CLOUD STORAGE SECURITY USING BLOCK CHAIN TECHNOLOGY

BY

JIBRIL AISHAT GABI

HND/23/COM/FT/458

A PROJECT SUBMITTED TO THE DEPARTMENT OF

COMPUTER SCIENCE

INSTITUTE OF INFORMATION AND COMUNICATION

TECHNOLOGY (IICT)

KWARA STATE POLYTECHNIC ILORIN, KWARA STATE.

IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR

THE AWARD OF HIGHER NATIONAL DIPLOMA (HND) IN

COMPUTER SCIENCE

JULY, 2025

CERTIFICATION

This is to certify that this project was carried out by **JIBRIL AISHAT GABI HND/23/COM/FT/458,** as part of the requirements for the award of Higher National Diploma (HND) in Computer Science.

________________________ ____________________

Dr. Mrs. Dada O.M
Date

(Project Supervisor)

________________________ ____________________

Mr. Oyedepo F.S **Date**

(Head of Department)

__________________________ _____________________

External Examiner
Date

DEDICATION

This project is dedicated to the creator of the earth and universe, the Almighty God. It is also dedicated to my parents for their moral and financial support.

ACKNOWLEDGEMENT

All praise due to Almighty God the Lord of the Universe. I praise Him and thank Him for giving me the strength and knowledge to complete my HND programme and also for my continue existence on the earth.

We appreciate the utmost effort of our supervisor, Dr. (Mrs.) Dada**,** whose patience support and encourages have been the driving force behind the success of this research work. She gave useful corrections, constructive criticisms, comments, recommendations, advice and always ensures that an excellent research is done. My sincere gratitude goes to Head of the Department and other members of staff of the Department of Computer Science, Kwara State Polytechnic, Ilorin, for their constant cooperation, constructive criticisms and encouragements throughout the programme.

Special gratitude to our parents who exhibited immeasurable financial, patience, support, prayers and understanding during the periods in we were busy tirelessly in my studies. Special thanks go to all my lovely siblings.

Our sincere appreciation goes to our friends and classmates.

TABLE OF CONTENTS

CHAPTER THREE: RESEARCH METHODOLOGY AND ANALYSIS

References

ABSTRACT

The rapid adoption of cloud storage has revolutionized data management, enabling scalable, accessible, and cost-effective solutions. However, it also introduces critical security challenges, including unauthorized access, data breaches, and trust issues with centralized providers. Blockchain technology, with its decentralized, immutable, and transparent nature, presents a promising approach to enhancing cloud storage security. This project explores the integration of blockchain technology into cloud storage systems to address these security concerns. By leveraging a distributed ledger, blockchain ensures data integrity, confidentiality, and access control. Smart contracts automate permissions and authentication processes, reducing the reliance on centralized authorities and mitigating single points of failure. The proposed framework includes encryption mechanisms for data privacy and a consensus protocol to validate transactions, ensuring only authorized users can access stored data.

CHAPTER ONE

GENERAL INTRODUCTION

1.1 Background of the study

Nowadays, the problem faced by various organizations is storing an enormous amount of data. To address this issue, organizations have adopted cloud storage as an option to store data. Due to this in the last few years, cloud-based services have increased. These services facilitate remote storage of user data on the cloud as well as properties like sharing and transferring of data. Organizations need not maintain in-house storage because services are available irrespective of time and location across multiple platforms. Despite the mentioned benefits, there are various problems associated with cloud storage. They are maintaining the confidentiality and integrity of data (Aishwarya et.al, 2020).

Blockchain is a technology that has a record of the distributed database or public ledger of all those different proceedings that are implemented and all the contributions sharing it. The transaction that occurred is authenticated by most of the participants by agreeing. When the information is entered into the system, it cannot be undone (Fran, 2018).

Data stored on the cloud may contain sensitive information. However, copyright issues come into the picture. As we are uploading data on the external environment, anyone other than the owner can access the data. Security is the most crucial parameter that should be taken into consideration while storing data on the cloud. But, loud service providers don't ensure a high level of security. Currently, there are very few options available to guarantee the security of data on cloud servers (Aishwarya et.al, 2020).

Advancements in communication and computing technologies, inexpensive data rates, and increased usage of portable devices have led to an escalation in online data storage over the Internet. According to the latest study, Walmart handles transactions of more than 1 million clients every hour, estimated to be more than 2.5 petabytes of information—the equivalent of 167 times the books in America's Congress Library (Pro, 2023).

Stored data plays an essential role in future plans, advertisements, service illustrations, etc. Cloud computing is the technology that is used to remotely store your data on a pay-as-you-use basis without worrying about managing the hardware or other resources. However, due to the lack of direct owner’s control over the data, privacy, and security have become the primary concerns in adopting Cloud computing.

Cloud computing provides services on user’s demand mostly on a rental basis, without worrying about managing the resources. It provides many potential services like one demand services, huge data storage, etc. Due to this scenario, many technologies are invented to handle this mass storage access over the network. Along with huge data storage, concerns such as security, availability, reliability, failure recovery, and on-demand access are also important nowadays. Cloud computing offers huge virtual data storage with solutions to these concerns. As the data owner stores data on Cloud storage which is a non-trusted third party, issues arise such as privacy and security due to loss of direct control over the data (Nakamoto, 2019).

