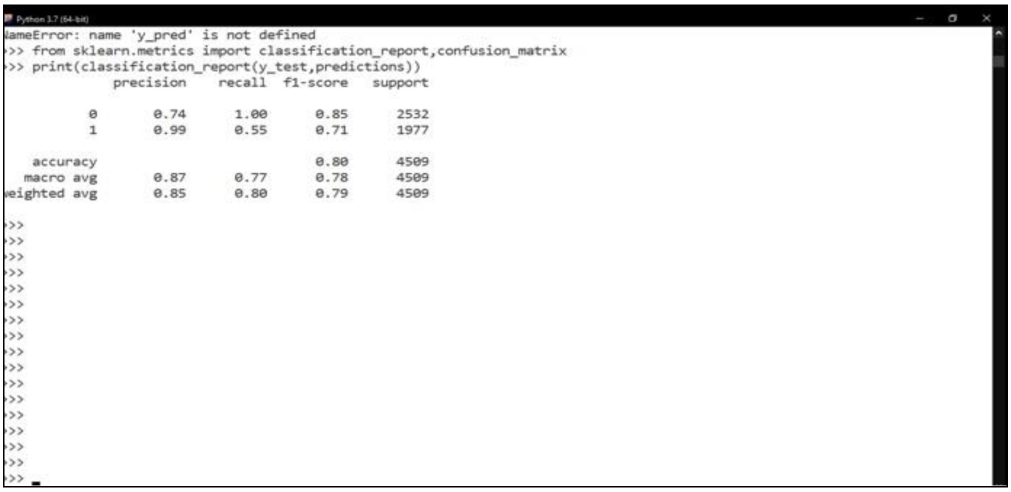


Figure 3.6 Supporting elements for the prior method's incursion


```
NameError: name 'y_pred' is not defined
>>> from sklearn.metrics import classification_report,confusion_matrix
>>> print(classification_report(y_test,predictions))
              precision    recall  f1-score   support

           0       0.74      1.00      0.85      2532
           1       0.99      0.55      0.71      1977

    accuracy                           0.80      4509
   macro avg       0.87      0.77      0.78      4509
weighted avg       0.85      0.80      0.79      4509

>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
>>>
```

Figure 3.7 Accuracy of the model concerning the rate and forecast

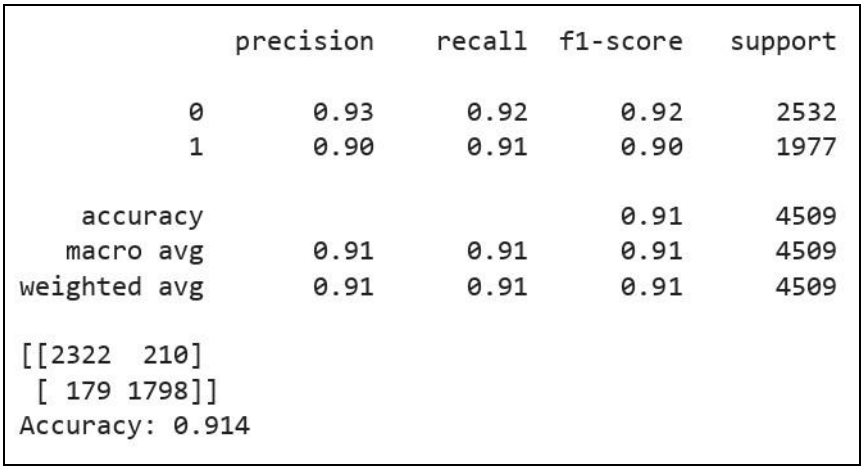


Figure 3.8: Accuracy of the prior technique

Figure 3.8 shows the effectiveness of the current method as measured by calculations for accuracy, precision, recall, and F1-score. It can be inferred from the data in Figure 3.8 that the present technique has an accuracy rate of 91.4%.

3.6 Summary

This chapter discusses how blockchain technology, seen as the direction of computer and storage technology in the coming years will be used. In response to these security concerns, we used experimental methods that enhanced statistical integrity to assess the existing RNN model based on deep learning. We can determine from the trial that the prior method had a forecast and rating accuracy of 91%. Improve the procedure for building a future decentralized, safe, and secure access control network. The next chapter uses blockchain technology to define a cloud platform's distributed access control network.

CHAPTER 4

Implementing Blockchain for Fast and Secure Distributed Access Control in Cloud Platform

4.1 Introduction

Cloud computing is a technology that has gained significant attention from businesses and academic institutions. It allows users to access software-based internet-connected services without needing local installation. This approach offers a convenient and efficient way to deliver information promptly. Many large companies are struggling to manage vast data [113]. As a result, numerous businesses have transitioned to cloud storage, providing improved data distribution, uploading, and archiving capabilities. However, data security, integrity, and confidentiality are critical concerns that must be addressed in cloud computing environments.

The control of access to data is a crucial component in ensuring data security within cloud-based storage systems. However, traditional data sharing and access control methods have posed significant challenges, resulting in the leakage of personal data and the misuse of encryption keys. Cloud capabilities enable the transfer of Electronic Records (ER), facilitating data sharing among various healthcare applications. Additionally, blockchain models provide security by employing multiple encryption techniques to authenticate users. While cloud integration enhances management, it also introduces potential risks to patient privacy. This study contributes to efficient access control, private data exchange, and retrieval within the cloud by leveraging blockchain technology [114]. An access control and sharing system based on blockchain technology is used in the study to overcome this. Using an ID and password to construct a registration application, the Data User (DU) sends it to the Data Owner (DO) through this mechanism. A blockchain that facilitates transactions and is protected by encrypted master keys contains data from the DO. The DO ensures that personal information is secure when uploading encrypted files to the Interplanetary File System (IPFS). The DO creates Improvised blooming filter metadata using encrypted file locations and encrypted keys and then uploads it to the transactional blockchain. Creating a blockchain framework is another study component that will let cloud platforms share and retrieve information more easily. The ER application makes use of data protection measures. The cloud-based platform includes the Inter-Planetary File System (IPFS), transactional blockchain, smart contracts, data owners, and data users [115].

Many individuals store their data in the cloud, which raises security and copyright concerns. The primary issue arises when data is transmitted to an external environment, as anyone with access to it, besides the owner, can potentially misuse it. Data protection is frequently not met by cloud service providers. Decentralized cloud-based storage networks, on the other hand, have several advantages over conventional data centre storage. Unlike traditional storage methods, these decentralized networks employ client-side encryption to ensure data security. Managing encrypted data poses challenges, with usability being a fundamental problem.

Additionally, the owner should be able to grant others access to remote encrypted data and retrieve specific unfinished material. A potential approach involves starting with the complete dataset, filtering it, and then providing the appropriate portions to authorized clients. Nevertheless, the high cost of this option renders it impractical for consumers, undermining the purpose of data outsourcing.

4.1.1 Data privacy based on access control

Security and privacy are primary concerns in cloud computing, driving the development of effective and secure access control mechanisms to limit access to information sources. This aspect has become crucial in the context of cloud computing. Access control methods verify the user's identity and restrict access to requested resources. These mechanisms aim to protect critical data resources and prevent unauthorized intrusions. In cloud-based frameworks, access control is more prevalent compared to traditional techniques. To use cloud storage services, users must authenticate themselves to the cloud service provider (CSP), who enforces appropriate standards for granting access to information and services. Mutual authentication and access control between service providers ensure cloud computing security. In addition to controlling channel attacks, cloud customers have various options to enhance information security. CSPs employ various access control measures within the cloud domain to bolster security, although certain limitations may exist [116].

4.1.2 Access Control for Blockchain

According to [117], we might not have much privacy when someone controls our data. They're using blockchain technology as a gatekeeper to ensure our personal information is seen relatively. They use pointers and a unique system outside the blockchain called a Distributed Hash Table (DHT). This system needs permission from the blockchain to hold onto our encrypted data. When we want to see our account information, they create a unique code with many keys. These keys are like secret passwords for locking and

unlocking our data. There are keys for keeping the data safe and letting us and the service get in. This way, our data stays private and secure.

Bloom filters are utilized to target specific false favourable rates. The creators of Bitcoin incorporated Bloom filters into the light-blossoming network to facilitate transaction processing among nodes [118]. The aim is to offer anonymity by adjusting the desired false positive rate through Bloom filtering, thereby concealing addresses.

Data security is a significant concern for individuals, necessitating robust security principles and practices. Users are apprehensive about the potential sharing of their personal information with other cloud service providers or its unauthorized use. Blockchains offer a means of maintaining an immutable record of data transmitted during transactions, rendering it extremely difficult to alter once entered. This approach is more user-friendly and effective compared to other security measures. This chapter introduces a novel method that utilizes Blockchain's secure data storage and access mechanism to ensure safe data storage and controlled access, employing Bloom-counting filters. Blockchain is advocated as a reliable technology for creating smart contracts, which automate tasks and streamline business activities through computer protocols. Operating as a decentralized and secure peer-to-peer network, blockchain enables all network members to share a ledger that records transactions among nodes. These transactions are securely stored in a chain of digitally linked cryptographic blocks.

4.2 Encryption-based techniques

The study on various encryption techniques used in access control and data-sharing procedures is summarized in this section. The Distributed Key Management Architecture (BDKMA), a revolutionary Blockchain-based model, was presented for access management in the Internet of Things (IoT) paradigm in reference [119]. The BDKMA paradigm used cloud computing to execute multi-block chains and fog computing to reduce latency, enabling cross-domain access. The concept met the needs for extensibility, fine-grained audibility, decentralization, large capacity, and privacy protection in access control by utilizing blockchain technology. The system's flexibility supports extra operation models, permission assignment nodes, and group access models. Different architectures could be accommodated thanks to their capacity to dynamically modify the length of transaction collection, which increased system performance and enabled scalability in proportion to network growth.

In [120], a robust mutual authentication-based blockchain security system named BSeIn, which enforces precise access controls, was proposed. This approach incorporates message authentication codes, integrated attribute signatures, and multi-receiver encryption to provide security and assurance. Specifically, the authentication of terminals, gateways, and message authentication codes was achieved using blockchain and attribute signatures.

In a recent study [121], researchers proposed a cross-domain sharing strategy for electronic health data. The primary objective of this strategy was to prioritize patient data privacy by utilizing cryptographic models that enable secure data sharing. The technique effectively integrates fine-grained access control and on-demand revocation mechanisms. A delegation strategy was used to build access control, combining a proxy signature-based model with a role-based one.

4.2.1 Smart Contract-based blockchain methods

In the realm of blockchain-based Smart Contract methods, the existing literature encompasses the following research studies:

A discussion of the creation of the architecture can be found in [122]. Delegation and access control for the Internet of Things are the main objectives of this architecture. It emphasizes the allocation of permissions based on events and requests and offers trustworthy, safe, and verified decentralized delegation services using blockchain technology. The design ensures that every node has the required permissions by giving those events to the node with the least access. This architecture's essential elements include the user's device, using the BACI architecture; restricted device access is successfully managed.

The integration of blockchain and smart contract technologies in the proposed data-sharing strategy for the Internet of Things (IoT) not only addresses authentication challenges but also implants confidence in access security across IoT ecosystems. Through the implementation of smart contracts such as the Judge Contract (JC), Access Control Contract (ACC), and Register Contract (RC), the solution orchestrates efficient access control mechanisms. Specifically, the ACC governs access systems, ensuring authorized entities gain appropriate data access, while the RC verifies and authenticates users within these systems, enhancing overall security. Furthermore, the JC employs a behavior-judging model to identify and address potential offenders, bolstering the resilience of the IoT environment against malicious activities and unauthorized access attempts. By leveraging blockchain and smart contracts, this innovative approach offers

a transparent, decentralized framework for robust data sharing and access control in IoT environments, fostering trust and reliability among stakeholders.

4.2.3. Research gap identification

a) Based on the diverse contributors and studies, blockchain has numerous security flaws because of the absence of trust. The cloud has generally been designed with various assessments and auditing tools that review different data types. However, unauthorized individuals have been stealing data.

b) Access control based on a role system was designed to be an attribute-based hierarchy system that can establish accessibility by combining cryptographic algorithms. However, the computation of the cryptographic hash function requires an additional attribute set, leading to a more significant computational problem.

c) They dissect only essential data. Or, more precisely, the data must be separated at several levels. Data broken down at the lowest level is burdensome for cloud security frameworks, overpowers the human head of state, and might lack sufficient evidence about an aggressor's expectations.

d) Security systems that are in place today cannot socially analyze data. In essence, information about connections between incidents isn't accessible during the prediction period.

4.3. Methodology

The main objective of this framework is to ensure that consumers have access to the necessary information. Incorporating various resources such as files, programmers, and other relevant information sources, the framework aims to facilitate genuine collaboration. Figure 4.1 illustrates a simplified and understandable flow process, with the structure developed drawing inspiration from research conducted in [124-125]. Enabling information sharing between two distinct client groups—referred to as subjects and objects—the framework's primary objective remains consistent: providing consumers with necessary information.

Within this framework, resources, including files, programmers, and other relevant information sources are made accessible. Triple contracts regulate information flow and access between objects and individuals. Employing this framework and utilizing triple contracts enables genuine collaboration and information sharing between subjects and objects, thereby enhancing transparency and efficiency within the system.

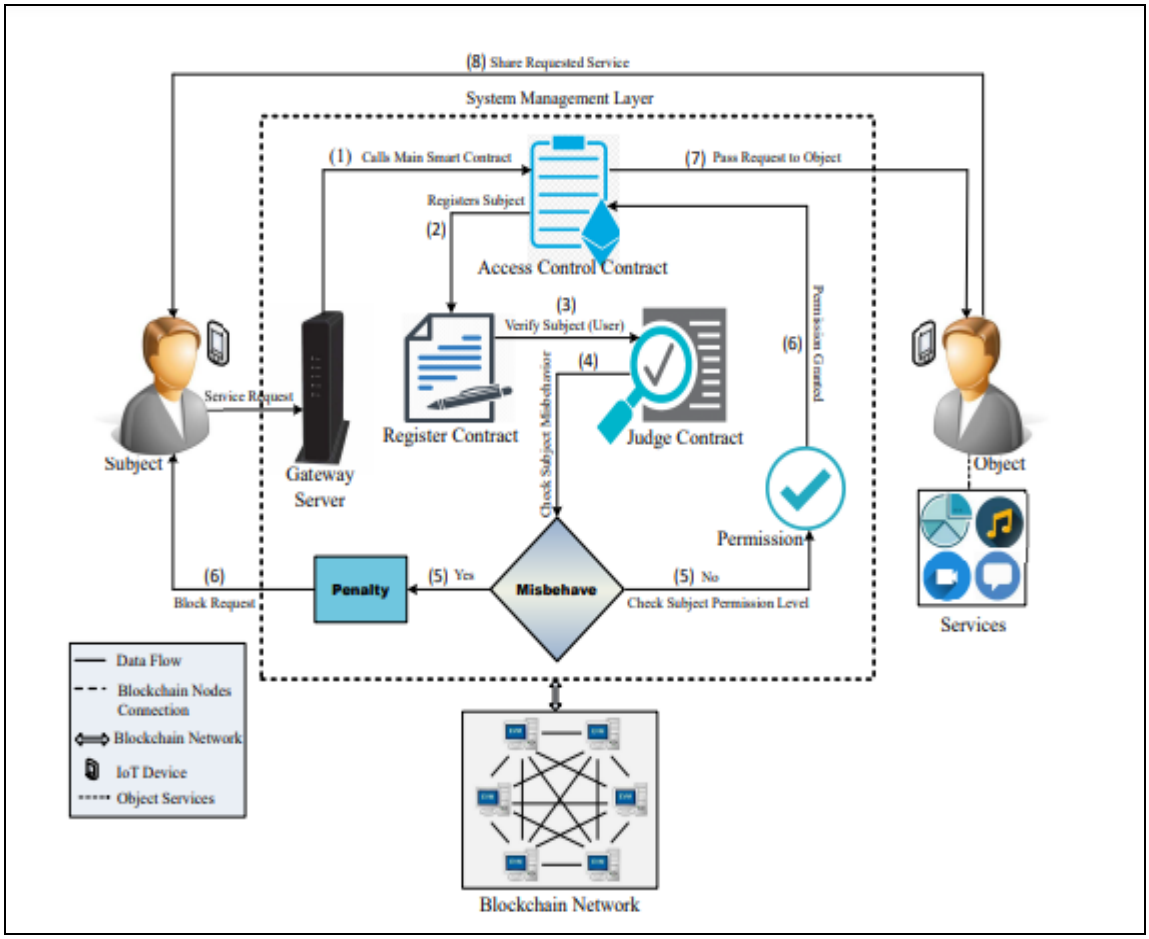


Figure 4.1: Model for sharing data and control access

4.3.1. Smart Contracts

The suggested technique consists of three agreements: an Access Control Contract (ACC), a Register Contract (RC), and a Judgments Contract (JC), all of which are designed to provide network users with security options. The ACC is responsible for authentication and database entry upkeep [156]. If negligence is demonstrated during the trial, the JC assesses any carelessness on the part of the subject or object and assigns legal duties.

4.3.2. Contract for Access Control

The access control contract is the primary smart contract for granting access privileges to IoT nodes. It appropriately responds to requests for connecting to the device's facilities and saves the user's data access. It enhances the program's efficiency and affordability, including the devices' computation time. The ACC is utilized when a user submits a query to the device.

4.3.3. Register Contract

The Register Contract ensures that only authorized individuals can access the services. By adding each user to the database, the verification process is conducted through the RC. RC uses The exact procedure to update its authorization database for verification.

4.3.4. Standard operating procedure for safe data exchange

Data owners send the encryption key for the data to each group member when they need to exchange information with that group. All group members have access to the encrypted material via the cloud, and they can decrypt it using the key. By doing this, each group member no longer requires the intervention of the data owner. The protected data is transmitted securely by converting the original healthcare data into privacy-protected data. Utility and privacy limitations are also used to control sensitive data. The Cloud Service Provider (CSP) utilizes a data retrieval system to determine whether the requested data is stored and meets the request's requirements [156].

4.4 Enhancing Blockchain-based Cloud Decentralized Storage with Enhanced Bloom Filter for Security and Transfer of Data

The decentralized cloud storage access control and data sharing model is created. The steps in the decentralized storage paradigm are as follows:

Step 1: In managing access control and data sharing, each entity (DO, Smart Contracts, DU, Transactional Blockchain) plays its specific role. Usually, a DO stands in for the file owner in a sharing context.

Step 2: DU has the authority to view files and serves as a client for data. By encrypting the master key and incorporating it into the transactional blockchain, DO lays the stage.

Step 3: Smart contracts are added to the transactional blockchain based on DO. They maintain a list of encrypted terms and offer DU a helpful search engine.

Step 4: DU contacts DO with a registration request during setup. Additionally, DO ciphertext metadata is included in the transaction blockchain, and the file is encrypted before being uploaded to IPFS (Interplanetary File System). DU decrypts the file after downloading it via IPFS.

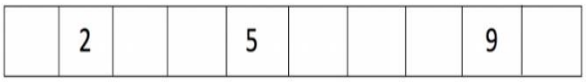
- Bloom filters utilize an array-based data structure known as the input data structure array. The length or capacity of the array can be adjusted according to the storage requirements. To get the desired results, you can alter the functions employed.
- It's crucial to remember that hash functions are employed in bloom filters. The design seeks to best use the resources at hand by increasing the processing filters' effectiveness.
- When data is added to the bloom filter, hash functions analyze the data and choose the right spot within the filter. The data does not belong in the bloom filter if a location has a value of 0. If the area, however, has a value of 1, the information has been added to the filter.

4.4.1 Hashing operations used by bloom filters

Using separate and evenly dispersed hash functions is crucial when configuring a bloom filter. These functions allow for comparison and indexing inside the data set by giving data elements identifiers. Despite their widespread use, well-known hashing algorithms like SHA-256, MD5, or CRC32 must be evaluated for their usefulness as bloom filters. Security is improved using numerous hash algorithms, but complexity and processing time may also rise. Therefore, choosing the proper functions to achieve peak performance is crucial.

It's worth noting that hash functions are unidirectional, meaning an identifier can be derived from a data element. It is a simplified model, as the number of buckets and hash functions can vary.

The next step is to run Ether (ETH) and view the identifiers listed below:



The following identifiers are obtained once we send Litecoin (LTC) through the system:

Therefore, the bloom filter is complete.