Blockchain technology permits distributed public ledgers that hold immutable information through a secure and encrypted method and makes sure that transactions/data stored on it will never be altered. It is the technology that allows all users to keep a replica of the common ledger containing all transactional data and update it to maintain consistency among them. Unlike Cloud, there is no central authority in Blockchain as it offers distributed and decentralized environment. In absence of a trusted third party, the transactions in a block are validated through a group of selected nodes (sometimes also known as miners) which makes it error-proof (Nakamoto, 2019).

Cloud computing is the recent arising technology of IT industry to solve the problems and difficulties of business database services such as storage capacity, performance, stability, security, load and many other issues. Cloud storage was used to provide the cloud-based data storage platform. The computing tasks are distributed to a large number of computer systems, so that all applications can access the calculation capability, storage space and software services (Kranti et.al, 2022)..

Blockchain plays a key part in the decentralized peer-to-peer system that is driving the rapid development of information technology in security. Blockchain technologies like the hashing algorithm, public/private key encryption, and transaction ledgers make this possible. Every piece of data is kept in a different decentralized place. If hackers attempt to access it, they first obtain encrypted data and then only a portion of the file, not the entire thing. This protects documents stored in cloud storage powered by blockchain. Blockchain is having a good effect and making it easier, faster, and more reliable to use storage, transactions, and business operations. The way forward is to combine blockchain and cloud to benefit from increased security and decentralization, which improves authorization, privacy, and efficiency (Kranti et.al, 2022).

Data is becoming an increasingly important asset as we navigate the digital era. Due to the ubiquitous nature of the internet, data is stored and shared via cloud services, which have become the primary medium for exchanging and storing information. This evolution, however, has resulted in an increasing concern over data security and privacy. Security measures currently employed by cloud service providers are vulnerable to data breaches, piracy, and cyberattacks caused by various security issues. Moreover, Traditional security solutions, which rely on centralization, are no longer sufficient to protect against cyber-attacks and breaches (Taylor et.al, 2019)

1.2 Statement of the Problem

The increasing reliance on cloud storage has raised significant concerns about data security, privacy, and trust. Centralized storage systems are vulnerable to data breaches, unauthorized access, and a lack of transparency in data management. They also face risks of single points of failure and challenges in ensuring data integrity. These issues highlight the need for innovative solutions to enhance cloud storage security, such as leveraging blockchain technology to provide decentralized, transparent, and tamper-resistant data storage systems.

1.3 Aim and Objectives of the Study

The aim of this research is to enhance the security, transparency, and reliability of cloud storage systems by leveraging blockchain technology. The objectives are to:

i. Investigate the vulnerabilities and limitations of existing centralized cloud storage systems in ensuring data security and integrity.

ii. Design a blockchain-based framework for decentralized, tamper-proof, and transparent cloud storage.

iii. Implement smart contracts for automated and secure data access control and management.

iv. Evaluate the performance, scalability, and security of the proposed blockchain-based cloud storage solution.

1.4 Significance of the Study

This study is significant as it addresses critical security challenges in cloud storage by leveraging blockchain technology to enhance data protection, transparency, and trust. It aims to eliminate vulnerabilities such as unauthorized access, data tampering, and single points of failure, contributing to the advancement of secure and reliable cloud storage solutions.

1.5 **Scope of the Study**

The study focuses on utilizing blockchain technology to improve cloud storage security, specifically addressing issues of data integrity, transparency, and access control. It evaluates the performance and scalability of a proposed blockchain-based framework, with an emphasis on its application in modern cloud environments.

1.6 ORGANIZATION OF THE REPORT

This is the overall organizational structure of the work as presented in this project. Chapter one of this project deals with the general introduction to the work in the project. It also entails the aim and objectives of the project, significance of the study, the scope and organization of the project. Chapter focuses on literature review and discussion of related aspect of the project topic. Chapter three covers the methodology, the analysis of the existing system, description of the current procedure, problems of existing system (procedure) itemized, description of the proposed system and the basic advantages of the proposed online water billing system. Chapter four entails design, implementation and documentation of the system. The design involves the system design, output design form, input design form, database structure and the procedure of the system. The implementation involves the implementation techniques used in details, choice of programming language used and the hardware and software support. The documentation of the system involves the operation of the system and the maintenance of the system. Chapter five centres on summary, conclusion and recommendation.

CHAPTER TWO

LITERATURE REVIEW

2.1 REVIEW OF RELATED WORKS

To overcome the problem of multiperson sharing of encrypted data, an attribute-based encryption system (ABE) (Sahai, 2017) was proposed as a one-to-many encryption mechanism. More specifically, ciphertext-policy attribute-based encryption (CP-ABE) (Bethencou, 2021) allows the data owner to refine the user authority of the data visitor to the attribute level by setting a policy. In other words, CP-ABE can achieve effective fine-grained access control under the condition of ensuring data security. However, the traditional CP-ABE Schemes (Li et.al, 2018) usually publish the access policy in the form of plaintext. Anyone who obtains the ciphertext (including cloud servers) can infer part of the secret information included in the ciphertext, endangering the user's identity privacy. In addition, sensitive data must also be protected as private data in specific fields. To address the above issues, Kapadia and other authors made the following proposals.