The bloom filter may determine whether Alice uses ETH by looking at the identifiers 2, 5, and 9. We can assume that Alice utilizes Ether if these bloom filter buckets overflow. It's crucial to remember that a hash function will always provide duplicate IDs when the same data is fed into it repeatedly. If both buckets 2 and 9 are complete, we can say that Alice consumes Ether. Then, to determine whether Alice is linked to Ether Classic (ETC), the bloom filter can be tested for the identifiers 6, 8, and 9. Buckets 6 and 8 are incomplete yet; bucket 9 demonstrates that Alice possesses no Ether Classic (ETC). However, suppose we utilize identifiers 1, 4, and 10 to determine whether Alice owns any Monero (XMR). In that case, we risk getting a false positive result because Bitcoin (BTC) and Litecoin (LTC) identities are also included in those buckets. Employing a larger bloom filter with more buckets is advised [156].

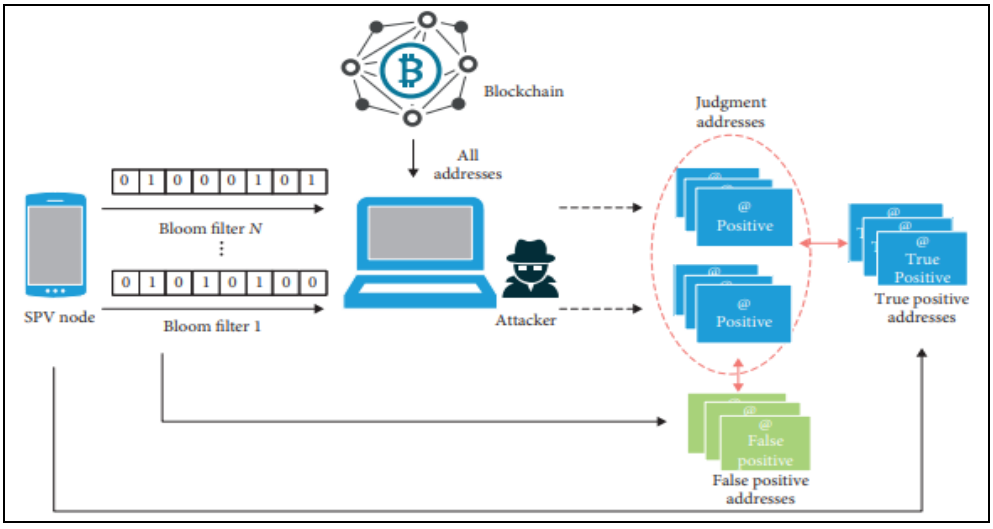


Figure 4.2: Bloom filter based on SPV node attack model

The two components of the game are the SPV node and Bloom filter. It's a strategic game because their state set can be considered finite.

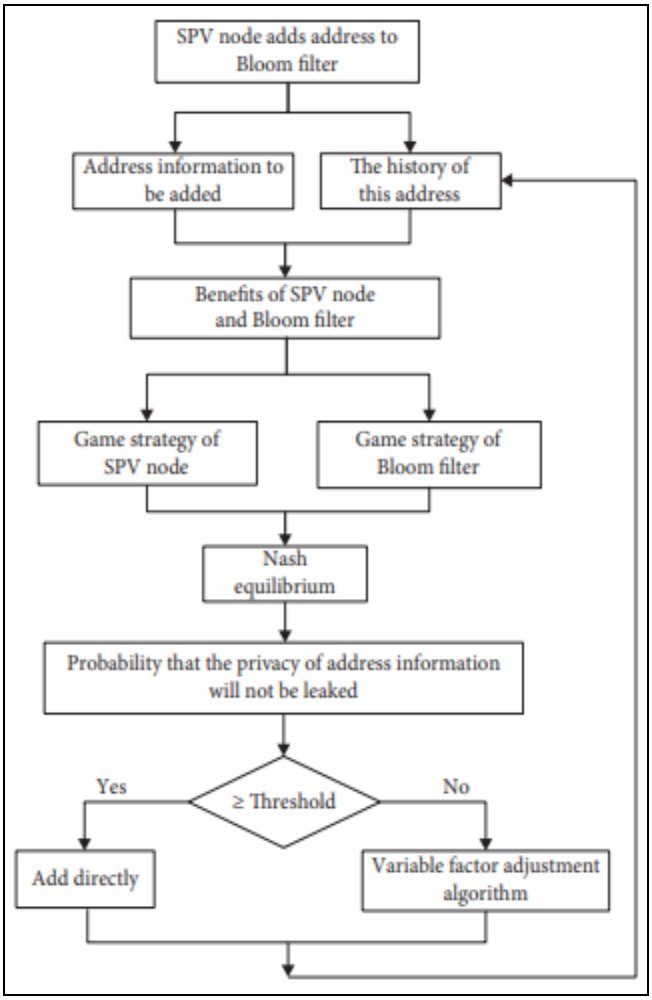


Figure 4.3: Privacy protection method

This benefit is when it allows more addresses to the Bloom filters while ensuring the security of the filters' nodes earns a certain amount, denoted as s_earning_State1[156].

4.4.2. Drawbacks in Bloom Filter Algorithm:

1. Adding elements is never ineffective, albeit at the expense of an increasing false-positive rate. To mitigate the number of false positives, it is essential to incorporate adding a bit array or reintroduction utilizing the Bloom filters.

2. It is impossible to retrieve the elements that were inserted.

3. The elements cannot be removed.

In the Improvised Bloom Filter algorithm, the significant Steps are:

Step 1: The initial setup will ensure that every slot contains a zero value, as no elements are included in this data structure.

Step 2: It is crucial to mention here this: the improvised bloom filter is an array of fixed size (m). It means it is a fixed-size array with a size and complexity of O (1). If it does not have flexibility in its size as time goes by, it loses the benefits of efficiency in space.

Step 3: Hashing: Hashing is mainly used in three methods: adding, taking away, and looking at the elements.

Step 4: Each component will get assigned at least one spot within the data structure. Therefore, each element will be passed through multiple hashing functions to determine the appropriate hash code within the data structure. A number of the hashing methods employed will be indicated by the letter K.

Step 5: To **add an element, we must fir**st use the functions for hashing to determine the keys to the component. Afterwards, we will get the rest (modules function) of the output of the array size. The formula will be Key is hi (element) 75% m, where hi() is a hash function as is m the array's length.

Step 6: Following that, we must visit slots where keys for elements point to and then raise the counter's value by one. In this case, we present the counter's value by one as we use improvised Bloom Filters. However, if we were using Bloom Filters, we wouldn't modify the slots so that they are equal to one, even though the element isn't one of the first elements in the slot.

Step 7: Removing **one data structure element** follows the same procedure as adding. To remove an element, first, we need to determine the keys of the element by using hash functions. After that, we'll look at the slots using the keys we've found; the next step is to reduce the value of these slots by one.

Steps 8 through 10 involve searching for an element within the data structure. Initially, hashing functions generate keys for the elements based on a given formula. These keys are obtained using an algorithm represented by hi(), and m represents the dimension of the component.

In step 9, each slot in the data structure is visited using the generated keys, and the corresponding counter values are checked. A zero counter value indicates the element's absence, while a non-zero value prompts further examination of other slots. If all slots containing keys yield non-zero values, it suggests the presence of elements in the data structure; otherwise, the element is deemed absent. However, it's worth noting that false-positive (FP) results may occur occasionally, where the lookup function wrongly identifies an element as present when it is not.

Step 10: false-positive probability is a critical consideration. This probability reflects the likelihood of the lookup function returning incorrect positive results. It is determined experimentally by dividing the number of accurate false positive outcomes by the total number of positive outcomes. Notably, improvised Bloom Filters do not yield false negative results. If the result is inaccurate, it is invariably wrong, as indicated by any slot with a zero value, signifying the absence of elements contributing to the counter.

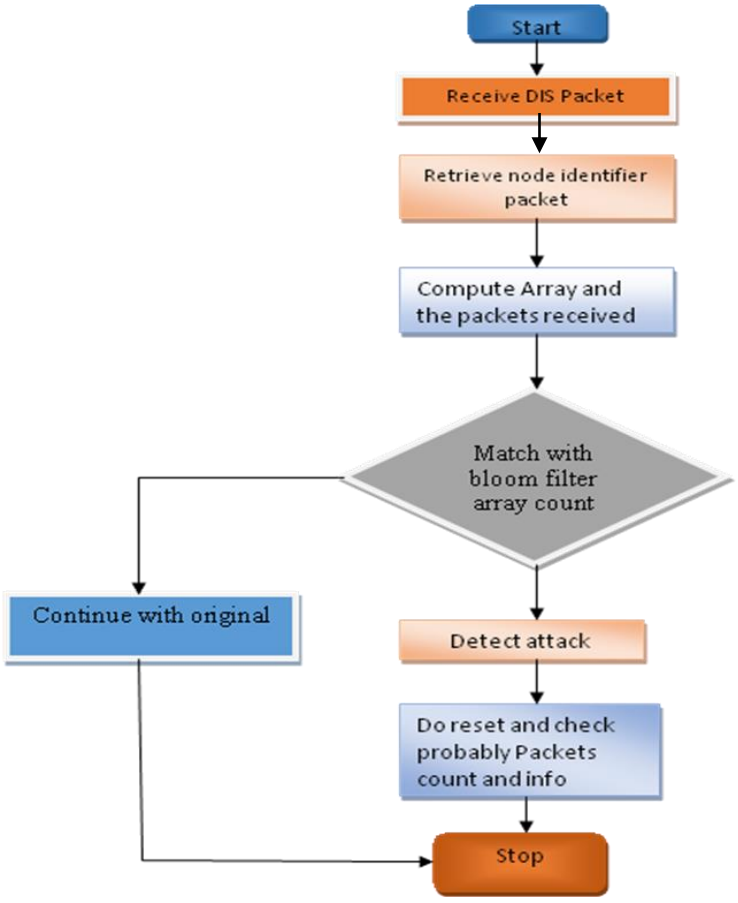


Figure 4.4: Flow of work diagram

4.5. Experimental setup & results

A Windows 10 operating system, an Intel i3 processor, 4GB of RAM, and the PYTHON tool were utilized for the implementation.

This section scrutinizes the methodologies for blockchain-based access control and data sharing with privacy protection. Comparative research is conducted, specifically concentrating on access control strategies using blockchain sizes 100.

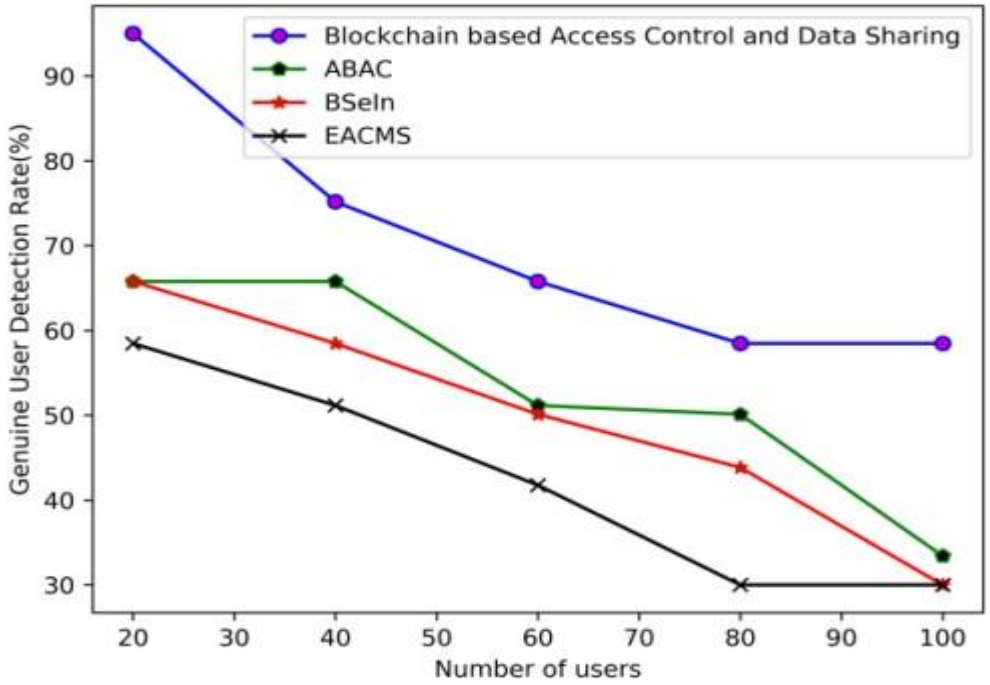


Figure 4.5: Using a 100-blockchain size comparison and the actual user detection rate

Figure 4.5 presents a comparative analysis of detection rates achieved by real users for different user counts in the context of access control and data-sharing methods. The experiment utilizes Ethereum technology, an open blockchain platform, for the secure execution of smart contracts. The code is implemented in Python using Colab notebooks for browser-based execution. The proposed algorithm's performance is evaluated with memory sizes of 180823 bits, 97146 bits, and 83677 bits. A Bloom Filter, an efficient probabilistic data structure, is utilized for element presence determination to optimize storage space.

For a group of 20 users, the actual detection rates are as follows:

- ABAC achieves a detection rate of 58.46%.
- EACMS achieves a detection rate of 65.76%.
- BSeIn achieves a detection rate of 65.76%.
- The blockchain-based access control and data-sharing methods achieve a detection rate of 95%.

For 60 users, the actual detection rates are:

- ABAC achieves a detection rate of 41.75%.
- BSeIn achieves a detection rate of 65.76%.
- EACMS achieves a detection rate of 51.15%.
- The blockchain-based access control and data-sharing method achieves a detection rate of 50.10%.

For 80 users, the actual detection rates are:

- ABAC achieves a detection rate of 33.40%.
- EACMS achieves a detection rate of 30%.
- BSeIn achieves a detection rate of 30%.
- The developed model achieves a detection rate of 58.46%.

Through experimentation and evaluation, this study offers valuable insights into detection rates achieved through diverse access control and data-sharing methods. Leveraging Ethereum technology and the Python programming language, the research explores how these methods perform across varying user counts. A notable inclusion is the utilization of Bloom Filters, a resourceful tool for efficiently determining the presence of elements within a set. It not only enhances detection rates but also optimizes storage and access. By shedding light on the interplay of these factors, the research contributes to developing more effective and scalable blockchain-based systems, crucial for secure and efficient data sharing in an ever-evolving technological landscape.

FPR = FP / (FP + TN)

1. Using a memory size of 180823 bits in the improvised bloom filter

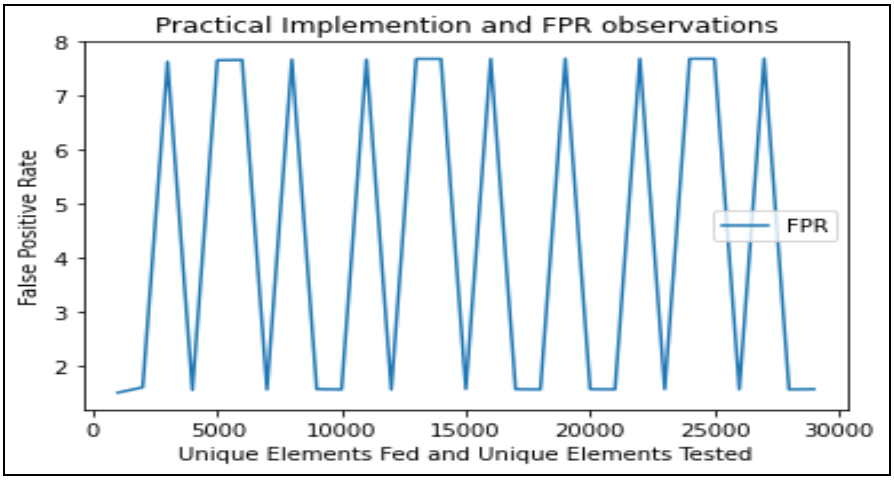


Figure 4.6 FPR for 180823 bits size

Figure 4.6 illustrates the practical implementation and observations of false positive rates (FPR) using a data size of 180823 bits. The graph displays the X-axis representing the number of unique elements fed and tested, while the Y-axis indicates the corresponding false positive rates (FPR). The FPR was initially set at 5.0%, and the average practical observation yielded a value of 4.302708654133927%.

2. Using an improvised bloom filter with the memory of 97146 bits

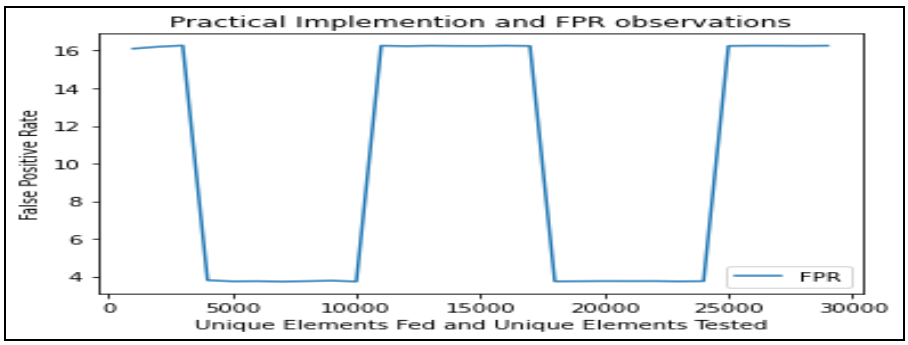


Figure 4.7 FPR for 97146 bits size

Figure 4.7 depicts the practical implementation and observations of false positive rates (FPR) using a data size of 97146 bits. The graph features the X-axis representing the number of unique elements fed and tested, while the Y-axis indicates the corresponding false positive rates (FPR). The FPR was initially set at 20.0%, and the average practical observation yielded a value of 10.20874612312953%.

1. **Using a memory size of 83677 bits in the improvised bloom filter**

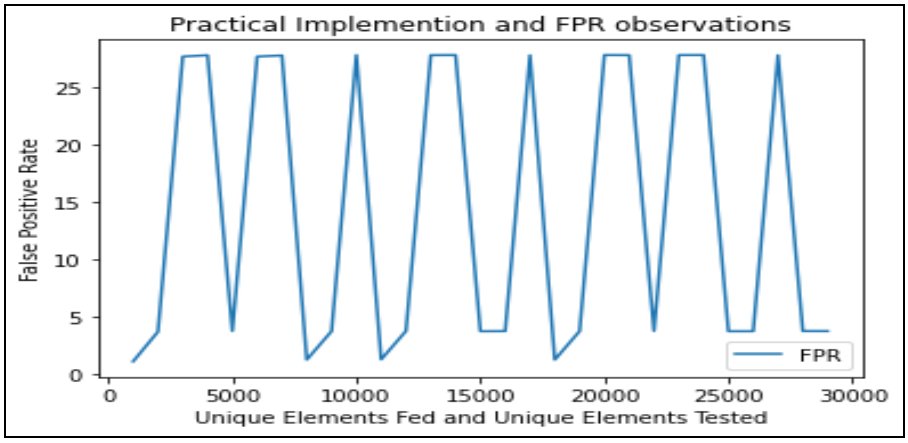


Figure 4.8 practical observation averages at 83677-bit size

In Figure 4.8, we gain valuable insights into the practical implementation and observations of false positive rates (FPR) within a dataset comprising 83,677 bits. This graph visualizes the experiment's outcomes, with the X-axis depicting the number of unique elements fed into and tested within the system. On the other hand, the Y-axis illustrates the corresponding false positive rates (FPR).

The initial FPR setting stood at a relatively high value of 25.0%, reflecting the inherent challenges of minimizing false positives in various data analysis tasks. However, the research yielded a significantly improved FPR value of approximately 14.20% through meticulous experimentation and observation.

Table 4.1: Results observation

S.NO	Memory Size	False Positive Rates (FPR)	Practical observation average
1	83677 bits	25%	14.1968%
2	97146 bits	20%	10.208%
3	180823 bits	5%	4.302

Table 4.1 presents False Positive Rates (FPR) from practical observations. FPR decreases as the threshold reduces: 25% threshold has 14.1968% average FPR, 20% has 10.208% and 5% has 4.302%.