Kapadia (2023) proposed a policy-hiding CP-ABE scheme. However, an online semitrusted server was introduced in Kapadia (2023) to re-encrypt the ciphertext for each user, thus making the server a bottleneck in the entire system. Nishide (2018) developed two CPABE schemes to hide the policy, which express the access control policy through AND logic with wildcards. Based on the decisional assumption of subgroups, J. Lai, et.(2011) at suggested an adaptively secure policy hiding the CP-ABE technique over a bilinear group of combinatorial orders. Although the scheme in Improves security, the computational cost grows with the increase of the attributes. Hur (2018) constructed a scheme that supports arbitrary expressions with monotonicity and blinds the access policy within the ciphertext. However, this scheme is proven to be secure using the generic group model, which is normally considered heuristically rather than provably secure. Afterwards, Helil Rahman.

According to Eniola (2024) she stated that cloud storage is a popular model of the application in various fields, and the security of storage data and access permission have been widely considered. Attribute-based encryption (ABE) provides fine-grained user access control and ensures data confidentiality. However, current ABE access control schemes rely on trusted cloud servers and provide a low level of security. To solve these problems of traditional encryption schemes, we propose a blockchain-based and ABE cloud storage data access control scheme. In this article, blockchain and smart contract technology are the core elements to ensure data integrity and build a decentralized verification method for outsourcing results.

Aishwarya et.al (2020) opined that; in today's world, the simplest way to share data is through the internet. Cloud computing is a technology provided by the internet, which is dependent on large storage providers. These storage providers act as untrusted third parties who manage enormous data stored on the cloud. This data may contain sensitive information that belongs to multiple individuals or organizations. Such types of models may involve security issues like privacy and integrity. In this paper, we introduce a prototype of a multi-user system for access control to documents that use the blockchain technology for securing shared data storage. The data owner is allowed to upload the documents on the cloud using Web Portal and the user will request an access link of the document from the owner. Whenever the user tries to access the document using the provided link, a smart contract will be triggered which will send a notification to the owner. The owner will receive the notification to grant permission to the user. The user who has the permission to access a particular document stored on the cloud can only access it. The above operation on the document will be recorded on the blockchain.

Owner can always see the logs to find any suspicious operation on the documents. Therefore, the privacy of data is ensured using the smart contracts, immutability property and ledger of blockchain (Aishwarya et.al, 2020).

Parin and Patel (2023) suggest that; storage requirements are increasing rapidly with fast-growing Cloud computing technology. The more data storage and transaction processing requirements, the more chances of malicious activities. Storage security is a vital concern nowadays. To deal with this problem, in this research, we propose a system that provides an efficient security mechanism for data storage on the Cloud with enhanced access control policies by using Blockchain technology, which is immutable in nature. The usage of smart contracts improves transparency and creates a trust model that eliminates the requirement of a trusted third party. The system manages the log trails of all transactions and accomplishes all access policies. The proposed model is transparent, traceable, and secure. Data owners hold all rights to their data and any activity pertaining to accessing the data illegitimately shall not be accepted by the network and shall be notified to all the concerns. We demonstrate our proposed mechanism with details about all concerned stakeholders. The Attribute-Based Encryption (ABE) scheme is used with multiple authorities to manage the user attributes that avoid the use of the central authority. The smart contract avoids the computational burden on the user side and reduces communication costs. We analyze security and compare the performance of our proposed model (Parin and Patel (2023).

2.2 **Review of General Text**

2.2.1 **The Blockchain Defined**

The blockchain is considered the next big revolutionizing technology after the Internet, as it reinvents our way of working and living. In 2008, a scholar who applied the numerical cryptocurrency known as Bitcoin primary presented the impression of a blockchain. The blockchain is fundamentally an important slice of the process of Bitcoin. Since then there have been many cryptocurrencies with very advanced features, such as Ethereum, which introduces intelligent contracts.

From the exchange of information to money transfer and other belongings that require online transactions, everything involves a reliable intermediacy. This trusted mid-way is accountable and takes all the responsibility in case of any failure and handles all the glitches that are related to security. The need for a central authority between different companies or parties to carry out multiple functions like data transaction and financial processing has been eliminated by blockchain technology via using straight, undisputable and distributed open accounts.

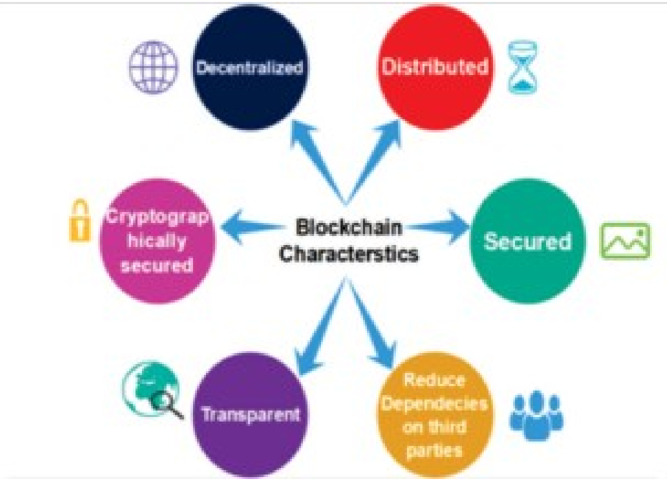

Decentralized
Distributed
Cryptographically secured
Blockchain Characterstics
Secured
Transparent
Reduce Dependecies on third parties

Figure 2.1: Blockchain Characteristics

The network users use the public ledger which is a distributed and shared database. The public ledger is a kind of record that cannot be interfered with and very secured via cryptographic key distribution and it keeps the records of all of the transactions that have been done among the network users. The property that makes blockchain technology permanent, unchallengeable and irretrievable is that users can view the transactions which are related to them any time they want, but there is a process of validation and once the data or transaction is validated and authenticated, then it can't be deleted nor modified and revised.