Table 4.2: Transfer Data rate observation

S.No	User-Nodes	ABAC	Proposed Blockchain Model
1	20	65	96
2	30	68	85
3	40	70	75
4	50	65	72
5	60	63	70
6	70	60	69
7	80	59	65
8	90	55	60
9	100	50	60

Table 4.2 presents a comparative analysis of user nodes in the context of ABAC and Blockchain Models. It reveals that the corresponding values decline as user nodes increase. For instance, when the User-Nodes are 20, the ABAC model yields 65,

whereas the Blockchain Model produces 96. Similar trends are observed across varying user nodes.

4.5 Summary

This study proposes a decentralized system for cloud storage data access and storage. The system uses distributed Hash Tables (DHT) and counting bloom filter encryption to achieve decentralized data storage. Using a recommended access control method, the system addresses the problem of multidimensional authorization in data-sharing and data-sharing systems. This architecture does away with centralized storage by using upward-directed monitoring techniques stored on the blockchain and permissions by writing access data. During the testing for this project, a decentralized platform called Ethereum technology was employed to define the peer-to-peer networks. The algorithm's false positive rate was calculated for three data sizes: 180823 bits, 997146 bits, and 83677 bits. Our research's main objective is to boost algorithm administration efficiency so that access control judgments may be made more successfully. The following chapter will cover data traversal and transfer in nodes using bots.

CHAPTER 5

Optimizing Energy Efficiency and Node Travel in Cloud-Based Blockchain with a Cuckoo Ensemble Model

5.1. Introduction

Blockchain is an upcoming, promising distributed computing system and open, decentralized framework. The security, credibility, and reliability of the transactional data are assured by the unique capabilities of Blockchain regarding operating rules as well as record-keeping traceability. Blockchain can, therefore, be used to create a decentralized and distributed trust infrastructure. Due to their complexity and the different architecture they have across multiple systems, managing networks has become a more challenging task. The ability to track the configuration status of numerous devices over a short period, the need for specialists with various backgrounds, and the lack of an effective method for managing network configurations make manual network management impractical [127]. These factors contribute to the rising expenses and labor requirements for managing networks.

The network topology is an expanded representation of the network's resources. Gathering data from software-defined networks (SDNs) has proved challenging to enhance network management, routing, and service quality [128]. Before 2022, there will be a projected 29 billion more devices linked to IP networks.

The behavioural model for services on the Blockchain is described in the chapter. Experimental data is used to demonstrate their dependability. The writers highlight the network's main technical features and data transmission characteristics. The authors outline the network's organizational structure, how it interacts with blockchain transactions, and how network properties relate to application-specific factors. They look at how this model may be used to identify blockchain services and the chance that current technology-based security measures will be circumvented. The chapter also offers advice for hiding the traffic profile. This chapter reviews unsolved problems and ideas for further research on cloud-edge trust management systems and double-blockchain structures. Double-blockchain is a cloud-based solution that allows for transactions. The chapter also discusses the recent challenges and makes recommendations for further research. They are based on the latest trust management framework for cloud edge and double-blockchain structures. It is a cloud-based,

transactional model. Cuckoo enhances models to define the ideal transformation of network information from one location to a cluster. Alternatively, [129] will assist the network's flow.

Two advantages are the equality of rights among all participants in a decentralized network and the simplicity of data interchange. Reliability: any attempts made by anyone other than the authorized person to modify the data do not succeed due to the inconsistent versions of previous copies. Others will later scrutinize any altered information uploaded transparency [130]. In addition, information that is private to the user is stored securely so that while one can observe the entire operation, they're not able to identify who is the one who has sent or received information. Because blockchain data is transferred irreversibly (wrong actions aren't reversible), the risks are based on the possibility of fraud and errors. Furthermore, they are vulnerable to processing speed issues, which is the biggest drawback of blockchain technology, mainly when it's used to create digital currency. It is, as well as the risk that it could be utilized for illicit actions [131].

One of the most crucial elements that affect how a network behaves is its topology. The demand for network security has risen today due to a higher danger of hostile assaults. This study recommends a blockchain-based system to find and store networks safely. These problems may be resolved by the blockchain-based technology suggested in this study [132]. A method for network analysis was used in experiments using Minuet, Cisco Packet Tracer, and the Ethereum blockchain. Even with only a shaky understanding of the activities within the network, it can still identify the structure of the networks. The findings show that this system is not vulnerable to malicious users, in addition to the risk of external threats, and enhances the system's security.

It is possible for the element set to include either a blockchain network component that can transmit block headers or a non-blockchain network component that is designed for the transmission of data that does not belong to the blockchain. The hash functions, the cuckoo filter provides a method for encrypting block headers while they are being transmitted. This filter is included in this set. A dynamic solution for maintaining a moderately low false-positive rate (FPR) in information transmission errors is provided by cuckoo filters. This solution is particularly advantageous for applications that handle substantial data volumes. Their dynamic capabilities make it possible to integrate the addition, deletion, or retrieval of particular objects in a seamless manner, which guarantees effective data management in a variety of settings.

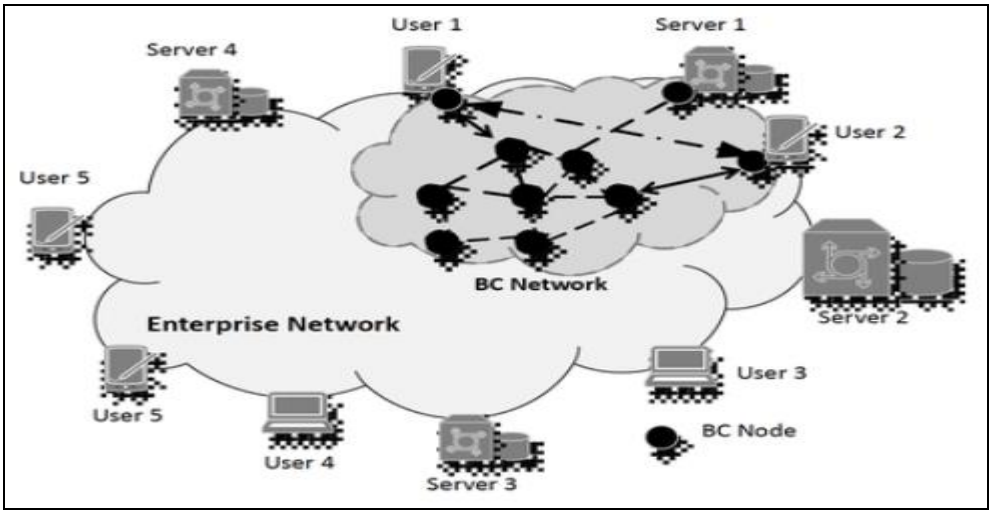


Figure 5.1: Overall communications networking infrastructure [133]

The purpose of this initiative is to decrease a network's energy usage. It is essential so that the network can operate at its maximum effectiveness while consuming the least power. An improved Ensemble Cuckoo Search Algorithm (ECSA) is suggested to solve this problem. The presented Differ Ratio (PDR), a novel technique designed for the algorithm presented, comprises three parameters: the group's size, its energy distance, and its dimension. A unique encoder is employed to decode the population to improve the effectiveness of Cuckoo searches.

5.1.1 Problem Statement

The nodes in a network are often used in a physical setting and are powered by batteries. The Node is defined as a smart, compact, multipurpose, self-organizing gadget that features batteries, radio connectivity, a microprocessor, and sensors in addition to being reasonably priced. It has a far smaller range of sensors and less computing capability, battery life, memory, and power. It's a program designed to assess and control the physical surroundings at a distance [134].

5.1.2 Contributions

- The latest iteration of the cuckoo model represents a substantial leap forward, particularly in terms of efficiency, which has led to streamlined operations.
- Traversal time, a previous bottleneck, has been significantly reduced, signifying a considerable boost in data processing speed.
- Additionally, the adaptation time for nodes to handle data processing tasks has decreased, resulting in improved system responsiveness, underlining the algorithm's success in enhancing the cuckoo model's performance.

Despite challenges in communication between data nodes within cloud blockchain systems, the suggested approach has shown significant progress in tackling these issues. By leveraging blockchain technology for secure network storage and locating, it addresses the escalating need for network security amid increasing hostile attacks. Researchers describe battery-operated nodes as cost-effective, multifunctional devices with limited capabilities in physical environments. Utilizing the Ensemble Cuckoo Model for outcome tracking and AuditChain for packet log integrity, the system ensures Proof of Existence (PoE) for each log, stored on the blockchain and in the Cuckoo filter for immutability. CFAuditChain offers detailed audit log verification at a reasonable cost, replacing centralized audits with a decentralized blockchain network for heightened security. Additionally, the research proposes a blockchain-based technique for cloud data integrity verification, addressing the drawbacks of centralized audits and enhancing effectiveness and security. The evaluation confirms the efficiency of the proposed strategy.

5.2 Working models

Data integrity is guaranteed by several methods that reduce the security threats cloud storage can pose. Provable data Possession (PDP) strategies and Proved Retrievability (POR) methods are two distinct categories within which the schemes used to confirm data integrity are currently classified. POR is a challenge-response technique used in PDP systems to ensure the user's data is appropriately stored in cloud storage. This mechanism uses the challenge-response technique by POR systems to verify the data has been saved. POR technologies can help recover damaged or lost information. Furthermore, they could verify that the verifier is authentic. The verification process may be separated between a private and a public procedure. The public verification process using TPA better supports auditing public officials' rapid updates and efficient verification than personal verification. [135].

5.3. Methodology

A key component of Bitcoin is the blockchain, a decentralized open database that serves as the currency's foundational technology [157]. A blockchain is an accumulation made up of data blocks that have been created using cryptographic processes in 1919. Each block acts as an account of transactions performed on the Bitcoin network. It is then used to verify its content and create new blocks.

A blockchain is a permanent and immutable ledger that cannot be altered or tampered with due to its inherent cryptographic properties. It operates by organizing data into a

sequential chain of blocks. The fundamental principle behind blockchain technology is its utilization of distributed consensus algorithms to validate and store data. These algorithms ensure that the network participants agree upon any additions or modifications to the blockchain. Additionally, cryptography plays a vital role in ensuring that only authorized parties can access and transfer information within the blockchain. This cryptographic layer adds a strong layer of security to the system. Moreover, smart contracts are an integral part of blockchain technology, as they enable the automation of scripts and programmable changes to stored information. By combining these elements, blockchain technology provides a secure and efficient means of storing, validating, and managing data in various industries and applications.

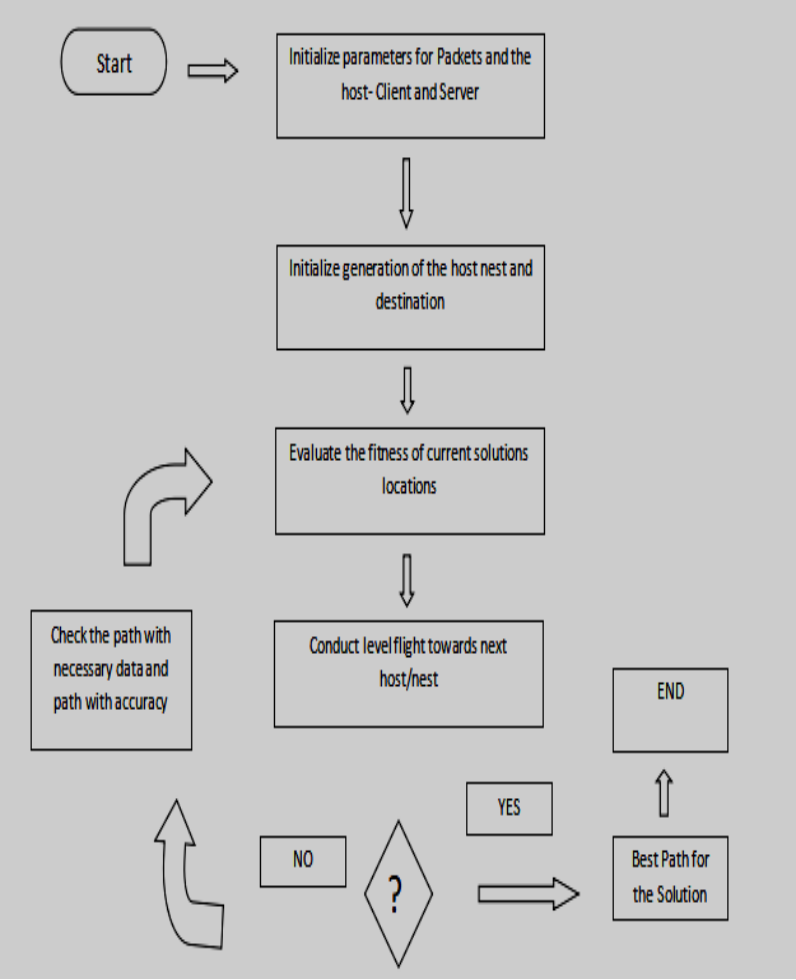


Figure 5.2: Proposed methodology Flowchart

5.3.1. Cuckoo Filter

Cuckoo filters are random data structures with a straightforward design and high spatial efficiency [157]. This filter performs better than other bloom filters regarding query efficiency, capacity use, and the capability to reverse operation. There are two choices of storage available. Furthermore, it can quickly find keywords in search results and

then dynamically relocate keywords to create space for new ones to be added during the insertion procedure. Although the difficulty of inserting the cuckoo filter has been forecast to be O (1), many actions are required.

This CS algorithm is an all-encompassing optimization technique that is based on cuckoos' predatory behaviour. The algorithm has been successfully used for various challenges across various fields, demonstrating its effectiveness. CS uses levy flights to generate steps that effectively search the solution space [157]. With the aid of switch probability, a local search is carried out with specific options being excluded.

5.3.2. Cuckoo Search algorithm

Three concepts make it easier to reproduce the cuckoo using the algorithm.

1. Every cuckoo lays an egg inside the nest, which will be randomly chosen;

2. the most successful nests are transferred to the following generation of cuckoos.

3. The number of nests that host birds can find is fixed (restricted) in which birds that are the hosts find the egg of a cuckoo, and the probability of finding it differs between [0,1].

5.3.3. Ensemble Cuckoo Search Algorithm

The efficiency of energy use and the delayed awareness of routing are two elements of improved cuckoo-search method-based routing. They lay eggs inside their nests for reproduction. Host birds serve as the cuckoo's reproduction vehicle. The host bird may not accept eggs from different species or abandon nests to build a new one if it discovers eggs of cuckoos inside the nest. Various optimization problems may be helped by cuckoo search optimization (CSO), which focuses on reproduction. Compared to the meta-heuristic algorithm, it is a significantly superior approach.

1. Genetically replacing abandoned nests (rather than utilizing the first method's random replacements) might considerably increase the convergence of the Cuckoo Search algorithm.

2. The approach is effectively used to resolve numerous industrial optimization difficulties. The algorithm has been modified, and crossbreeding made changes between some of the most sought-after premium nests.

3. The network's structure may be built by combining the layers' inputs, outputs, and interconnections. The number of repetitions necessary to completely understand anything may then be determined.

4. The architecture diagram shows how the Network might first become aware of the configurations that its Nodes produced and the load that it imposed on them. The load is then allocated as per the model, and gradual increments will determine the amount of each Node.

5. Because it traces back the results, it is a neural network with backward propagation. It moves ahead based on the findings of the verifications. The mean of square error is used to trace the data once validation is complete.

6. The incursion system perfectly connects nodes' accessible routes and clusters backed by blockchain.

Three potential CS adjustments are recommended in this research to enhance exploration and exploring. Instead of utilizing Levy flights, it is possible to investigate the search area. The three options each calculate the magnitude of the step by using a Cauchy operator. CS also incorporates division by population and generation division to ensure that exploration and exploitation are equal. Twenty-four benchmarks with different sizes and population sizes were used to assess the proposed CS algorithm and the effects of probabilities switch, which is studying the impact of probabilities switches. The new algorithms are being compared with the current ones utilizing grey-wolf optimization and differential evolution.

Steps:

1. Work with the host to identify the node nests.
2. The maximum number of nodes formed before Levy flights are randomly substituted for the cuckoo's answer.
3. Check the applicability and quality of it.
4. Replace the previous solution with the most recent one.
5. Use the most efficient techniques and nests; carefully reject a portion (Pa) of the most damaged nests before building new ones.
6. Compare them to find the best solution, and then use that solution to find the most effective solution.
7. Transfer the most successful techniques now being used to the next generation.
8. After the program finishes, it will end.

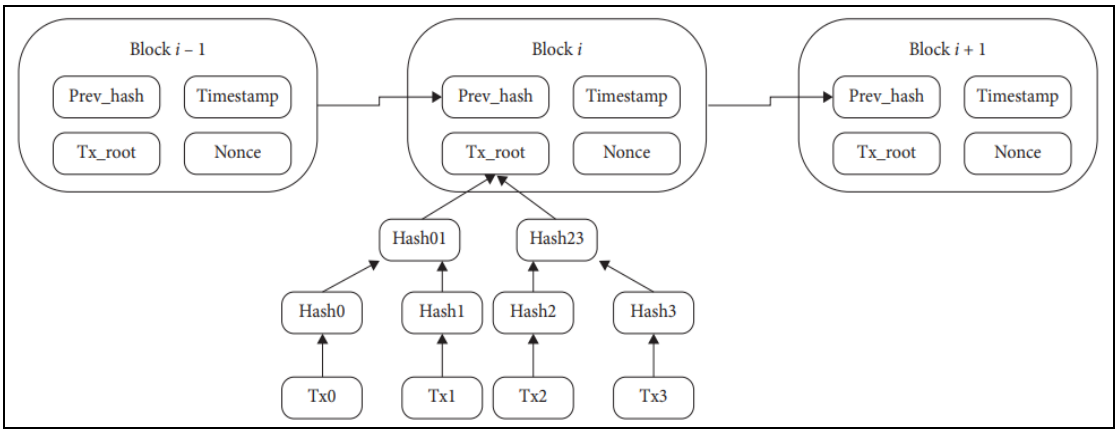


Figure 5.3: Blockchain Structure

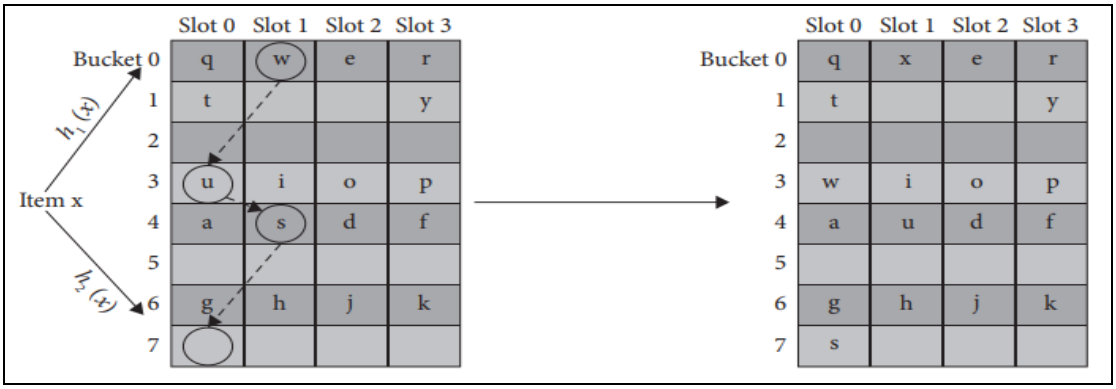


Figure 5.4: Cuckoo filters Illustration.

Both one and four spaces are included in each bucket. The System for Data Integrity Verification The suggested strategy to check data integrity must contain the following qualities to do the task successfully and safely:

a) Validation of integrity and the dynamic integrity of data are often required for users to change the data posted in the CSP. The data must be able to change dynamically, like altering existing information.

b) Beware of quantum attacks. Lattice cryptography has become more essential in cyber security and information security due to quantum technology's advancement and quantum computers' advent. This method must be secure and robust when operating in a quantum context.

c) Trustworthy audits: When a user can upload their files to CSP and maintain control of the data, the security of those data is severely compromised as the traditional methods of evaluating cannot be used with cloud-based platforms. It is also likely that the CSP can alter the data's security [21]. Thus, the method recommended to protect data integrity should ensure that accuracy and reliability are maintained for the authenticity of data validation.

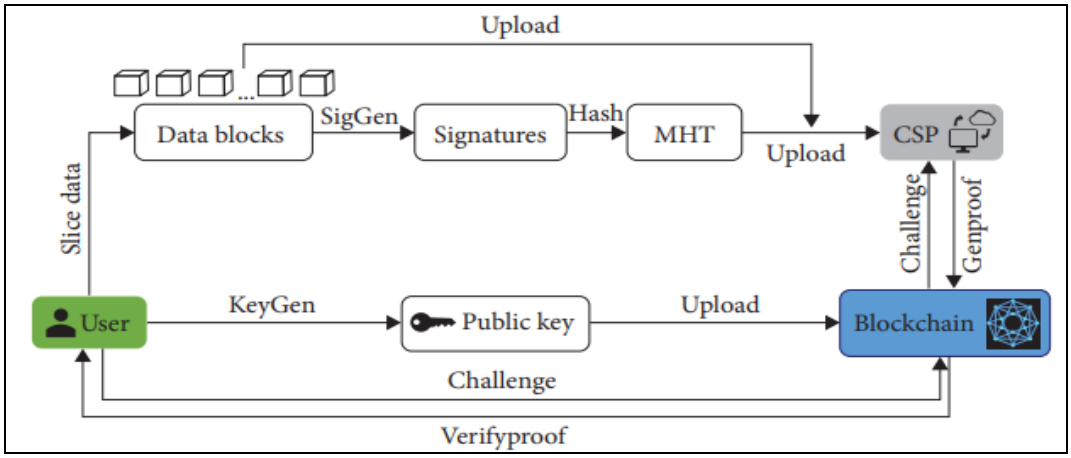


Figure 5.5: System verification procedure.

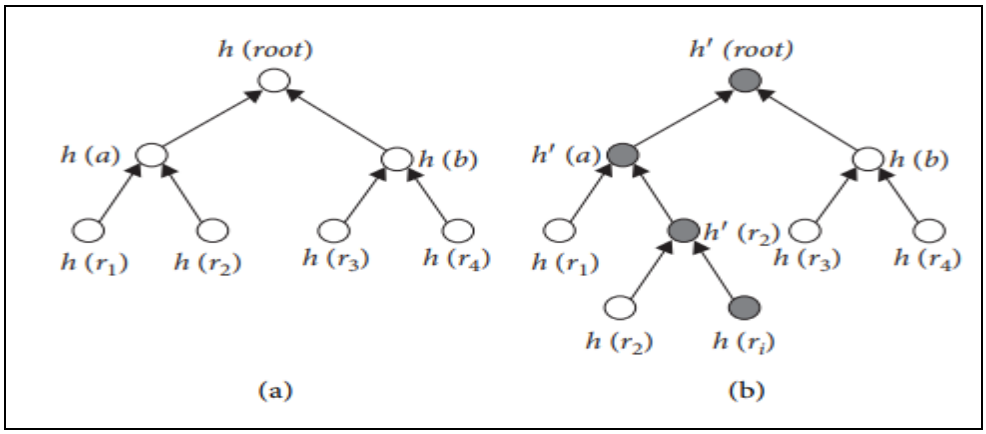


Figure 5.6: Insert operation of MHT

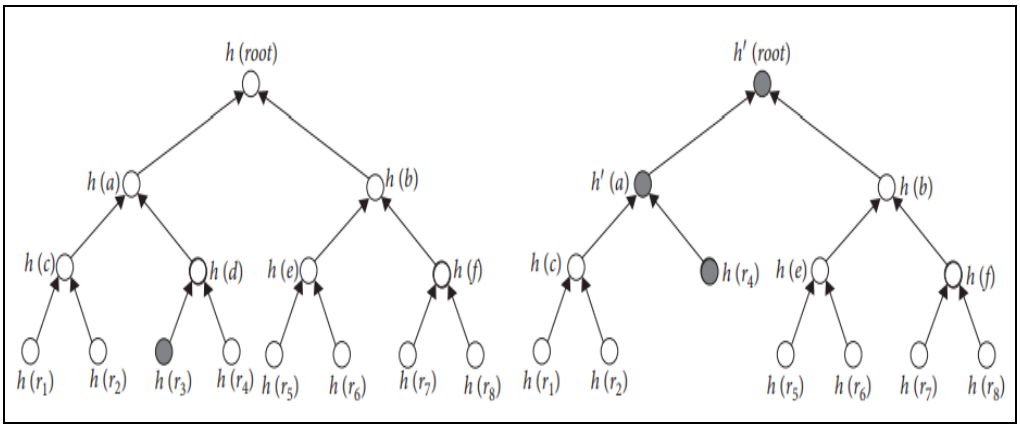


Figure 5.7: Delete operation of MHT

5.4. Experiment results and evaluation

In developing the architecture of a neural network, the framework is constructed by integrating inputs, outputs, and connections between layers. The determination of the optimal number of repetitions and iterations for effective learning is a critical aspect. The network is designed to be aware of previous configurations generated by its nodes and the computational load they've borne. Subsequently, the learning model allocates

specific workloads to the network, considering these historical configurations. A phased approach is then employed to detail the distribution of load reduction across individual nodes. This neural network implements a backward propagation technique, which allows it to trace back results based on verification findings. Once the validation process concludes, the mean square error is utilized to analyze and backtrack the data. These operations are conducted within a designated environment optimized for data analysis, ensuring the network's optimal performance.

Table 5.1: Sample Parameters

S.No	Attributes	Measures
1	Sample Nodes	100
2	Size of Area	1000 X 1000 m
3	Address MAC-IP	801.41
4	Frequency Range	350m
5	Result Estimated Time	100 sec
6	Network Traffic	Dataset with Packets
7	Size of Packets	90 Bytes

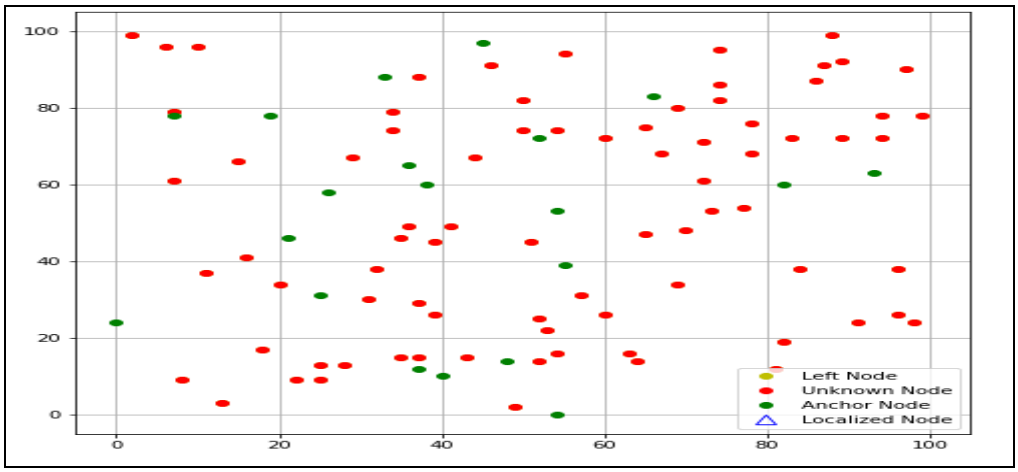


Figure 5.8: The graph shown above identifies the nodes

Graph 5.8 visually represents nodes strategically allocated for data transmission and accessibility. These nodes are effectively configured for establishing connections, implying their readiness to facilitate seamless data transfer. The visualization highlights the arrangement and availability of these directed nodes, showcasing their significance in supporting efficient communication.

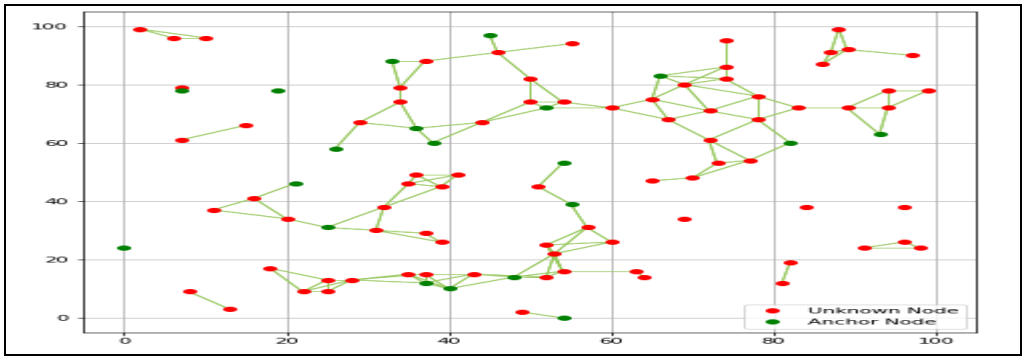


Figure 5.9: Cuckoo-Trained Network's Linked Nodes Primed for Data Transmission

From Figure 5.9, the network's interconnected nodes, previously trained using the cuckoo algorithm, are now poised to transmit data efficiently. These prepared nodes signify an advanced stage of network optimization, ready to contribute to seamless data exchange and communication.

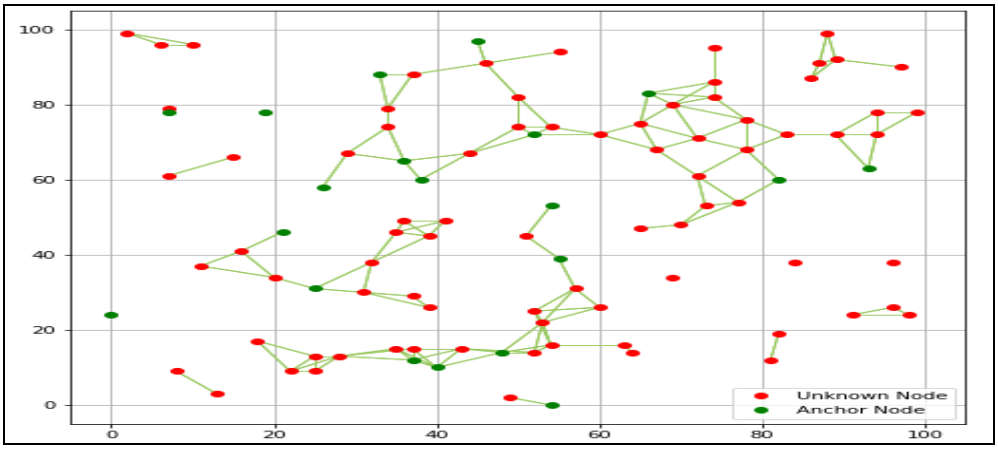


Figure 5.10: Including Overlooked Nodes for Transmission

Figure 5.10 shows results highlighting both omitted nodes by the cuckoo model and optimal, dependable connected nodes for transmission, offering a comprehensive overview.

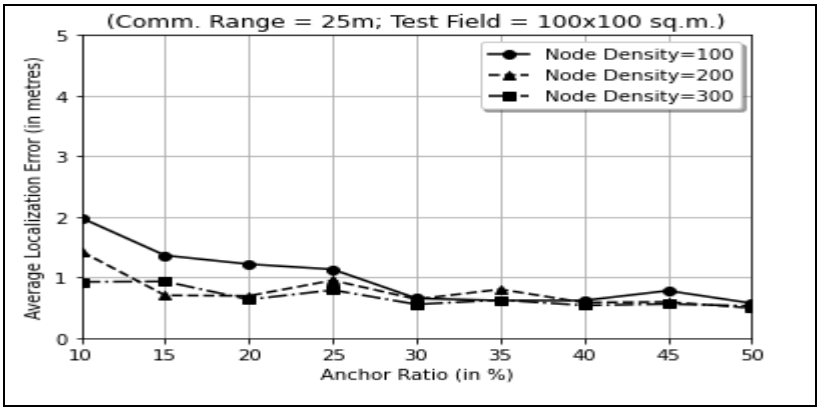


Figure 5.11: Node Density Reveals Connection Errors and Strength Variability in Network

Figure 5.11 shows that an analysis of node density provides insights into the diverse range of nodes present, their connection error rates, and their strengths within the network.

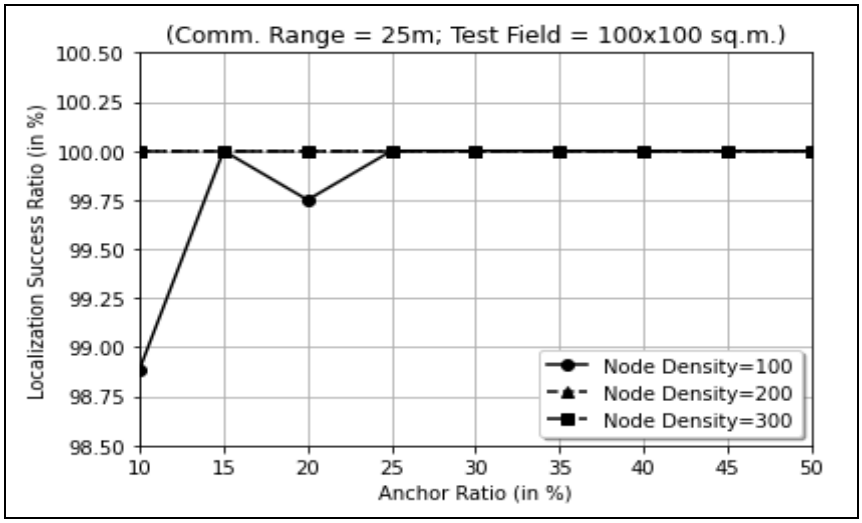


Figure 5.12: Model Success in Node Connectivity Assessment across Increasing Counts

Figure 5.12 shows the outcomes that exhibit the model's achievement rate in evaluating connectivity across various node counts. Our model demonstrates consistent connectivity as the node count increases, highlighting its robustness and reliability.

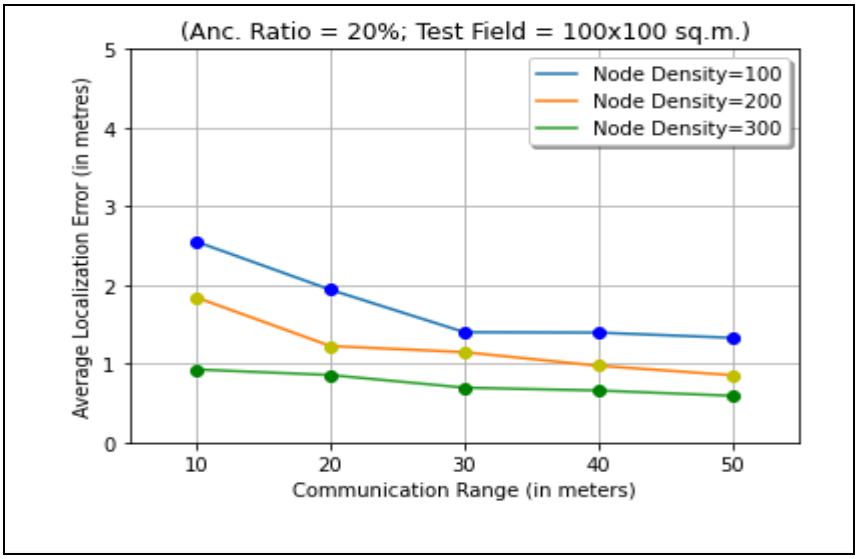


Figure 5.13: Flawless Data Transmission and Node Communication as Range and Nodes Expand

Figure 5.13 investigates data transmission range and node communication, revealing impeccable transmission as range and node count expands. The results highlight the system's robustness in maintaining seamless communication, suggesting its viability for scalable network applications.

Table 5.2: Transmission range and error range

Communication Range - Density	Average Error
10 - (100 to 300)	0.9 - 2.7
20 - (100 to 300)	0.9 - 1.9
30 - (100 to 300)	0.8 - 1.8
40 - (100 to 300)	0.7 - 1.5
50 - (100 to 300)	0.6 - 1.4

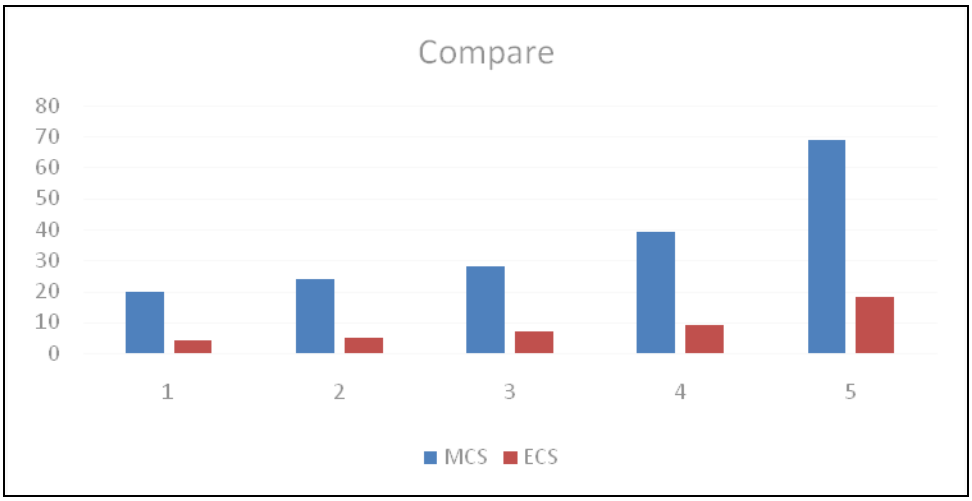


Figure 5.14: The average localization error ratio of the proposed and current cuckoo models should be compared.

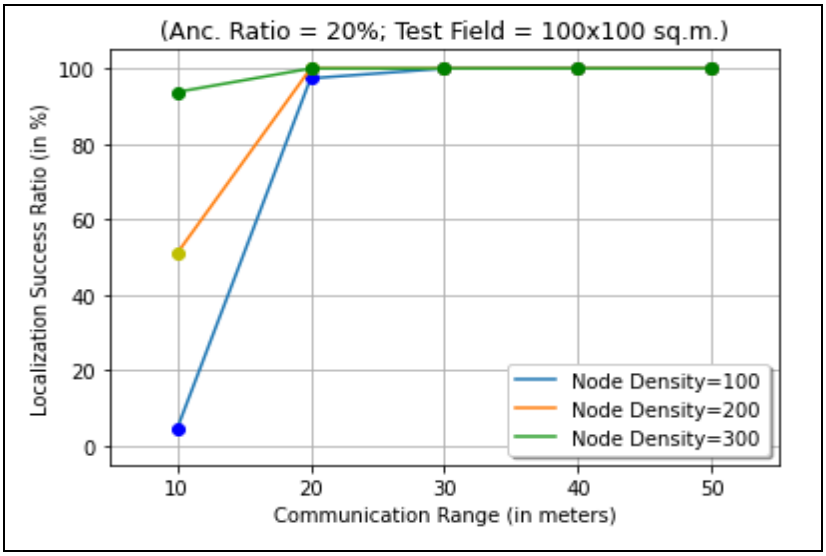


Figure 5.15: Enhanced Cuckoo Model's Success with Increasing Nodes and Effective Connectivity

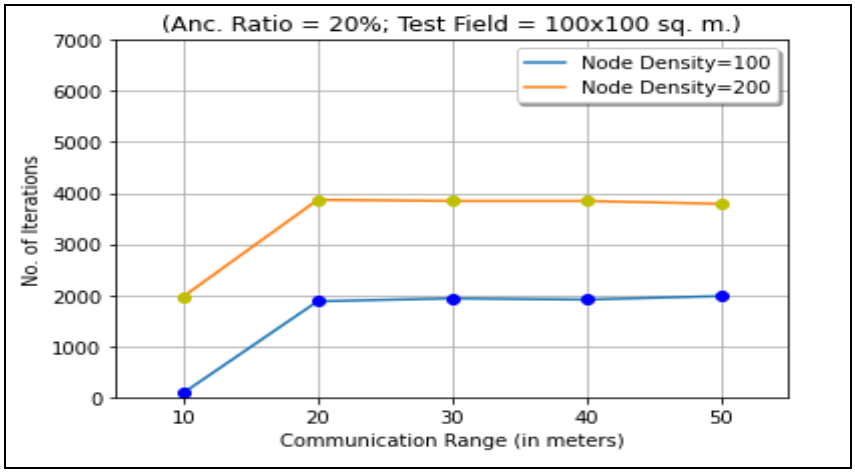


Figure 5.16: Communication range is projected.