2.2.2 **Blockchain Secured Cloud Storage Using Chainfs**

This exertion boons ChainFS, a bridge scheme that safeguards cloud storing facilities by means of a slightly reliable Blockchain. ChainFS toughens the cloud storing safety in contradiction of splitting rounds . The chains Bridge delivers the end workers through a file scheme border. Within, ChainFS supplies information records in the cloud and spreads to the blockchain negligible and essential functioning for key delivery and cataloging of file operations. We organize and carefully assimilate the ChainFS scheme on Ethereum and S3FS with FUSE patrons and Amazon S3 cloud storing. We amount the presentation of the scheme and display little overhead.

2.2.3 **Security Analysis With Chainfs**

ChainFS influences the Blockchain to add forking-attack pliability to an encoded file scheme on the cloud. For equal open key almanac and file scheme processes, it upholds a lined record of application-dependent entrances and charts the record to Blockchain. Forcing attacks in the open almanac means that the cloud has dissimilar key terms (of the same person) for dissimilar customers. For the customer to receive the requisite, recall that it forms the presence of the compulsory in the almanac snap with abridgment as a checked log entrance in the blockchain. Two record entrances must be checked in the blockchain at the similar time to let two patrons to receive two cleft bands.

2.3 Blockchain-Based Access Control Scheme for Cloud Storage

In this approach, a multiple worker system prototypes for controlling access is used for data sets to be stored in a cloud atmosphere that is not trusted. Just like any untrusted environment, cloud storage requires the ability to secure information sharing. This approach allows access to data/information which is stored in the secured cloud without the participation of the provider. The main tool which is used to access the control mechanism is a text-policy encryption scheme based on static attributes with dynamic attributes. The proposed scheme delivers an immutable record of all meaningful data security events, such as key generation, access policy assignment, access request, change or revocation, using a blockchain-based decentralized ledger. We suggest a set of cryptographic procedures to ensure the privacy of secret or private key cryptographic operations. Only hash code ciphertexts are transmitted via the blockchain ledger. Our system's prototype is implemented with intelligent contracts and tested on the Ethereum blockchain platform . The aim of the problem-solving approach is to develop an access control model based on blockchain transactions, data storage in untrusted storage and the implementation of Ethereum smart contracts based on attributebased encryption. We use a model of access control based on attributes. XACML is the most commonly used standard for access control based on attributes. This standard describes the components, purpose, interaction and use of the access control system. The system is expected to apply to various types of data, such as multimedia information, electronic documents, etc. It is not advisable to store this amount of data directly in the blockchain, as increasing the number and the size of the blocks increases the complexity of Ethereum, which mainly affects the cost of transactions. Therefore, data is stored in cloud storage in which the file identifying information is only available.

The Ethereum platform is designed to create a blockchain-based decentralized service. It's a single virtual machine distributed. Smart contracts Unlike Bitcoin, Ethereum supports cycles that, on the one hand, have led to the introduction of fees for their implementation, called gas, and have significantly expanded their applications on the other. Changing the virtual machine status can be written in the full script language of Turing. For each file, the user creates a smart contract that stores owner information, access policy, hash sum of the stored information, cloud identifying information, and any changes to the file. Since the information stored in the blockchain is public, information must be encrypted before it is sent to storage and access controlled.

2.4 Blockchain Cloud and Related Susceptibilities

Amongst all the safety matters that occur in the cloud atmosphere, blockchain will be very operative in addressing the tasks and challenges intricate in the application of certain data attribution. We extant the tests related to certain data attribution in the cloud and blockchain competences to report them.

2.4.1 Blockchain and Cloud Security

Cloud computing permits users to distantly stock their data into the cloud and delivers on-demand requests and facilities from a shared loch of configurable calculating properties. The sanctuary of the subcontracted data in the cloud is reliant on the safety of the cloud computing scheme and net. Though, cloud's key features, on-demand facilities, continuous ne twork contact, reserve assembling, and fast resistance are vulnerable to vulnerabilities. In adding, the cloud computing's central tools for virtualization, cryptography, and net amenities have susceptibilities, that The problem relies on the cloud substructure is that if some unauthorized entity tries to interfere and change the data, it cannot be detected. It happens because of the PKI based nature of the cloud. Therefore, a very strong attribution structure is required so that this problem can be eliminated and the responsible entity can be detected. Data authority is a thing that delivers information about all the changes and variations accomplished through data exchange between different units. Scholars have projected safety keys, such as PKI signatures, to guarantee the provenance. Whereas the application of PKI signatures normally rests on a central authority, that is not operative in the cloud substructure . Blockchain claims that it does not require a central system or central authority because its execution is different from the rest of the technologies. There are some ledgers which are distributed, that ledges hold and record all of the transactions and actions that have been done on data. After maintaining the record it shares that with all of the other users who are the participating units. Blockchain provides complete and safe transmission of information via a system of some cryptographically secure keys in a distributed environment. Hence, blockchain and keyless signatures can be the replacement of PKI signatures. The transactions in the public ledger are verified by a consensus of the majority of participating entities.are consequences of uncertain application. At a similar time, security checks, such as key organizations, in the cloud computing environment have numerous trials. For example, to the appliance, an operative key management scheme in cloud computing substructure needs administration and storing of many types of keys. The trouble in conveying standard key organization twigs from the point that simulated technologies typically have varied and heterogeneous hardware/software, and the cloud-dependent computing and storing are purely distributed.

2.5 Blockchain Technology

Blockchain technology is a distributed ledger technology that allows participants to store and verify data in a secure, transparent, and immutable manner without the need for a central authority. It is a decentralized database that consists of blocks of information that are cryptographically linked to each other to form a chain. The information is stored in a decentralized manner across a network of computers, making it difficult to tamper with or modify the data without the consensus of the network. The key characteristics of blockchain technology are: Decentralization: There is no central authority controlling the blockchain network. The data is stored and verified by a network of participants, making it more secure and resistant to tampering. Transparency: All the transactions on the blockchain network are visible to all participants, ensuring transparency and accountability.

2.5.1 . Blockchain Types:

There are mainly three types of blockchain networks: Public Blockchain: Anyone can participate and access the network. Examples include Bitcoin and Ethereum. Private Blockchain: Access to the network is restricted to a group of participants who are authorized to access the data. Examples include Hyperledger Fabric and Corda. Hybrid Blockchain: It is a combination of public and private blockchain networks. It allows certain participants to access the network and maintain the privacy of the data.

2.5.2. **Blockchain Security Features:**

The following are the key security features of blockchain technology: Consensus: The blockchain network uses a consensus mechanism to ensure that all the participants agree on the data added to the network. Cryptography: The data on the blockchain network is secured using cryptographic algorithms like hashing and digital signatures. Immutable Ledger: Once the data is added to the blockchain, it cannot be modified or deleted, ensuring the integrity and immutability of the data. Distributed Storage: The data is stored in a decentralized manner across a network of computers, making it difficult to hack or tamper with the data.

2.5.3 **Blockchain Applications in Different Domains:**

Blockchain technology has a wide range of applications in different domains, including: Financial Services: Blockchain is used in the financial industry for secure and transparent transactions, digital identity management, and smart contracts. Supply Chain Management: Blockchain is used to track and trace the movement of goods in the supply chain, ensuring transparency and accountability. Healthcare: Blockchain is used to store and share patient data securely and efficiently, ensuring privacy and security.

2.6 **Cloud Computing**

Cloud computing is a model for delivering on-demand computing resources over the internet. It enables users to access a shared pool of computing resources, including servers, storage, and applications, without the need for on-premise infrastructure. The key characteristics of cloud computing include: On-demand self-service: Users can access computing resources on-demand without the need for human intervention. Broad network access: Cloud computing resources can be accessed over the internet from any device. Resource pooling: Cloud computing resources are shared among multiple users, enabling efficient resource utilization.

2.6.1 **Cloud Computing Models**

There are three main cloud computing models: Infrastructure as a Service (IaaS): IaaS provides users with access to computing infrastructure such as servers, storage, and networking resources. Platform as a Service (PaaS): PaaS provides users with access to a platform that enables them to develop, test, and deploy applications. Software as a Service (SaaS): SaaS provides users with access to software applications over the internet.

2.6.2 **Cloud Computing Security Issues:**

Cloud computing introduces several security issues that need to be addressed, including: Data Security: Cloud computing involves the storage and processing of sensitive data, which makes data security a major concern. Data Privacy: Cloud computing introduces privacy concerns as data is processed and stored in third-party data centers. Cloud Provider Security: Cloud providers may be vulnerable to cyber-attacks, which can result in the compromise of sensitive data. Compliance: Cloud computing may introduce compliance issues, particularly in industries such as healthcare and finance.

2.6.3. **Cloud Computing Applications in Different Domains:**

Cloud computing has numerous applications in different domains, including: E-commerce: Cloud computing can be used to provide scalable and secure e-commerce platforms. Healthcare: Cloud computing can be used to store and process medical records and enable remote patient monitoring. Education: Cloud computing can be used to deliver educational content and provide collaborative learning environments. Finance: Cloud computing can be used to provide secure and scalable financial services, such as online banking and trading platforms.

2.7 Blockchain in Cloud Computing

Blockchain technology can be used in cloud computing to enhance security and privacy by providing a decentralized and transparent ledger that is resistant to tampering. The key characteristics of blockchain in cloud computing include: Decentralization: Blockchain technology enables cloud computing to be decentralized, meaning that data can be stored and processed on a network of nodes rather than in a centralized data center. Transparency: Blockchain technology provides a transparent and immutable ledger that can be used to verify the authenticity and integrity of data stored in the cloud. Security: Blockchain technology uses cryptographic algorithms to secure data stored in the cloud, protecting it from unauthorized access and tampering. Privacy: Blockchain technology can be used to provide privacy-preserving cloud computing, enabling users to keep their data and activities confidential.

2.7.1 Blockchain-based Cloud Computing Architecture:

A blockchain-based cloud computing architecture consists of a decentralized network of nodes that store and process data. Each node in the network has a copy of the blockchain ledger, which contains a record of all transactions that have taken place. When a user requests a computation, the request is broadcasted to the network, and the nodes work together to process the computation. Once the computation is complete, the result is added to the blockchain ledger, ensuring that it is transparent and immutable.