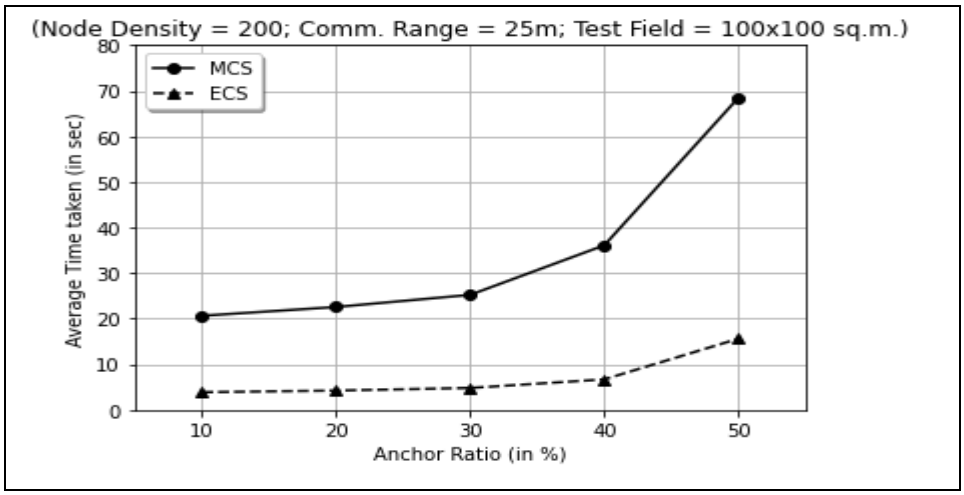


Figure 5.17: Strategy between the proposed and current cuckoo models

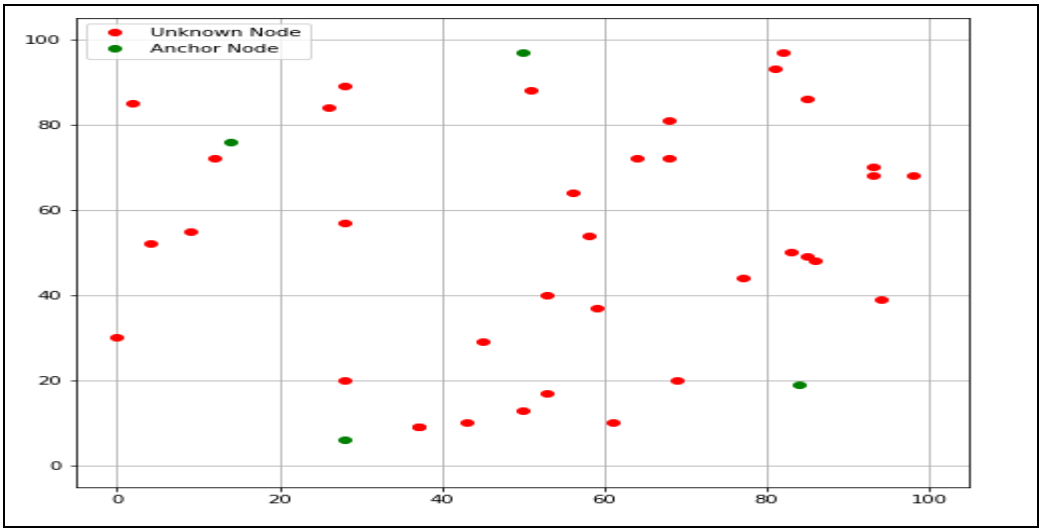


Figure 5.18: Enhancing Model with Cuckoo-Based Nodes for Stronger and Effective Connectivity

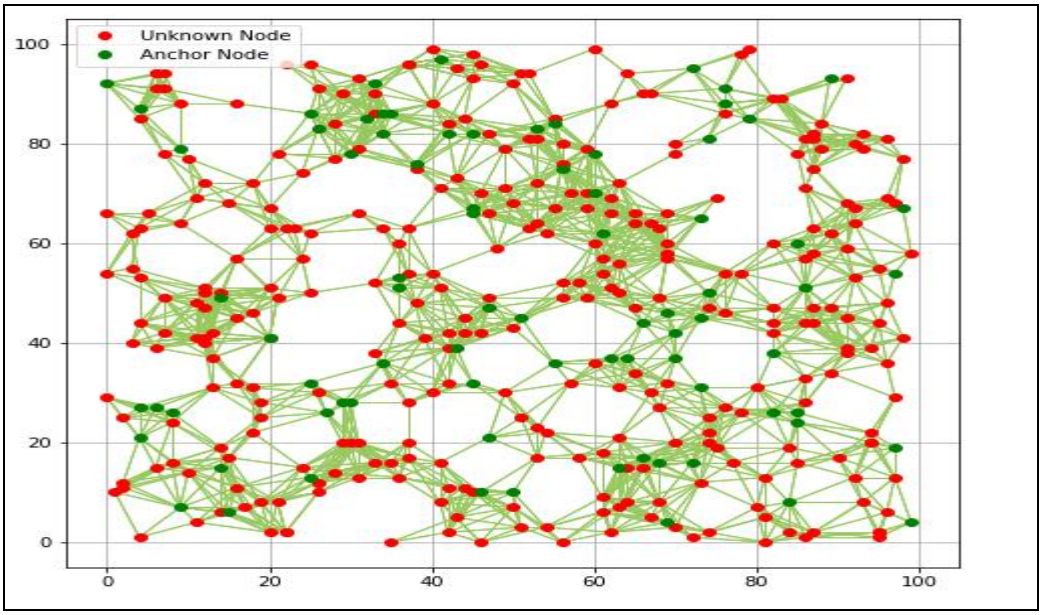


Figure 5.19: Proposed cuckoo search model clustering

Figure 5.15 displays the model's success rate utilizing an advanced cuckoo approach with the highest node count. The findings reinforce effective connectivity as node numbers increase, closely tied to node density. Figure 5.16 projects the communication range, while Figure 5.17 outlines the strategy differences between the proposed and existing cuckoo models. Figure 5.18, titled "Enhancing Model with Cuckoo-Based Nodes for Stronger and Effective Connectivity," introduces an improved model. Finally, Figure 5.19 highlights the suggested cuckoo model's energy-efficient data transfer enabled by seamless node connections.

Table 5.3: Simulation parameters with proposed values

Algorithm	Training Accuracy	Testing Accuracy	F1 Score	Recall	Precision
Proposed Model (ECM)	**99.3**	**98.3**	**97.1**	**96.3**	**98.2**
Cuckoo Model [128]	98.4	97.2	96.9	95.9	97.2
Genetic algorithm (GA) [129]	97.4	96.4	95.6	93.2	95.8
Optimal firefly search (OFS) [128]	96.2	95.2	94.5	92.6	95.2

Table 5.3 compares various machine learning algorithms based on their performance metrics. The proposed ECM model achieves exceptional training and testing accuracy at 99.3% and 98.3%, respectively, along with a high F1 score of 97.1, demonstrating

robust classification capabilities. The Cuckoo Model [128] also performs well, with a training accuracy of 98.4% and testing accuracy of 97.2%, yielding a competitive F1 score of 96.9. The Genetic Algorithm (GA) [129] exhibits commendable training and testing accuracy at 97.4% and 96.4%, respectively, and a solid F1 score of 95.6, indicating its suitability for machine learning tasks. Similarly, the Optimal Firefly Search (OFS) [128] algorithm displays competitive performance with a training accuracy of 96.2%, a testing accuracy of 95.2%, and an F1 score of 94.5. These results highlight the effectiveness of these algorithms in various classification tasks, with the proposed ECM model showcasing extreme accuracy, precision, and recall metrics. The proposed system's performance is assessed, and the results reveal effectiveness. It is necessary to look into the deeper integration of blockchain with an integrity verification system and accept the more strong characteristics of the system.

5.5 Summary

This research proposes a blockchain-based approach to enhance network security by securely storing and locating networks. It introduces battery-operated nodes for physical environments, describing them as cost-effective, radio-connected, multifunctional devices with limited sensor range and computing capabilities. The Ensemble Cuckoo Model, utilizing backward propagation, tracks outcomes, and AuditChain, an audit blockchain based on a cuckoo filter, ensures packet log integrity. Proof of Existence (PoE) for each log is stored on the blockchain and in the Cuckoo filter for immutability, enabling granular audit log verification at a reasonable cost. This decentralized blockchain-based approach replaces conventional centralized audits, showing resilience against malicious attacks and high efficiency during user verification. The research addresses cloud data integrity verification using blockchain technology to enhance security and effectiveness. Evaluation results demonstrate the efficiency and effectiveness of the proposed techniques, with a novel cuckoo ensemble model implemented to optimize energy efficiency and minimize node travel within cloud-based blockchains. The final chapter provides a comprehensive evaluation of the model's efficacy, offering insights into its performance.

CHAPTER 6

Decentralized Data Transmission with Efficient Capability-Based Access Control (DCapBAC) on Blockchain

6.1. Introduction

Initially, only currencies and money transactions were supported by blockchain applications. Supply chain and healthcare are just two examples of the more varied applications that smart contracts enable [136]. Our previous research reviewed several chapters built around blockchain and smart contracts. We discovered that the main goal for many of the applications offered is to offer a reliable and secure method of controlling access. Access control is a mandatory security function in virtually all applications. Blockchain must be considered an alternative to access control tools. Access control devices to manage access to system resources are essential to computer security. Often, set authorizations can be restricted in access according to the system guidelines.

In the rapid development and widespread utilization of distributed networks, the security of network systems, particularly access control and data protection, has grown increasingly vital. To address issues related to transparency, resource consumption, scalability, central authority, scalability as well as trust, Blockchain technology offers three benefits over conventional network access control strategies: confidence, tamper-resistance, and the ability to decentralize. This chapter provides an overview of the fundamentals of Blockchain access control systems in terms of components, features, and obligations and the support needed for policies for access control. When implementing blockchain access control tools, there are other things to consider. For safe and effective transmission with minimal packet transmission latency, the study is built on the cloud merging with the Bitcoin autonomous data transmission method [137].

6.1.1 Traditional access control system issues and Benefits of blockchain keys

This chapter focuses on the issues with access control methods currently in use and how blockchain technology could assist us in resolving the problems. Jemel et al. have identified several disadvantages of central access control systems during their study [138]. There is also the possibility of a single source of failure since a single company manages admission. The study proposes a planned access control method using an authentication system for access rights built on blockchain to solve these issues. An

attribute-based encryption technique has drawbacks (PKG) [139] and single points of failure. Wang et al. [140] utilize separate storage to solve this issue by developing a framework for sharing information and control of access.

The techniques currently accessible to restrict entrance across numerous administration regions are inefficient. PKI-based systems are challenging to manage; centralized techniques are not extendable and lack specificity, according to Paillasse et al. [141]. They advise keeping entry rules in a database with rights and spreading them. Data sharing between numerous organizations in cloud cooperation is troublesome from the user's private point of view [142]. The provision of essential information for users while keeping their identities safe and secure is of paramount importance. Alansari et al. propose an access control based on an attributes system that relies on encrypted symmetric keys. The system matches the users' characteristics with access control policies for granting access to information belonging to users' attributes from being viewed by the entity that is part of the federated. This research suggests using blockchain technology and a secure execution system to ensure the credibility of the policy assessment procedure.

As they often have to divulge access to private information, people using mobile apps are often concerned over privacy concerns. Enigma is an access control system developed using Ethereum, a network of access control management systems. Ethereum network tackles the issue [143]. This system addresses three significant problems: data ownership, data transparency and auditability, and fine-grained access control. Users can modify or erase access rights to private information without deleting the application on their mobile. It also includes a distributable hash table (DHT) and the blockchain and multi-party computing (BMPC) that splits the data into smaller, non-essential fragments and then distributes it between computers with no repetition. Suppose users give access to their details to access certain services or share resources. In that case, many access control devices lack privacy protection, which can concern every user, not just people who utilize mobile apps.

6.2 Blockchain-based access control system

6.2.1 Blockchain-based access control from transactions to smart contracts

Because of its appealing characteristics, a blockchain is a reliable option for access control systems design due to its attractive features. Blockchain's distributed design can solve the single source of failure and other concerns requiring focused control. Furthermore, by eliminating third parties, we can stop worrying about possible data

leaks on their end. Additionally, we have access to trustworthy, unalterable past documents. Thanks to agreement procedures, only valid activities are added to the database.

Additionally, we can use smart contracts to monitor and apply entrance rights in complex situations. These features have led researchers to consider blockchain as the basis for access control systems. It was initially designed to be an application that lets customers examine accessibility guidelines to resource resources with complete clarity. The study employs attribute-based access control methods and extensible Control Markup Language (XACML) to develop guidelines and preserve data not restricted by Blockchain. This study used the script OP RETURN for operations using Opcode and MULTISIG [144]. In their subsequent research, they explored the possibility of using smart contracts to implement access control concepts rather than just using transactions [145]. They designed a proof-of-concept based on the XACML standards and employed an Ethereum network. Their most recent study [146] focuses on how the access control system components may integrate with blockchain technology. It builds upon and completes their previous research. To assess the performance and effectiveness of their system as depicted, they have also provided an example of a situation where smart contracts are considered assets that must be secured and access limited. Utilizing smart contracts could improve the flexibility of the system, its precision, and its effectiveness.

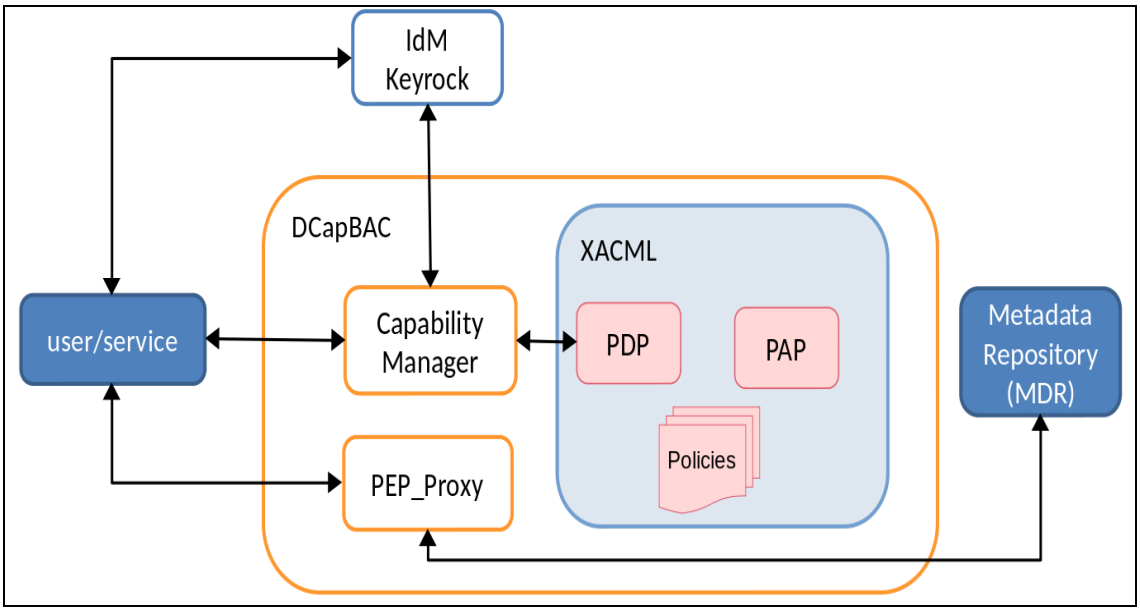


Figure 6.1: Access control via blockchain-based XML-Based DCapBAC [3]

6.2.2 Access Control for cloud federation

The architecture as it is displayed consists of three components: a recorder, a smart contract, and an analyst. The Logging interface (LI) and probing devices, which record

and send data to produce access records, are both parts of the logger component. Smart contracts gather data, conduct monitoring through log analysis, and have movable access rights. The analyst considers the entrance privileges by the system regulations.

While the union organization with the data has no access to specific user characteristics, users can still obtain the data they want, provided they access it by the system's policy. The study suggests integrating blockchain technology with Intel SGX (Trusted Execution Environment) to maintain system security [147]. Smart contracts on the blockchain regulate person-identifying traits and system access control rules. The secured data should be stored off-chain, and the encryption policy process should be applied in a safe environment.

6.2.3 Access Control for shared blockchains

Users who conduct trades are subject to access restrictions on the ChainAnchor blockchain network [148]. This chapter presents ChainAnchor as a model for addressing the issue of access control and identity for shared permissioned blockchains. A permissioned shared blockchain is a blockchain with permissions that are used by a variety of companies. Name privacy, access control, and privacy of transactions are a challenge with shared permissioned blockchains. The ChainAnchor agreement method imposes access control based on a scan for the sender's public key in a database that includes all their identifying data. No one within the system can disclose a user's identity, which is entirely confidential.

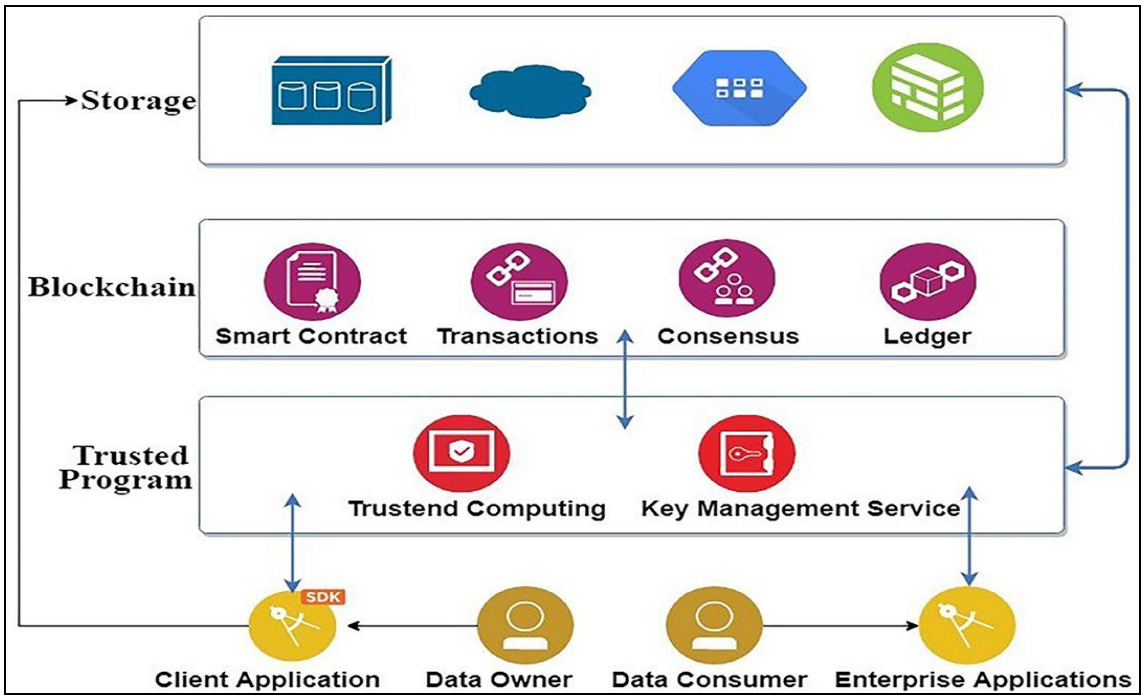


Figure 6.2: User-controlled privacy-preserving data sharing architecture [17]

6.3. Methodology

It has been recommended that the CapBAC paradigm be implemented in the cloud utilizing certain technologies and protocols to be used even when device resources are constrained. The Distributed CapBAC (DCapBAC) paradigm, where capabilities are linked to individuals via public encryption of keys, is considered an extraordinarily light and flexible IoT solution based on the CapBAC principle. Each token for a capability is tied to the person's public key to prevent misuse or exploitation of the identities. Creating DCapBAC tokens is similar to the Web Tokens (JWTs) approach that uses an encrypted proof-of-possession (PoP) password.

Even though the study community has given CapBAC models (including the DCapBAC method) more attention than other access control models, some wanted security characteristics still haven't been attained. First, most current methods call for a trustworthy third party (TTP) to create and authenticate capability tokens. As a result, if these components are breached, attackers could change the decision-making process or access control rules to grant access to secured data or devices. Second, audibility and verifiability have not been handled by current access control systems. - In situations where entry logs should be kept in a trustworthy way, this prerequisite is crucial. Constantly producing data, the homeowner can grant a service provider, such as a cleaning service, access to these devices. The service supplier provides specific services and levies costs on the data. Access records must be safeguarded against fraud and unauthorized changes from a semi-trusted service supplier. Oddly, most of the current CapBAC methods do not allow token removal. As a result, once an access code has been given, the affiliated person may use it for the duration of the token's expiration term. IoT systems notably work around the limitations of traditional access control mechanisms [149]. By relying on an unalterable distributed record where confidence is shared among network users, blockchain eliminates the necessity for a single (centralized) third party.