2.7.2 **Advantages and Disadvantages of Using Blockchain in Cloud Computing:**

The advantages of using blockchain in cloud computing include: Decentralization: Blockchain technology enables cloud computing to be decentralized, reducing the risk of data loss or downtime. Security: Blockchain technology provides a secure and tamper-proof ledger that can be used to protect data stored in the cloud. Privacy: Blockchain technology can be used to provide privacy-preserving cloud computing, protecting users' data and activities from prying eyes. The disadvantages of using blockchain in cloud computing include: Scalability: Blockchain technology can be slow and resource-intensive, making it challenging to scale. Complexity: Blockchain technology is complex and requires specialized expertise, making it difficult to implement for many organizations. Cost: Implementing a blockchain-based cloud computing architecture can be expensive, requiring significant investments in hardware, software, and infrastructure.

2.7.3 **Blockchain-based Cloud Computing Applications:**

Blockchain technology can be used in cloud computing to provide secure and privacy-preserving applications, including: Decentralized cloud storage: Blockchain technology can be used to create decentralized cloud storage platforms that are resistant to data loss and tampering. Privacy-preserving cloud computing: Blockchain technology can be used to enable secure and private computation in the cloud, protecting users' data and activities from prying eyes. Decentralized applications (DApps): Blockchain technology can be used to develop DApps that run on a decentralized network of nodes, providing increased security and transparency.

CHAPTER THREE

RESEARCH METHODOLOGY AND ANALYSIS OF THE EXISTING SYSTEM

3.1 RESEARCH METHODOLOGY

In a research methodology using **Proof of Work (PoW)** for cloud computing security, the first step involves identifying the security challenges in traditional cloud storage systems, such as data tampering, unauthorized access, and centralization. A literature review is conducted to examine existing security solutions, focusing on PoW and its proven ability to secure decentralized networks, primarily in the cryptocurrency domain, and its potential for securing cloud environments.

Based on this review, the hypothesis is formulated that PoW can improve data integrity, prevent unauthorized access, and enhance the overall security of cloud storage systems. The hypothesis sets the foundation for testing how PoW, as a consensus mechanism, can be applied to cloud computing.

The design phase follows, where a blockchain-based architecture for cloud storage is created, integrating PoW. The design includes decentralized storage using blockchain, with PoW ensuring only verified and legitimate data can be uploaded or accessed. The PoW mechanism would require users to solve cryptographic puzzles before they can interact with data, making unauthorized access computationally expensive. Smart contracts are incorporated to automate access control and enforce security policies.

In the implementation phase, a prototype of the cloud storage system is built using blockchain platforms like Ethereum or Hyperledger. The system employs PoW for validating user interactions with the cloud, ensuring only authorized actions are permitted. Cryptographic hashing functions are used to protect data and verify the integrity of transactions within the blockchain.

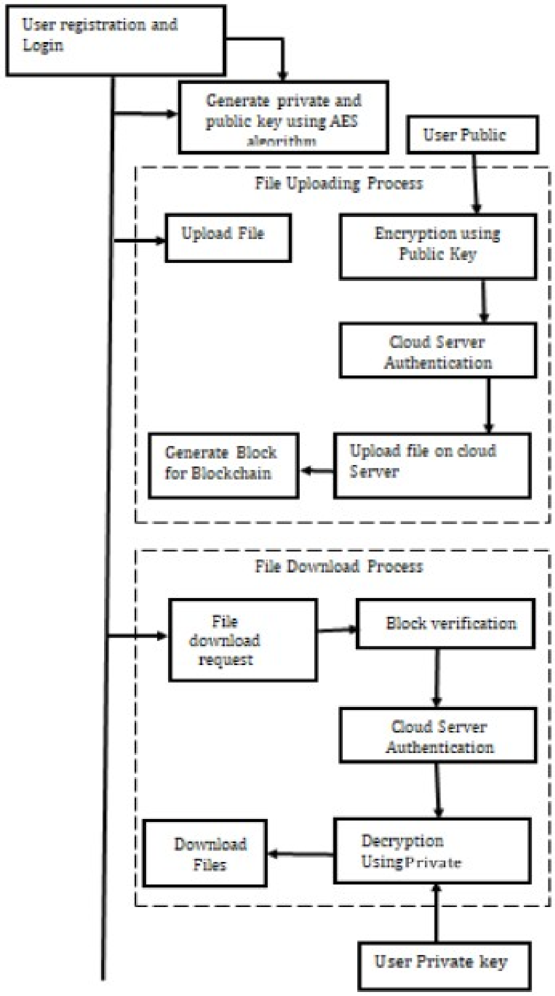
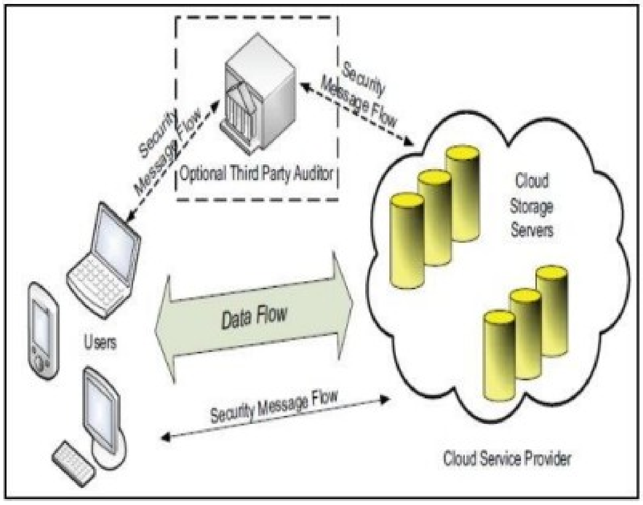