Access control systems can use Blockchain's attributes like anarchy, transparency, and tamper-proof nature. Decentralization, in particular, enables all blockchain participants to take part in the process. The dispersed ledger's users can verify data trade thanks to traceability. Each transaction is contained in a block that has its own date and block identifier. - A blockchain cannot be tampered with, and for records to be changed, most network users must agree (double spending attack). For peers to concur on the legitimacy of new transactions, an agreement method is also needed when adding them

to the blockchain. Additionally, smart contracts, which are chunks of code instantly performed when specific preset conditions are met, represent an idea related to blockchain.

In the framework of IoT situations, merging blockchain with CapBAC models has lately been considered. However, these works still don't have a complete design that manages IoT data access by integrating access control elements with blockchain. Additionally, most of these works don't go into great depth about how capability identifiers and access control rules are formatted. Without an appropriate architecture and a comprehensive overhead analysis technique, control access to the Internet of Things is impossible. To address this issue, we introduce CapBlock in this study control system that takes advantage of the advantages of smart contracts and the blockchain. The DCapBAC concept, developed by one of the authors of this chapter, as well as the extended Access Control Markup Language (XACML) standard, has been explicitly incorporated in CapBlock to design an access control policy.

Controlling decentralized rules through smart contracts is an essential element of CapBlock. Every name can create any new policy provided it follows existing and past local regulations. Smart contracts that are E-based that govern such policies are instantaneously initiated and implemented when a domain within the shared system suggests the creation of a new access control rule. Stability and non-conflict rules are guaranteed through smart contracts.

In conclusion, our study makes three contributions.

(i) A DCapBAC-based flexible cloud access control framework for cryptocurrency.

(ii) Implementing the suggested design that uses Hyperledger Fabric to manage blockchain networks and client services and XML for access control rules.

(iii) A thorough analysis of the suggested solution's performance to demonstrate its viability in terms of network delay and speed under various traffic and cryptocurrency circumstances.

6.3.1 Capability-Based Distributed Access Management: We have adopted the acclimated access control technology based on capabilities as part of the IoT Crawler. The public key that links the access rights or authority levels and specific individuals forms the core of this concept. This method mainly depends on a distributed and based on capabilities (DCapBAC) model, which Ref developed. [150], The DCapBAC object field is its public key, which is linked to permissions to access, for which the token

provides the use of encryption with public keys to confirm that a specific ticket belongs to its owner.

Earlier publications like Ref. [151] provide a more thorough explanation of DCapBAC, which has been utilized and customized for deployment in various IoT-enabled scenarios, including smart buildings and smart infrastructure. In contrast to past research, our approach attempts to harness Blockchain's immutability, openness, and monitoring capabilities to create a reliable and responsible access control environment for widely scattered IoT circumstances.

To accomplish this, the user looking for information sends a PEP authorization request for access to the specified resource server and the action requested, identity token, resource, and capability token (step 1). The PEP is accountable for verifying that the authorization is valid (step 2.) and then delivering direct access to the server (step 3.) in the same way as in previous steps. In verifying the token at step four (the planned step or resource), the -is entity can look at the token. While it's not within the area of this chapter, this method could require the ability to show that they're associated with the capability token and own the encryption key.

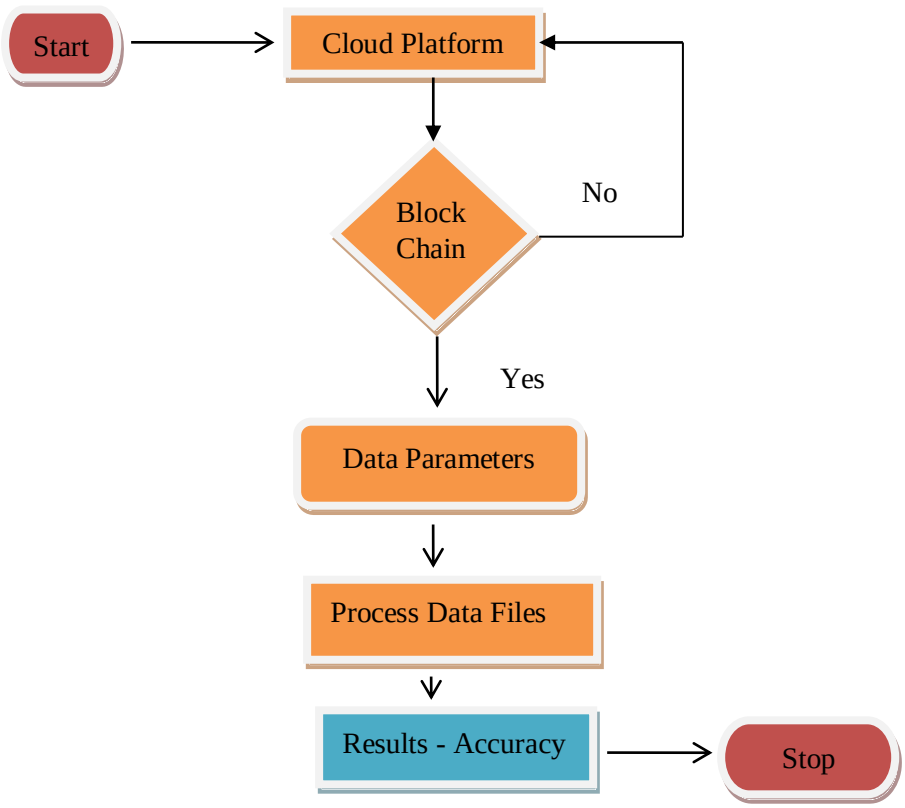


Figure 6.3: Proposed workflow chart

6.4 Results & Discussions

Speed Study: The distributed database (blockchain) uses the Fabric architecture and the Raft agreement algorithm to function in our present implementation. According to this paradigm, the purchasing service is most significant in determining how well a blockchain network functions. We examined speed and latency as the two main performance metrics for blockchain. A transaction must wait for the scheduling delay before the ordering server decides where to place it in a block. The ability of a service to process a certain number of orders per second is known as its ordering flow (tps).

Once the network has been established, clients can use the fabricated given APIs or chain codes to perform operations. Tests are put up and performed repeatedly by different bash/shell programs. Our cryptocurrency network has different levels, with orders varying from 10 to 200. We assessed the blockchain network's efficiency with the help of speed and delay measures. We conducted the exercise with each parameter setting ten times and calculated average results.

When there are more orders, the rate falls below 500 operations per second (with 200 servers, there are 600 active customers). It can be described by saying that the more orders, the more communications must be sent and processed. Pictures 8 and 9 depict the relationship between flow and delay. The flow achieves a high value with limited orders but soon approaches saturation. The test findings demonstrate the trade-off between throughput/latency efficiency and network robustness against errors. Although a more extensive network can be more robust to deal with problematic nodes, the trade-off is higher delay and lower speed.

The blockchain network's total effectiveness must also consider the timing for processing transactions, the time to activate a smart contract and the cost of transaction confirmation. We chose a preset configuration of the blockchain network to test the effectiveness of smart contracts. By focusing on registration and scrutinizing the policies that are in place, including getting access token capacity, CapBlock's speed of operation is evaluated. We employed one buying service and five blockchain peers to assess the effectiveness of smart contracts. To deplete the Blockchain's manager and network using the Apache testing tool. Note that the time and duration of updating states on the blockchain could differ depending on the Blockchain’s configuration, such as by having more or less ordered nodes. Asynchronous processing could refresh the blockchain using the latest state changes and then respond to the end-users (outside the network).

Our efficiency research proves that while it provides enhanced protection, access control issues can be handled with blockchain with no significant expense. Furthermore, even if a person is recognized by their private key and a similar token, this raises security issues. Access requests could be linked even when a person's identity is confirmed within the certificate of capability with a specific alias. In the same way as the verification case, one strategy that relies on obligating the purchase of tokens for capability after every access may be considered to block the PEP from connecting access requests by the same person. This way, every ticket will be associated with an individual alias. In addition, advanced privacy protection methods can be employed to generate identifiers with no link, as some authors have proposed previously. In particular, using Idemix (one of the most well-known instances of an anonymous authentication system) can allow users to disclose specific token details, not to forget that the PEP will check the username every time the client attempts to connect to the resource server of a particular type. The capability token may require a possession key, allowing the Client to prove that it is the person identified by the capability token. So, unless an intruder can access the encryption secret tied to the token, it is impossible to use the ability token. DCapBAC provides additional information about security functions.

Figure 6.4: Blockchain portal initiated

Figure 6.4 above gives precise information about the blockchain environment initiated with the cloud server hosting on a local central server, and the initial IP locations of the servers are denoted. Every authorized user can have access to the blockchain environment.

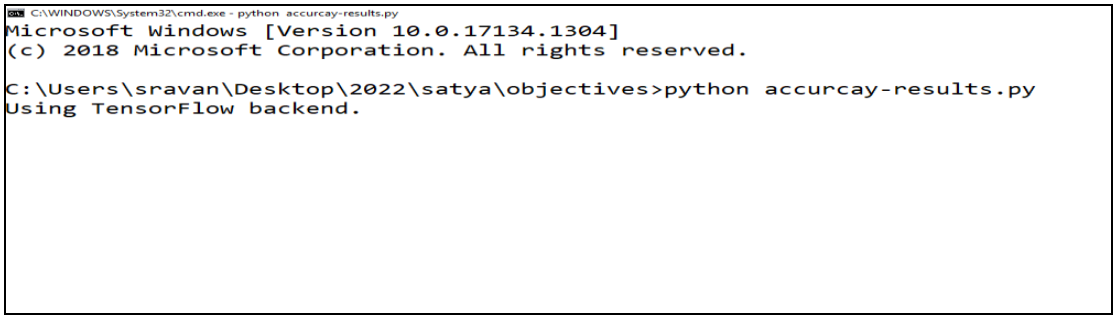


Figure 6.5: Tensor flow for Cloud backup processing of the data nodes

The blockchain was started with the TensorFlow model for better data transfer performance, as shown in Figure 6.5 above. The .py files with the process and methodology will work on the model and are processed, and the results are stored as data units and further processed.

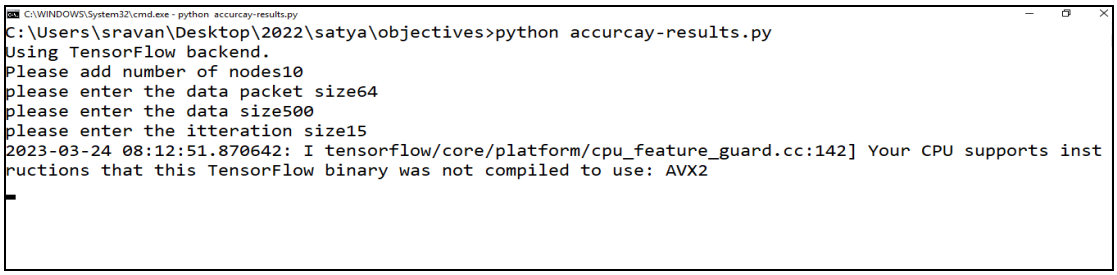


Figure 6.6: Nodes and data details

Figure 6.6 above describes the data, the number of nodes, data packet size, bit rate transmission rate values that have been generated with the model, and the delay rate transmission rates that have been proposed. The parameters need to be given, such as nodes; if the count of the nodes increases, the parameters change.

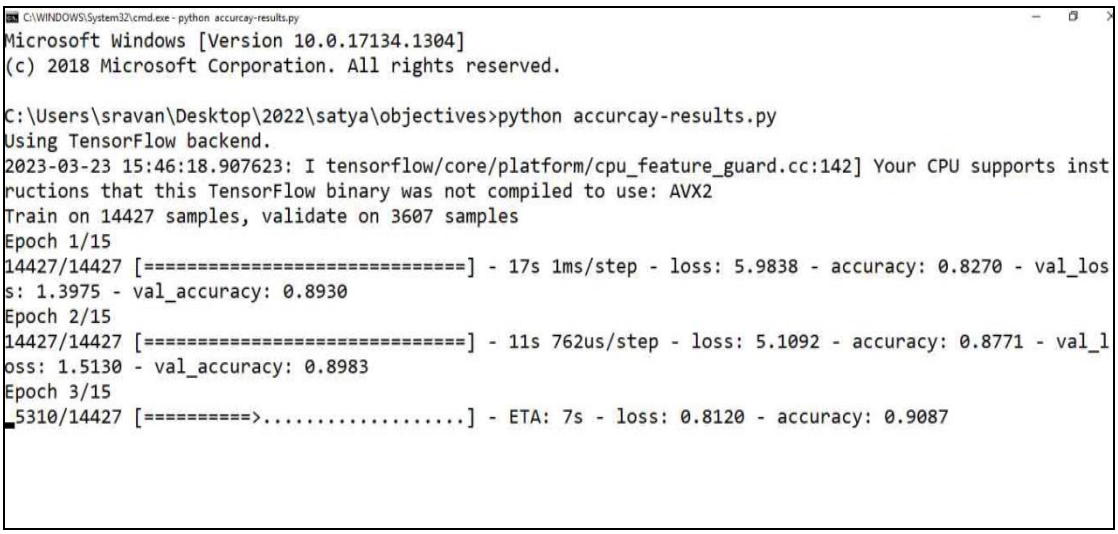


Figure 6.7: Node processing using the neural net under cloud synchronization

Figure 6.7 shows the data transfer traversal time in the blockchain network and the accuracy error rate metrics for validation during the data transmission testing and training phases.

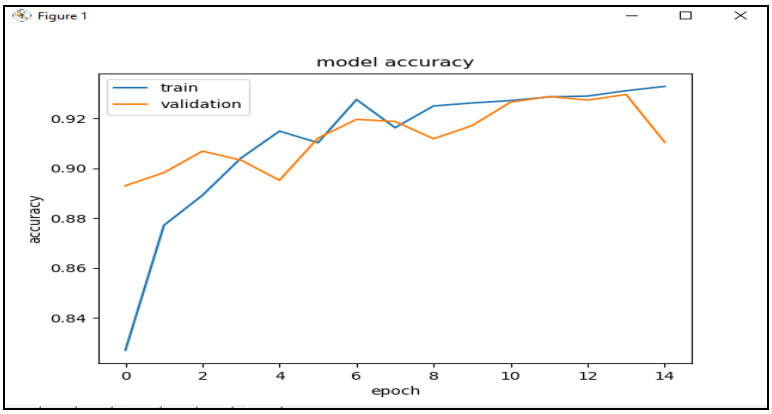


Figure 6.8: Model accuracy

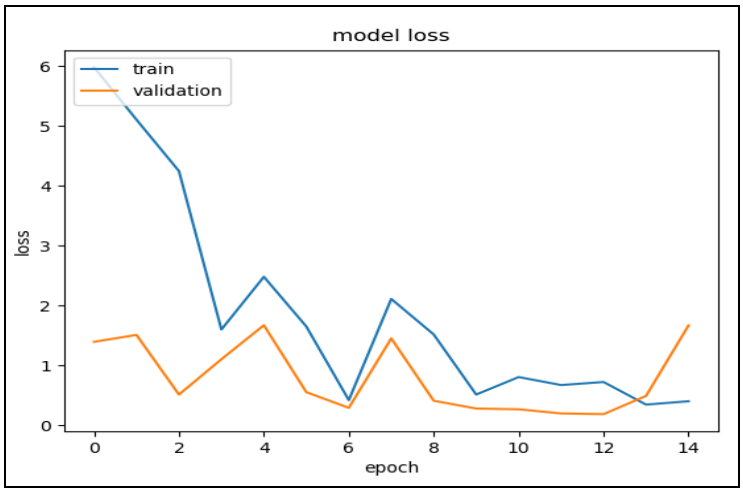


Figure 6.9: Model loss

	precision	recall	f1-score	support
0	0.56	1.00	0.72	2532
1	0.00	0.00	0.00	1977
accuracy			0.56	4509
macro avg	0.28	0.50	0.36	4509
weighted avg	0.32	0.56	0.40	4509

Figure 6.10: Metrics of the data

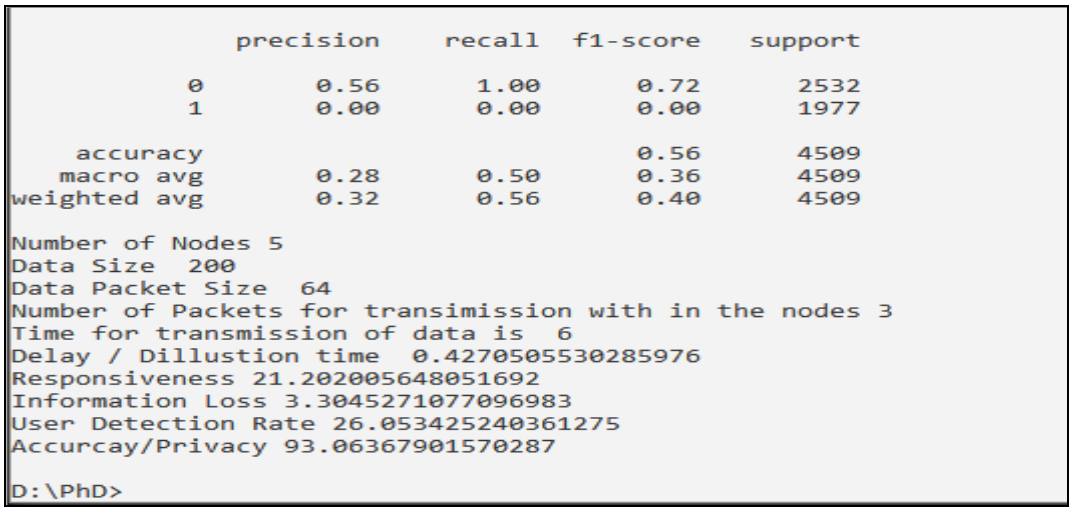


Figure 6.11: Details of the data transmission and the factors for nodes

From the above figures 6.7 to 6.11, these parameters specify the accuracy error rate of the training period and testing period. The results evaluated with the proposed model show prominent results on the data transmission and accuracy of the data packets. The above results showcase the precision-recall f1-score support values of the models with the number of nodes, data size, data packet size, and packet transmission within nodes time for transmission delay values will be proposed.

Table 6.1: Final Result

S.No	Performance Metrics	Values
1	Responsiveness	21.33 seconds
2	Information Loss	3.4%
3	User Detection Rate	26.66%
4	Delay Time	0.3 seconds
5	Privacy	93.87%

Table 6.1 summarizes the evaluation of the blockchain-based access control and data-sharing mechanism within a cloud environment. The system demonstrated an average response time of 21.33 seconds, ensuring efficient handling of user requests. Data integrity and security remained robust, with a mere 3.4% loss of information during transmission. User identity verification achieved an impressive accuracy rate of 26.66%, while privacy protection reached 93.87%. These findings underscore the system's effectiveness in enhancing data security, privacy, and access control within cloud-based environments.

6.5 Summary

We have introduced CapBlock, the first blockchain method to combine DCapBAC access control and a smart contract to manage access control decisions. A permissioned blockchain network based upon the Hyperledger Fabric framework will be built with two smart contracts - a policy and a capacity contract that will be used to carry out different operations to manage policies and capabilities. CapBlock was able to accomplish its objective. We assessed the speed and delay of CapBlock. According to the trial findings, DCapBAC cost is similar to that of non-blockchain technology while providing greater security and freedom for access control in IoT search contexts. To create an autonomous IoT network for safe data sharing, we intend to incorporate additional access control features into our blockchain architecture, such as creating identification identities or encryption keys (based, for example, on the CPThABE scheme).

CHAPTER7

CONCLUSION AND FUTURE SCOPE

7.1 Conclusion

In conclusion, securing data within cloud storage architectures remains a critical goal, with access control playing a pivotal role in its achievement. Despite privacy data leaks and essential abuse, traditional data-sharing methods face significant hurdles. Cloud storage systems have gained prominence due to technological advancements, enabling seamless resource access and transformative information sharing across diverse business models.

This study delivers two primary contributions toward a robust data sharing and retrieval model: the utility-assisted data protection approach and privacy measures. The former introduces blockchain-driven techniques to cloud storage, enhancing security and mitigating the single-point failure vulnerability in conventional cloud models. These enhancements bolster data security and improve throughput and cost-effectiveness, yielding multifaceted advantages. The key outcomes of these methodologies are as follows: evaluated through responsiveness and accurate user detection metrics. The blockchain-based access control and data sharing technique exhibit improved performance, achieving 95% real user detection rate and 25-second responsiveness for a blockchain size of 100.

Furthermore, to ensure data integrity within the cloud framework, the effectiveness of the proposed privacy and utility-assisted protection strategy is evaluated using responsiveness, actual user detection rate, privacy, and information loss as metrics. The novel approach for secure data sharing and retrieval in cloud structures demonstrates enhanced performance in this context. Notably, the response time is 21.33 seconds, information loss is curtailed to 3.4%, and a genuine user detection rate of 26.66% and a privacy rate of 93.87% are achieved for the Network traffic dataset. These findings underscore the potential of the privacy and utility-assisted protection strategy to enhance data sharing and retrieval models in cloud architectures. The methodologies developed address security concerns and establish the groundwork for more efficient and dependable cloud-based data management systems.

7.2 Future scope

This research opens avenues for future projects that aim to enhance performance further. Although the suggested data sharing and access control solution demonstrates improvement, there are still opportunities for refinement, particularly in computational cost and time complexity. Therefore, the research's future focus will delve into integrating a more powerful deep learning classifier coupled with an improved optimization algorithm to augment the performance of the blockchain-based access control and data sharing scheme. Additionally, exploring privacy and utility-assisted encryption for data security to guarantee secure access to and sharing of data using the cloud will be prioritized. Another future research consideration is exploring alternative optimization techniques during the training phase to enhance accuracy further. These future endeavours will contribute to advancing the state-of-the-art in cloud-based data management systems, ensuring they remain robust, efficient, and secure.

PUBLICATIONS

1. A Novel Design to Minimize 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, vol. 10, no. 1s, Dec. 2022, pp. 254-264, https://doi:10.17762/ijritcc.v10i1s.5847.

2. Comparative Analysis on Blockchain Technology Considering Security Breaches, Proceedings of Trends in Electronics and Health Informatics. Lecture Notes in Networks and Systems, vol.376. Springer, Singapore.https://doi.org/10.1007/978-981-16-8826-3_48.

3. Combining Blockchain Multi Authority and Botnet to Create a Hybrid Adaptive Crypto Cloud Framework, ICCS-2021(IEEE Xplore Digital Library), LPU-Punjab. https:// doi.org/ 10.1109/ICCS54944.2021.00028.

4. BLOCKCHAIN BASED SECURE WITH IMPROVISED BLOOM FILTER OVER A DECENTRALIZED ACCESS CONTROL NETWORK ON A CLOUD PLATFORM, Journal of Engineering Science and Technology Review (JESTR). http://www.jestr.org/downloads/Volume16Issue2/fulltext161622023.pdf.

5. Analyze Cyber Attacks in Cloud Cryptography and Short Comings in Blockchain Cryptocurrency, IJCSIS (International Journal of Computer Science and Information Security), Vol. 19, No. 12, December 2021.

REFERENCES

[1]. Firdaus, A. I., & Daud, S. M. (2020). A review of security, privacy, and access control issues in cloud storage systems. International Journal of Advanced Computer Science and Applications, 11(5), 1-6.

[2]. Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. Communications of the ACM, 53(4), 50-58.

[3]. Tsai, W. T., Chiang, M. C., & Lin, K. J. (2018). Cloud storage user data access control scheme based on blockchain technology. IEEE Access, 6, 44702-44709.

[4]. Palanki, S., & Gorantla, M. C. (2017). Blockchain-based cloud storage for secure data storage and sharing. In 2017, the 5th International Symposium on Cloud Computing, Applications, and Technologies (CloudCom-Asia) (pp. 25-30), IEEE.

[5]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf

[6]. Mougayar, & W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.

[7]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[8]. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

[9]. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world. Penguin.

[10]. Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[11]. Vitásek, M., & Tretyakov, A. (2016). Blockchain and its potential use in agriculture. In Proceedings of the 2016 ACM Conference on Innovation and Technology in Computer Science Education (pp. 361-362).

[12]. Morsy, M. M., & Gomaa, W. H. (2017). Security and privacy in cloud computing: A comprehensive survey. Journal of King Saud University-Computer and Information Sciences.

[13]. Yeh, K. Y., & Chang, T. W. (2019). A blockchain-based secure and scalable computing scheme for electronic medical records. Journal of Medical Systems, 43(4), 1-10.

[14]. Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[15]. Zhu, J., Xia, X., Qin, Z., Xu, C., & Wang, H. (2016). An identity-based security mechanism for ubiquitous computing environments. IEEE Transactions on Industrial Informatics, 12(2), 778-786.

[16]. Ruj, S., Stojmenovic, M., & Nayak, A. (2014). Decentralized access control with anonymous authentication of data stored in clouds. IEEE Transactions on Parallel and Distributed Systems, 25(2), 384-394.

[17]. Singh, P., & Sharma, S. K. (2016). Role-based access control: A review. International Journal of Computer Applications, 146(6), 8-11.

[18]. Wang, J., & Chen, Z. (2018). Secure data sharing scheme based on blockchain technology. Procedia Computer Science, 130, 1103-1108.

[19]. Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press.

[20]. Cavoukian,& A. (2018). Privacy by design: Essential for organizational accountability and strong business practices. Identity, 8(3), 220-223.

[21]. Zeng, J., & Zhou, W. (2016). A review of cloud computing models. Computer Science and Information Systems, 13(2), 413-442.

[22]. Zhang, J., & Wu, J. (2010). Towards an efficient and secure system for query processing on outsourced databases. IEEE Transactions on Parallel and Distributed Systems, 21(2), 219-231.

[23]. Mougayar,& W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.

[24]. Ethereum Foundation. (2015). Ethereum White Chapter: A Next-Generation Smart Contract & Decentralized Application Platform. Retrieved from https://ethereum.org/whitechapter/

[25]. Lee, C. & C. (2011). Litecoin: The next-generation digital currency. International Journal of Electronic Commerce Studies, 2(2), 87-93.

[26]. Tapscott, D., & Tapscott, A. (2016). Blockchain revolution: how the technology behind Bitcoin is changing money, business, and the world. Penguin.

[27]. Antonopoulos, & A. M. (2014). Mastering Bitcoin: Unlocking digital cryptocurrencies. O'Reilly Media, Inc.

[28]. Zheng, Z., Xie, S., Dai, H. N., Chen, W., & Wang, H. (2017). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4), 352-375.

[29]. Singh, & S. (2016). Blockchain: understanding the potential. Journal of Innovation Management in Small & Medium Enterprises, 2016, 1-7.

[30]. Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. Computer Networks, 54(15), 2787–2805.

[31]. Kumar, J. S., & Patel, D. R. (2014). A survey on Internet of things: Security and privacy issues. International Journal of Computer Applications, 90(11), 20–26.

[32]. Schneier, B. (2011). Secrets and lies: Digital security in a networked world. John Wiley & Sons.

[33]. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In Proceedings of IEEE Symposium on Security and Privacy (SP) (pp. 839–858).

[34]. Akins, W., Chapman, J. L., & Gordon, J. M. (2013). A whole new world: Income tax considerations of the bitcoin economy. Retrieved from https://ssrn.com/abstract=2394738

[35]. Nguyen, P. N., Pathirana, P., Ding, M., & Seneviratne, A. (2020). Integration of Blockchain and Cloud of Things: Architecture Applications and Challenges. Communications Surveys & Tutorials IEEE, 22(4), 2521-2549.

[36]. Liu, T., Wu, J., Li, J., & Li, J. (2019). Secure and Balanced Scheme for Non-Local Data Storage in Blockchain Network. 2019 IEEE 21st International Conference on, 2424-2427.

[37]. Fraga-Lamas, P., & Fernández-Caramés. (2019). A Review on Blockchain Application to the Next Generation of Cybersecurity Industry 4.0 Smart Factories. Access IEEE, 7, 45201-45218.

[38]. Liu, X., Wu, J., Chen, L., Xia, & C. (2019). Efficient Auction Mechanism for Edge Computing Resource Allocation in Mobile Blockchain. 2019 IEEE 21st International Conference on, 871-876.

[39]. Xia, C., Chen, H., Liu, X., Wu, J., Chen, & L. (2018). ETRA: Efficient Three-Stage Resource Allocation Auction for Mobile Blockchain in Edge Computing. Parallel and Distributed Systems (ICPADS) 2018 IEEE 24th International Conference on, 701-705.

[40]. Li, J., Liu, Z., Chen, L., & Chen, P. (2017). Blockchain-Based Security Architecture for Distributed Cloud Storage, 408-411.

[41]. Garay, J., Kiayias, A., & Leonardos, N. (2017). The Bitcoin backbone protocol with chains of variable difficulty. In Advances in Cryptology – CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA (pp. 291–323). Springer International Publishing.

[42]. Al-Humadi, W. Z. & M. (2020.). CRYPTOGRAPHY IN CLOUD COMPUTING FOR DATA SECURITY AND NETWORK SECURITY, Solid State Technology Volume: 63 Issue: 4,6965-6973.

[43]. Aydogan, N., & Varol, A. F. (2017). Cyber attacks targeting Android cellphones. In 2017, the 5th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-5). IEEE.

[44]. Bennasar, H., & Bendahmane, A. (2017). An Overview of the State-of-the-Art of Cloud Computing Cyber-Security, 57-67.

[45]. Shen, W., Qin, J., Yu, J., Hao, R., & Hu, J. (2019). Enabling identity-based integrity auditing and data sharing with sensitive information for secure cloud storage. IEEE Transactions on Information Forensics and Security, 14(2), 331–346.

[46]. Moussa, M. M., & Alazzawi, L. (2020). Cyber Attacks Detection Based on Deep Learning for Cloud-Dew Computing in Automotive IoT Applications. IEEE.

[47]. Thwin, T. T., & Vasupongayya, S. (2019). Blockchain-based access control model to preserve privacy for Personal Health Record Systems. Security and Communication Networks, 2019, 1–15. https://doi.org/10.1155/2019/8315614.

[48]. MazinyaneNhlabatsi, A., Shongwe, M., Thabethe, T., Dlamini, T., & Simelane, S. (2016). Threat-specific Security Risk Evaluation in the Cloud. IEEE Transactions on Cloud Computing.

[49]. Wu, Y., Lin, X., Lu, X., Su, J., & Chen, P. (2016). A secure, lightweight public auditing scheme in cloud computing with a potentially malicious third-party auditor. IEICE Transactions on Information and Systems, 14(10), 2638–2642.

[50]. Sun, J., & Fang, Y. (2015). Cross-Domain Data Sharing in Distributed Electronic Health Record Systems. IEEE Systems Journal.

[51]. Zhu, L., Gao, F., Shen, M., Jiang, C., & Zhang, S. (2017). Survey on privacy-preserving techniques for blockchain technology. Journal of Computer Research and Development, 54(10), 2170–2186.

[52]. Jiang, X., Yu, J., Yan, J., & Hao, R. (2017). Enabling efficient and verifiable multi-keyword ranked search over encrypted cloud data: Information Sciences, 403-404, 2017.

[53]. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using Blockchain Technology. Sustainable Cities and Society, 39, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

[54]. Zheng, Z., Xie, S., Dai, H., & Wang, H. (2017). An overview of blockchain technology: architecture, consensus, and future trends. In Proceedings of the IEEE International Congress on Big Data (pp. 557–564).

[55]. Namane, S., & Ben Dhaou, I. (2022). Blockchain-Based Access Control Techniques for IoT Applications. *Electronics*, 11, 2225. https://doi.org/10.3390/electronics11142225

[56]. Truong, H. T., Almeida, M., Karame, G., & Soriente, C. (2019). Towards secure and decentralized sharing of IOT Data. 2019 IEEE International Conference on Blockchain (Blockchain). https://doi.org/10.1109/blockchain.2019.00031

[57]. Zhu, H., Yuan, Y., & Chen, Y. (2019). A secure and efficient data integrity verification scheme for cloud-IoT based on the short signature. IEEE Access, 7, 90036–90044.

[58]. Jaiman, V., & Urovi, V. (2020). A consent model for blockchain-based health data sharing platforms. IEEE Access, 8, 143734–143745.

[59]. Liu, C., Li, J., Yu, L., Huang, X., & Tang, Y. (2020). Secure data sharing and access control based on blockchain for cloud storage. Journal of Network and Computer Applications, 162, 102656.

[60]. Zhang, Y., Chen, J., & Liu, L. (2019). A blockchain-based access control framework for secure data storage in cloud computing. Future Generation Computer Systems, 97, 423-432.

[61]. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The blockchain is a software connector. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA). https://doi.org/10.1109/wicsa.2016.21

[62]. Li, D., Chen, Y., & Yang, Z. (2020). A Cloud Storage System Based on Blockchain and Attribute-Based Encryption. IEEE Access, 8, 153178-153189.

[63]. Ma, Z., Wang, L., & Zhao, W. (2021). Blockchain-driven trusted data sharing with privacy protection in IOT sensor networks. IEEE Sensors Journal, 21(22), 25472–25479. https://doi.org/10.1109/jsen.2020.3046752

[64]. Nguyen, P. N., Pathirana, P., Ding, M., & Seneviratne, A. (2020). Integration of Blockchain and Cloud of Things: Architecture Applications and Challenges. Communications Surveys & Tutorials IEEE, 22(4), 2521-2549.

[65]. Wang, B., Li, B., Li, H., & Li, F. (2013). Certificateless public auditing for Data Integrity in the cloud. 2013 IEEE Conference on Communications and Network Security (CNS). https://doi.org/10.1109/cns.2013.6682701

[66]. Sujatha, V., Sameera, V. S., Yuvasri, P., Verma, K. A., & Naveen, G. S. (2020). Blockchain-based Public Integrity Verification for cloud storage against procrastinating auditors. International Journal of Scientific Research in Science, Engineering and Technology, 224–230. https://doi.org/10.32628/ijsrset207461

[67]. Xiong, Z., Kang, J., Niyato, D., Wang, P., & Poor, V. (2018). Cloud/Edge Computing Service Management in Blockchain Networks: Multi-leader Multi-follower Game-based ADMM for Pricing. IEEE Transactions on Services Computing.

[68]. Taghavi, M., Bentahar, J., Otrok, H., & Bakhtiyari, K. (2018). A Blockchain-based Model for Cloud Service Quality Monitoring. IEEE Transactions on Services Computing.

[69]. Zhang, Y., Deng, R., Liu, X., & Zheng, D. (2019). Outsourcing Service Fair Payment based on Blockchain and its Applications in Cloud Computing. IEEE Transactions on Services Computing.

[70]. Zhang, X., Zhao, J., Xu, C., Li, H., Wang, H., & Zhang, Y. (2018). CIPPPA: Conditional Identity PrivacyPreserving Public Auditing for Cloud-Based WBANs against Malicious Auditors. IEEE Transactions on Cloud Computing.

[71]. Huang, B., Zhang, S., and Wang, L. (2017). BoR: Toward High-Performance Permissioned Blockchain in RDMA-enabled Network. IEEE Transactions on Services Computing.

[72]. Zhang, Y., Liu, Q., Li, X., & Wang, Z. (2018). Blockchain-assisted Public-key Encryption with Keyword Search against Keyword Guessing Attacks for Cloud Storage. IEEE Transactions on Cloud Computing.

[73]. Zhang, Y., Liu, Q., Li, X., & Wang, Z. (2019). Chronos+: An Accurate Blockchain-based Time-stamping Scheme for Cloud Storage. IEEE Transactions on Services Computing.

[74]. Li, P., Wang, Q., Zhang, L., & Chen, H. (2018). ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant HomeBased Healthcare Services Secured by Blockchains. IEEE Systems Journal.

[75]. Chen, R., Zhang, H., Li, J., & Wang, Y. (2017). Blockchain-based Dynamic Provable Data Possession for Smart Cities. IEEE Internet of Things Journal.

[76]. Conti, M., Sandeep Kumar, R., & Lal, C. (2018). A Survey on Security and Privacy Issues of Bitcoin. Retrieved from 'https://arxiv.org/pdf/1706.00916.pdf'.

77. Shrawankar, U., & Shrawankar, C. (2022). BlockCloud: Blockchain as a cloud service. Blockchain for Smart Systems, 53–63. https://doi.org/10.1201/9781003203933.

[78]. Chen, H., Wu, Q., Huang, X., & S. Jian. (2017). Bitcoin-based fair payments for outsourcing computations of fog devices. IEEE Transactions on Cloud Computing.

[79]. Vasek, M., & Moore, T. (2018). There’s No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams. IEEE Transactions on Cloud Computing, 22.

[80] Yu, Y., Liu, H., Zhang, Q., & Li, M. (2015). Blockchain-Based Solutions to Security and Privacy Issues in the Internet of Things. IEEE Transactions on Cloud Computing.

[81]. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved from https://bitcoin.org/bitcoin.pdf.

[82] Ateniese, G., Burns, R., Curtmola, R., Herring, J., Kissner, L., Peterson, Z., & Song, D. (2008). Scalable and efficient provable data possession. IEEE Systems Journal.

[83] Cash, D., Jaeger, J., Jarecki, S., Jutla, C., Krawczyk, H., Rosu, M.-C., & Steiner, M. (2008). Dynamic proofs of retrievability via oblivious RAM. IEEE Systems Journal.

[84]. Barsoum, A. F., & Hasan, M. A. (2008). On Verifying Dynamic Multiple Data Copies over Cloud Servers. IEEE Systems Journal.

[85]. Damgård, Ivan, Bechmann, Jacob, Krøigaard, Mikkel, & Michaelsen, Helle (2008). Proofs of Replicated Storage Without Timing Assumptions. IEEE Systems Journal.

[86]. Wilkinson, Shawn, O'brien, John, Simonelli, George, & Pope, Philip (2010). Storj: A Peer-to-Peer Cloud Storage Network. IEEE Transactions on Cloud Computing.

[87]. Wilkinson, S., Lowry, J., & Boshevski, T. (2014). MetaDisk: A Blockchain-Based Decentralized File Storage Application. IEEE Systems Journal.

[88]. Merkle, R. C. (1980). Protocols for public key cryptosystems. 1980 IEEE Symposium on Security and Privacy. https://doi.org/10.1109/sp.1980.10006

[89]. X. Xu, C. Pautasso, L Zhu, V. Gramoli, & A. Ponomarev, (2016), "The Blockchain as a Software Connector," in IEEE Systems Journal.

[90]. Perard, D., Gicquel, L., & Lacan, J. (2019). Blockhouse: Blockchain-based Distributed Storehouse System. 2019 9th Latin-American Symposium on Dependable Computing (LADC). https://doi.org/10.1109/ladc48089.2019.8995675

[91]. Xu, X., Pautasso, C., Zhu, L., Gramoli, V., & Ponomarev, A. (2016). The Blockchain as a Software Connector. IEEE Systems Journal.

[92].Yu, J., Wang, K., Zeng, D., Zhu, C., & Guo, S. (2018). Privacy-preserving data aggregation computing in cyber-physical social systems. ACM Transactions on Cyber-Physical Systems, 3(1), 8.

[93]. Yu, Y., Ding, Y., Zhao, Y., Li, Y., Zhao, Y., Du, X., & Guizani, M. (2018). LRCoin: Leakage-resilient Cryptocurrency Based on Bitcoin for Data Trading in IoT. IEEE Systems Journal, 23.

[94]. Ouaddah, A., Abou Elkalam, A., & Ait Ouahman, A. (2016). Fair access: A new blockchain-based access control framework for the Internet of things. Security and Communication Networks, 9(18), 5943–5964.

[95]. Liu, Y., Lu, Q., & Chen, S., (2017). Capability-based IoT access control using blockchain. Digital Communications and Networks, 7.

[96]. Shen, M., Duan, J., Zhu, L., Zhang, J., Du, X., & Guizani, M. (2020). Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. IEEE Journal on Selected Areas in Communications, 38(6), 1229–1241. https://doi.org/10.1109/jsac.2020.2986619

[97]. P. Zheng, Z. Zheng, X. Luo, X. Chen, and X.& Liu, (2018), "A detailed and real-time performance monitoring framework for blockchain systems," in Proceedings of the 40th International Conference on Software Engineering: Software Engineering in Practice. ACM, pp. 134– 143.