User registration and Login
Generate private and public key using AES algorithm
User Public
File Uploading Process
Upload File
Encryption using Public Key
Cloud Server Authentication
Generate Block for Blockchain
Upload file on cloud Server
File Download Process
File download request
Block verification
Cloud Server Authentication
Download Files
Decryption UsingPrivate
User Private key

Figure 3.1: Blockchain

Once the system is implemented, it undergoes extensive testing to evaluate its effectiveness in enhancing data integrity, preventing unauthorized access, and ensuring system transparency. The performance of the system is measured by how effectively PoW prevents tampering with stored data, how efficiently it manages user requests for accessing or uploading data, and the overall impact on the cloud system's scalability and usability.



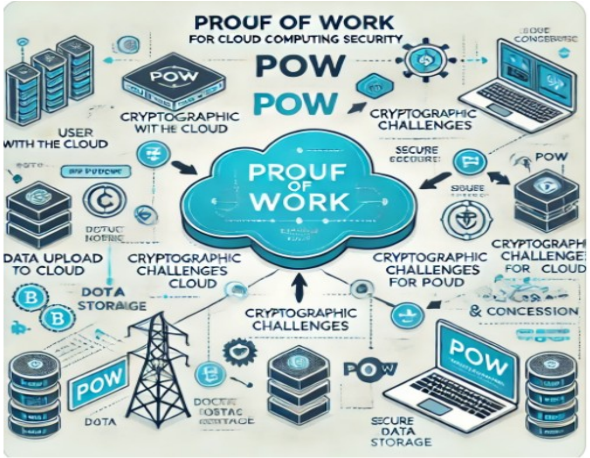


Figure 3.2: Cloud Storage Architecture

Figure 3.3: Proof of Work (PoW) Structure

3.1.1 Blockchain Solution for Cloud Environment

Users' sensitive information due to the monetary leak as well as psychological damages may occur in the environment of cloud computing. Cryptographic ledger is a representative technology for ensuring anonymity. Customer secrecy can be secured if the digital distributed ledger procedure is utilized in the cloud computing environment. Basically once using the blockchain technology e-wallet is installed and if e-wallet is not appropriately removed, the customer data or information may be left which may be utilized to estimate or conclude the customer information.

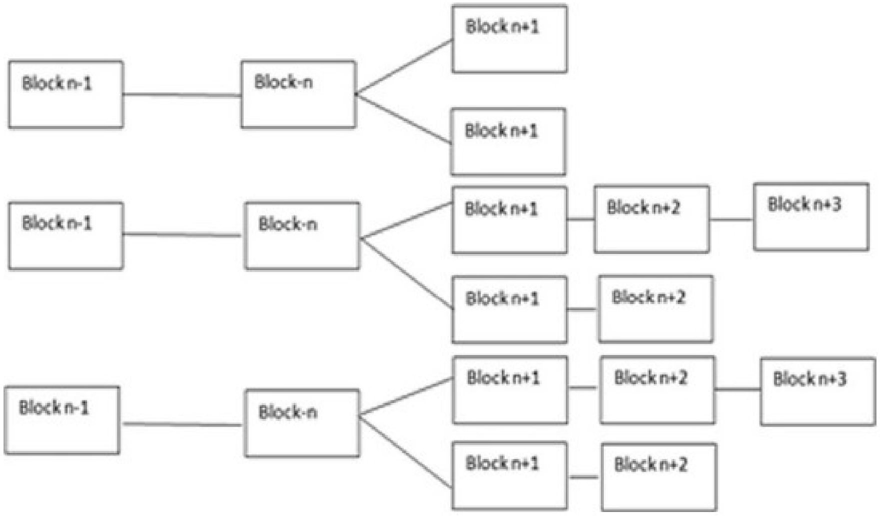


Figure 3.4: Technique for double spending prevention

3.1.2 **Blockchain Security for Cloud Computing**

Blockchain technology offers significant potential for improving the security of cloud computing systems by providing a decentralized and immutable ledger for storing and securing data. Cloud computing systems, which rely on centralized data storage and management, are vulnerable to various security threats, including data breaches, unauthorized access, and service interruptions. Blockchain's features, such as transparency, cryptographic security, and distributed consensus, can address these challenges and provide enhanced protection for cloud environments.

In the context of **cloud computing security**, blockchain can enhance various aspects, including data integrity, authentication, access control, and transparency. By using blockchain to store metadata or even actual data, cloud service providers can ensure that stored information is tamper-proof, transparent, and auditable. Blockchain’s cryptographic techniques (like public/private key encryption and hashing) ensure that only authorized parties can access and modify data.

3.1.3 Algorithm: Proof of Work (PoW) for Blockchain-Based Cloud Computing Security

Input:

- Data to upload or access (data).
- Previous block's proof of work (previous_proof).
- User credentials for access control (user_credentials).

Output:

- Data securely uploaded or retrieved.
- Validation of data integrity and access control.

Step 1: Blockchain Initialization

i. Create an empty blockchain (blockchain).

ii. Add the genesis block:

  - genesis_block = create_block(previous_hash="0", proof=0, data="Genesis Block").
  - Append genesis_block to blockchain.