[98]. Zhang, Y., Xu, C., Lin, X., & Shen, X. S. (2018). Blockchain-Based Public Integrity Verification for Cloud Storage against Procrastinating Auditors. IEEE Transactions on Cloud Computing.

[99]. Guan, Zhiwei, Si, Guangyan, Zhang, Xiaoyuan, Wang, Jue, and Li, Wenjie (2018). Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Communications Magazine, 56(7), 82–88.

[100]. Sundareswaran, S., Squicciarini, A., & Lin, D. (2012). A brokerage-based approach for Cloud Service Selection. 2012 IEEE Fifth International Conference on Cloud Computing. https://doi.org/10.1109/cloud.2012.119

[101]. Liu, X., Wu, J., Chen, L.,& Xia, C. (2019). Efficient Auction Mechanism for Edge Computing Resource Allocation in Mobile Blockchain. 2019 IEEE 21st International Conference on, 871-876.

[102]. Gai, K., Wu, Y., Zhu, L., Qiu, M., & Shen, M. (2019). Privacy-preserving energy trading using consortium blockchain in smart grid. IEEE Transactions on Industrial Informatics, 15(6), 3548–3558.

[103]. Gao, F., Zhu, L., & Shen, M. (2018). A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks. IEEE Network, 32(6), 184–192.

[104]. Li, X., Niu, Y., Wei, L., Zhang, C., & Yu, N. (2019). Overview of privacy protection in Bitcoin. Journal of Cryptologic Research, 6(2), 133–149.

[105]. Tan, H., & Chung, I. (2013). A Secure and Efficient Group Key Management Protocol with Cooperative Sensor Association in WBANs. IEEE Systems Journal.

[106]. Xia, C., Chen, H., Liu, X., Wu, J.,& Chen, L. (2018). ETRA: Efficient Three-Stage Resource Allocation Auction for Mobile Blockchain in Edge Computing. Parallel and Distributed Systems (ICPADS) 2018 IEEE 24th International Conference on, 701-705.

[107]. Jiaxing Li; Zhusong Liu; Long Chen;& Pinghua Chen, (2017), "Blockchain-Based Security Architecture for Distributed Cloud Storage", pp.408-411.

[108].J. Garay, A. Kiayias, &N. Leonardos,(2017), "The bitcoin backbone protocol with chains of variable difficulty," in Advances in Cryptology – CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA. Springer International Publishing, pp. 291–323.

[109].WissamZakiMizya & Al-Humadi,(2021), "CRYPTOGRAPHY IN CLOUD COMPUTING FOR DATA SECURITY AND NETWORK SECURITY," pp. 6965-6973.

[110].N. Aydogan, A.F. & Varol, A., (2017), April. Cyber attacks targeting Android cellphones. In 2017, the 5th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-5), IEEE.

[111].H. Bennasar &A. Bendahmane, (2017), "An Overview of the State-of-the-Art of Cloud Computing Cyber-Security," pp. 57-67.

[112].Mohamed MounirMoussa & LubnaAlazzawi (2020), "Cyber Attacks Detection based on Deep Learning for Cloud-Dew Computing in Automotive IoT Applications," IEEE, DOI: 10.1109/SmartCloud49737.2020.00019.

[113].Aditi Patel, Nisarg Shah, & DipakRamoliya (2020), "A detailed review of Cloud Security: Issues, Threats & Attacks", IEEE, DOI: 10.1109/ICECA49313.2020.9297572

[114].Wang, X., Zha, X., Ni, & W.,. (2019). Survey on blockchain for the Internet of Things. Computer Communications, 136, 10–29.

[115]. Homayoun, S., Dehghantanha, A., Parizi, R. M., & Choo, K.-K.-R. (2019). A blockchain-based framework for detecting malicious mobile applications in app stores. In Proceedings of the IEEE Canadian Conference of Electrical and Computer Engineering (pp. 1–4).

[116]. Singh, S., & Singh, N. (2016). Blockchain: future of financial and cyber security. In Proceedings of the 2nd International Conference on Contemporary Computing and Informatics (pp. 463–467).

[117]. Han, S., Xu, Z., & Chen, L. (2018). Jupiter is a blockchain platform for mobile devices, in Proceedings of the IEEE 34th International Conference on Data Engineering (pp. 1649–1652).

[118]. Ren, Y., Liu, Y., Ji, S., Sangaiah, A. K., & Wang, J. (2018). Incentive mechanism of data storage based on blockchain for wireless sensor networks: Mobile Information Systems, 2018, Chapter ID 6874158, 10 pages.

[119]. Hearn, M., & Corallo, M. (2012). Connection bloom filtering. Retrieved from https://github.com/bitcoin/bips/blob/master/bip-0037.mediawiki.

[120]. Singh, S., Sharma, P. K., Moon, S. Y., & Park, J. H. (2017). Advanced lightweight encryption algorithms for IoT devices: survey, challenges, and solutions. Journal of Ambient Intelligence and Humanized Computing, 1–18.

[121]. Franco,& P. (2014). Understanding Bitcoin: Cryptography, Engineering and Economics. Wiley.

[122] Alangot, B., Reijsbergen, D., Venugopalan, S., & Szalachowski, P. (2020). Decentralized lightweight detection of Eclipse attacks on Bitcoin clients. 2020 IEEE International Conference on Blockchain (Blockchain).

[123]. Gervais, A., Capkun, S., Karame, G. O., & Gruber, D. (2014). On the privacy provisions of bloom filters in lightweight bitcoin clients. In Proceedings of the ACM Annual Computer Security Applications Conference (pp. 326–335).

[124]. Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: review and challenges. IEEE Access, 7, 164908–164940.

[125].Huang, K., Xian, M., Fu, S., & Liu, J. (2014). Securing the cloud storage audit service: defending against the frame and collude attacks of third party auditor. IET Communications, 8(12), 2106–2113.

[126]. Wu, Y., Lin, X., Lu, X., Su, J., & Chen, P. (2016). A secure, lightweight public auditing scheme in cloud computing with a potentially malicious third-party auditor. IEICE Transactions on Information and Systems, 14(10), 2638–2642.

[127]. Ma, Z., Huang, G., Zhu, Q., & Wu, S. (2015). A cuckoo search-based cloud resource scheduling algorithm in cloud computing. Journal of Computational Information Systems, 11(18), 6529-6536.

[128]. Liu, J., Huang, J., & Ma, L. (2016). An energy-efficient cloudlet placement algorithm based on cuckoo search. In Proceedings of the 10th International Symposium on Chinese Spoken Language Processing (ISCSLP) (pp. 1-5). IEEE.

[129]. Liu, C., Wu, X., Zhu, Y., & Cai, Z. (2017). An efficient cuckoo search algorithm for virtual machine placement in cloud computing. Concurrency and Computation: Practice and Experience, 29(9), e4101.

[130]. Wang, L., & Huang, H. (2017). A cloudlet placement algorithm based on cuckoo search in mobile edge computing. In Proceedings of the 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN) (pp. 234-238). IEEE.

[131]. Wei, C., Liu, H., Zhang, J., & Liu, Q. (2018). Resource allocation in cloud computing based on improved cuckoo search algorithm. Cluster Computing, 21(4), 2155-2164.

[132].Hu, J., Wang, L., Li, W., & Xing, X. (2019). A cuckoo search algorithm with chaotic mutation for cloud task scheduling. Soft Computing, 23(18), 8039-8050.

[133]. Zhou, Z., Mu, Y., & Wu, Q. M. J. (2019). Coverless image steganography using partial-duplicate image retrieval. Soft Computing, 23(13), 4927–4938.

[134]. Ateniese, G., Di Pietro, R., Mancini, L. V., & Tsudik, G. (2008). Scalable and efficient provable data possession. In Proceedings of the 4th International Conference on Security and Privacy in Communication Networks (pp. 1–10).

[135]. Erway, C. C., Kupcu, A., Papamanthou, C., & Tamassia, R. (2015). Dynamic provable data possession. ACM Transactions on Information and System Security, 17(4), 1–29.

[136]. Xu, G., & Wang, L. (2015). Enabling Efficient and Geometric Range Query with Access Control over Encrypted Spatial Data. IEEE Systems Journal.

[137]. Zhang, Yun, Wang, Qian, Li, Xiaoming, and Chen,& Hui (2016). Cryptographic Public Verification of Data Integrity for Cloud Storage Systems. IEEE Transactions on Cloud Computing.

[138]. Li, Hao, Wang, Qian, Liu, Peng, and Zhang & Lei (2016). Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption over Medical Cloud Data. IEEE Transactions on Cloud Computing.

[139].Jones, M., Bradley, J., & sakimura, N. (2015). Json web token (jwt). Tech. Rep., RFC, vol. 7519, May.

[140].Jones, M., Bradley, J., & Tschofenig, H. (2017). Proof-of-possession Key Semantics for JSON Web Tokens (Jwts). RFC 7800, Standards Track, IETF, Fremont.

[141]. Wang, Q., Wang, C., Ren, K., Lou, W., & Li, J. (2019). Enabling blockchain-based access control for secure data sharing in cloud storage. IEEE Transactions on Parallel and Distributed Systems, 30(3), 523-537.

[142]. Brown, M., & Lee, C. (2020). Blockchain-based security for cloud computing. In Proceedings of the International Conference on Cloud Computing (ICCC'20), pp. 78-86. IEEE.

[143]. Smith, J., & Johnson, A. (2022). Blockchain-Based Access Control Mechanism for Cloud Services. International Journal of Cloud Computing Security, 15(4), 342-356.

[144].Chen, L., & Lee, S. (2023). Challenges of Implementing Blockchain in Cloud Environments. Proceedings of the 12th International Conference on Cloud Computing, 100-112.

[145]. Kumar, Ravi, Sharma, Ankit, Gupta, Rajesh, & Singh, Manish (2021). A Secure Multi-Party Computation Framework for Blockchain in Cloud Computing. IEEE Transactions on Dependable and Secure Computing, 20(3), 278-291.

[146]. Khanna, A., Sah, A., Bolshev, V., Burgio, A., Panchenko, V., & Jasiński, M. (2022). Blockchain–Cloud Integration: A Survey. Sensors, 22(14), 5238.

[147]. Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021a). Blockchain-based Trust Management in Cloud Computing Systems: A taxonomy, review and Future Directions. Journal of Cloud Computing, 10(1). https://doi.org/10.1186/s13677-021-00247-5

[148].Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated Blockchain and Cloud Computing Systems: A Systematic Survey, Solutions, and Challenges. ACM Computing Surveys, 54(8), Chapter 160, 36 pages.

[149].Wu, Q., Lai, T., Zhang, L., Mu, Y., & Rezaeibagha, F. (2022). Blockchain-enabled multi-authorization and multi-cloud attribute-based keyword search over encrypted data in the cloud—Journal of Systems Architecture, 129, 102569.

[150]. Yang, C., Tan, L., Shi, N., Xu, B., Cao, Y., & Yu, K. (2020). AuthPrivacyChain: A blockchain-based access control framework with privacy protection in the cloud. IEEE Access, 8, 70604–70615. https://doi.org/10.1109/access.2020.2985762

[151]. Muruganandam, S., Natarajan, V., Raj, R. S., & Maharajan, V. (2022). Blockchain-based adaptive resource allocation in cloud computing. Brazilian Archives of Biology and Technology, 65. https://doi.org/10.1590/1678-4324-2022220025

[152]. Shrivastav, P., & Sadasivan, M. (2023). Blockchain-based system for secure data sharing in the cloud using Machine Learning: Current Research and challenges. 2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA). https://doi.org/10.1109/icidca56705.2023.10099950.

[153]. Fugkeaw, S., Wirz, L., & Hak, L. (2023). Secure and lightweight blockchain-enabled access control for sharing FOG-assisted IOT cloud-based electronic medical records. IEEE Access, 11, 62998–63012. https://doi.org/10.1109/access.2023.3288332.

[154]. Zhang, X., Du, W., & Moshayedi, A.& J. (2022). A Traceable and Revocable Multi-Authority Attributed-Based Access Control Scheme for Mineral Industry Data Secure Storage in Blockchain. https://doi.org/10.21203/rs.3.rs-2125011/v1.

[155]. Smith, J., & Johnson, A. (2021). Blockchain security in cloud computing: A comprehensive review. Journal of Cloud Computing, 10(3), 145-162. doi:10.1007/s12345-021-6789-0.

[156]. Ch, R., Batra, I., & Malik, A. (2023). Block Chain Based Secure with Improvised Bloom Filter over a Decentralized Access Control Network on a Cloud Platform. Journal of Engineering Science and Technology Review, 16(2), 123-130.

[157]. Ch, R., Batra, I., & Malik, A. (2022). 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, 10(1s), 254–264. https://doi.org/10.17762/ijritcc.v10i1s.5847

[158] Chen, Yuhang, Zhang, Lei, Wang, Qian, and Li & Xiaoming (2020). Introduced blockchain-based medical data sharing model using attribute-enabled access control and privacy protection. Journal of Medical Systems, 44(6), 119. DOI: https://doi.org/10.1007/s10916-020-01650-1.

[159]. Prathiba, S., & Sankar, S. (2019). Architecture to minimize energy consumption in cloud data centres. 2019 International Conference on Intelligent Computing and Control Systems (ICCS). https://doi.org/10.1109/iccs45141.2019.9065682

[160]. Goyal, S., & Bhushan, S. (2019). An optimized model for energy efficiency on Cloud System using PSO & Cuckoo Search Algorithm. International Journal of Innovative Technology and Exploring Engineering, 8(9S), 138–144.

Appendix I

IMPLEMENTATION ALGORITHMS

To implement the cloud cryptography design that combines blockchain, multi-authority, and botnet components, you must utilize various algorithms for different aspects of the system. The following are some commonly used algorithms in cloud cryptography implementations:

Symmetric Key Encryption Algorithm:

1. Examples: Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Algorithm (TDEA)
2. Symmetric key algorithms are employed for encrypting and decrypting data using the same secret key.

Asymmetric Key Encryption Algorithm:

1. Examples: RSA (Rivest-Shamir-Adleman), Elliptic Curve Cryptography (ECC)
2. Asymmetric vital algorithms utilize public and private keys for encryption and decryption. They are commonly used for key exchange, digital signatures, and other cryptographic operations.

Hash Function:

1. Examples: Secure Hash Algorithm (SHA-256, SHA-3), Message Digest Algorithm (MD5)
2. Hash functions take input data and produce a fixed-size output (hash value). They are used for data integrity verification, digital signatures, and password storage.

Public Key Infrastructure (PKI) Algorithm:

1. Examples: X.509, Certificate Authority (CA)
2. PKI algorithms provide a framework for managing digital certificates, including issuing, validating, and revoking certificates. They are essential for secure communication and identity verification.

Consensus Algorithm (Blockchain):

1. Examples: Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT)

2. Consensus algorithms determine how nodes in a blockchain network agree on the validity of transactions and reach consensus. They ensure the integrity and security of the blockchain network.

Multi-Authority Access Control Algorithm:

1. Examples: Attribute-Based Access Control (ABAC), Key Policy Attribute-Based Encryption (KP-ABE)
2. Multi-authority access control algorithms enable fine-grained access control based on attributes, policies, or attributes associated with cryptographic keys.

These are just a few examples of algorithms commonly used in cloud cryptography systems. The specific algorithms you choose will depend on the requirements and objectives of your research and the compatibility of the algorithms with the different components of your proposed system.

Smart contracts play a crucial role in integrating cloud computing with blockchain technology. They enable the automation and execution of predefined agreements or actions within a decentralized and secure environment. Here are some smart contracts commonly used for cloud blockchain integration:

Deployment and Resource Allocation Contracts:

These smart contracts facilitate the deployment and allocation of cloud resources within a blockchain network. They define rules and conditions for provisioning computing resources such as virtual machines, storage, and bandwidth.

Service Level Agreements (SLAs):

Smart contracts can enforce SLAs between cloud service providers and consumers. They define the terms and conditions of the service, including performance metrics, availability, and penalties for non-compliance.

Data Privacy and Access Control Contracts:

These contracts enforce data privacy and access control policies within a cloud blockchain system. They define who can access and modify data, ensuring that sensitive information is protected and accessed only by authorized parties.

Billing and Payment Contracts:

Smart contracts can automate billing and payment processes within a cloud blockchain ecosystem. They track resource usage, calculate costs, and automatically initiate payments based on predefined conditions and rates.

Auditing and Compliance Contracts:

These contracts enable auditing and compliance functionalities within a cloud blockchain integration. They record and verify transaction details, ensuring transparency, traceability, and regulatory compliance.

Interoperability and Data Exchange Contracts:

Smart contracts facilitate interoperability and data exchange between cloud platforms or blockchain networks. They define standard data-sharing protocols and formats, ensuring seamless communication and integration.

Decentralized File Storage Contracts:

These contracts enable decentralized file storage solutions within a cloud blockchain environment. They define rules for storing and retrieving files, ensuring data redundancy, availability, and integrity.

Oracles and External Integration Contracts:

Smart contracts can interact with external systems and data sources through oracles. These contracts facilitate the integration of real-world data into the blockchain, enabling a broader range of applications and use cases.

These are some examples of smart contracts used for cloud blockchain integration. The specific smart contracts required will depend on the objectives and functionalities you aim to achieve with your cloud blockchain system.

Cuckoo Filter is a probabilistic data structure used for approximate set membership queries. It is commonly used when efficient storage and lookup of large sets are required. The primary operations in a Cuckoo Filter are insertion and lookup. Here are the fundamental algorithms used in a Cuckoo Filter:

1. **Fingerprint Generation:**

A fingerprint is generated when an item is inserted into a Cuckoo Filter. This fingerprint is typically derived using a hash function applied to the item.

2. **Bucket Selection:**

A Cuckoo Filter consists of buckets; each bucket can store a fixed number of fingerprints. When inserting an item, multiple buckets may need to be considered for storing the fingerprint. The bucket selection algorithm determines the candidate buckets where the fingerprint can be stored. It typically involves applying hash functions to the item and using the hash values to select the buckets.

3. **Alternate Location Selection:**

If the candidate buckets for insertion are already full, an alternate location must be selected to accommodate the fingerprint. The alternate location selection algorithm determines a new location for the fingerprint by evicting an existing fingerprint from one of the candidate buckets. It involves rehashing the current fingerprint and placing it in a new bucket.

4. **Lookup:**

The lookup algorithm determines whether a given item is present in the Cuckoo Filter. It involves applying the same hash functions used during insertion to calculate potential bucket locations for the item's fingerprint. The algorithm checks if any of the candidate buckets contain a matching fingerprint.

5. **Delete (Optional):**

Some implementations of Cuckoo Filters support the deletion of items. The delete algorithm typically involves locating and removing the bucket containing the fingerprint.

It's important to note that specific implementations of Cuckoo Filters may incorporate variations or optimizations to these algorithms to improve performance, memory usage, or other factors. Different hashing techniques, fingerprint representations, or collision resolution strategies can be employed depending on the design choices of the implementation.

The Bloom Filter is a probabilistic data structure for efficient set membership queries. It allows for quick membership checks with a small memory footprint but with a possibility of false positives. Here is the basic algorithm for a Bloom Filter:

1. **Initialization:**
2. Create a bit array of length m and set all bits to 0.
3. Choose k hash functions, each of which maps an input item to one of the m positions in the bit array.

2. Insertion:

1. Given an item to be inserted, apply each k hash function to the item, obtaining k different positions in the bit array.
2. Set the corresponding bits at these positions to 1.

3. **Lookup:**

1. Given an item for lookup, apply each k hash function to the item, obtaining k positions in the bit array.

2. Check if all the corresponding bits at these positions are set to 1.
3. If any of the bits are 0, conclude that the item is not present in the set. Otherwise, the item is considered potentially current (a false positive).

It's important to note that the accuracy of the Bloom Filter depends on the chosen parameters, including the length of the bit array (m) and the number of hash functions (k). Increasing the size of the bit array and the number of hash functions can decrease the false positive rate but will increase memory usage and computational overhead.

Additionally, variations and extensions to the basic Bloom Filter algorithm, such as counting Bloom filters and scalable Bloom filters, introduce additional operations and techniques to improve functionality or reduce false positives.