Step 2: Proof of Work Calculation

iii Define a cryptographic puzzle for PoW:

  - is_valid_proof(proof, previous_proof): Returns True if hash(proof + previous_proof).startswith("0000").

iv Implement PoW algorithm to find a valid proof:

- Start with proof = 0.
- Increment proof until is_valid_proof(proof, previous_proof) returns True.

Step 3: Data Upload

v. Accept the input data for upload.

vi. Retrieve the previous_block and previous_proof from blockchain.

vii. Perform PoW to calculate the new proof.

viii. Generate previous_hash using the hash of previous_block.

ix. Create a new block with create_block(previous_hash, proof, data).

x. Append the new block to blockchain.

Step 4: Data Access

xi. Accept data_request and user_credentials.

xii. Authenticate the user:

1. If authentication fails, return "Access denied".

xiii. Search the blockchain for the requested data:

1. If the data exists, validate its hash and return the data.
2. Otherwise, return "Data not found".

Step 5: Validation and Security

xiv. Ensure all blocks in the blockchain have valid PoW and hash connections:

1. For each block, check is_valid_proof and hash(previous_block) == block.previous_hash.

3.2 ANALYSIS OF THE EXISTING SYSTEM

The existing cloud computing systems provide substantial benefits such as scalability, accessibility, and cost-efficiency. However, they are accompanied by significant security vulnerabilities, primarily due to their reliance on centralized architectures. In these systems, a single entity manages the data and infrastructure, which creates a single point of failure. This design increases the risk of data breaches, system downtime due to hardware or software issues, and malicious activities from insiders within the service provider’s organization.

Data integrity and protection from tampering are persistent challenges in centralized systems. The reliance on conventional checksum-based integrity checks leaves data vulnerable if an attacker gains control of the storage system. Unauthorized access remains a critical issue, often stemming from weak passwords, stolen credentials, insufficient multi-factor authentication mechanisms, and poorly defined access control policies that enable privilege escalation.

3.3 PROBLEMS OF THE EXISTING PROBLEM

The existing cloud computing systems face numerous challenges that hinder their ability to provide robust security, transparency, and reliability. One of the primary issues is their centralized architecture, which makes them prone to single points of failure. This centralization exposes the systems to a higher risk of data breaches, where unauthorized entities can exploit vulnerabilities to access sensitive information. It also increases susceptibility to insider threats, where malicious actors within the service provider's organization can compromise the system.

Another significant problem is lack of data integrity and the potential for tampering. Current systems rely heavily on conventional methods like checksum verification, which are not foolproof against sophisticated attacks. If an attacker gains control over the storage system, they can alter data or bypass these integrity checks, leading to compromised information.

Unauthorized access is a persistent concern in these systems due to weak authentication mechanisms. Poorly implemented access control policies, lack of multi-factor authentication, and dependence on vulnerable credentials like passwords make these systems easy targets for attackers. Privilege escalation attacks further amplify the risk, allowing unauthorized users to gain higher levels of access.

3.4 DESCRIPTION OF THE PROPOSED SYSTEM

The proposed system integrates blockchain technology and the Proof of Work (PoW) mechanism to enhance the security, transparency, and efficiency of cloud computing. Unlike traditional centralized systems, this decentralized approach eliminated the single point of failure, distributing control across multiple nodes in the blockchain network. This ensures that no single entity has complete authority over the data, enhancing the system's resilience against breaches and insider threats.

Data integrity is a central feature of the proposed system. Each transaction or data upload to the cloud is validated using the PoW mechanism, which requires computational effort to solve cryptographic puzzles. Once validated, the data is stored in a block, cryptographically linked to the previous block, forming a secure and immutable chain. This approach prevents unauthorized tampering and ensures that any modification attempts are immediately detectable.

The system also incorporated robust access control mechanisms, leveraging smart contracts to manage permissions and enforced multi-factor authentication. Users are required to authenticate their identity through secure processes before gaining access to stored data. The blockchain provided an immutable audit trail, ensuring transparency and enabling users to trace every interaction with their data. This capability addressed the lack of visibility that plagues traditional systems.

Scalability and secure data sharing are achieved through the distributed nature of the blockchain. Data can be securely shared among users or systems without compromising its integrity, thanks to encryption and consensus protocols. The decentralized architecture also ensures high availability, as the system remains operational even if some nodes fail.

3.5 ADVANTAGES OF THE PROPOSED SYSTEM

The proposed system, which integrated blockchain technology with the Proof of Work (PoW) mechanism, offered several significant advantages over traditional cloud computing systems. The following are the advantages:

i. **Elimination of Single Point of Failure**

Decentralized architecture ensures resilience against attacks, outages, and insider threats. Services remain operational even if some nodes fail.

ii **Enhanced Data Integrity**

Blockchain immutability prevents unauthorized modifications. Cryptographic linking of blocks ensures tamper resistance.

iii **Improved Transparency**

Immutable blockchain records create a verifiable audit trail. Users can monitor all interactions with their data.

iv. Strengthened Access Control

Multi-factor authentication and smart contracts prevent unauthorized access. Automated permissions reduce human error and mismanagement.

v. **Scalability**

Distributed architecture supports large-scale operations efficiently. Enables secure data sharing across multiple users and platforms.

CHAPTER FOUR

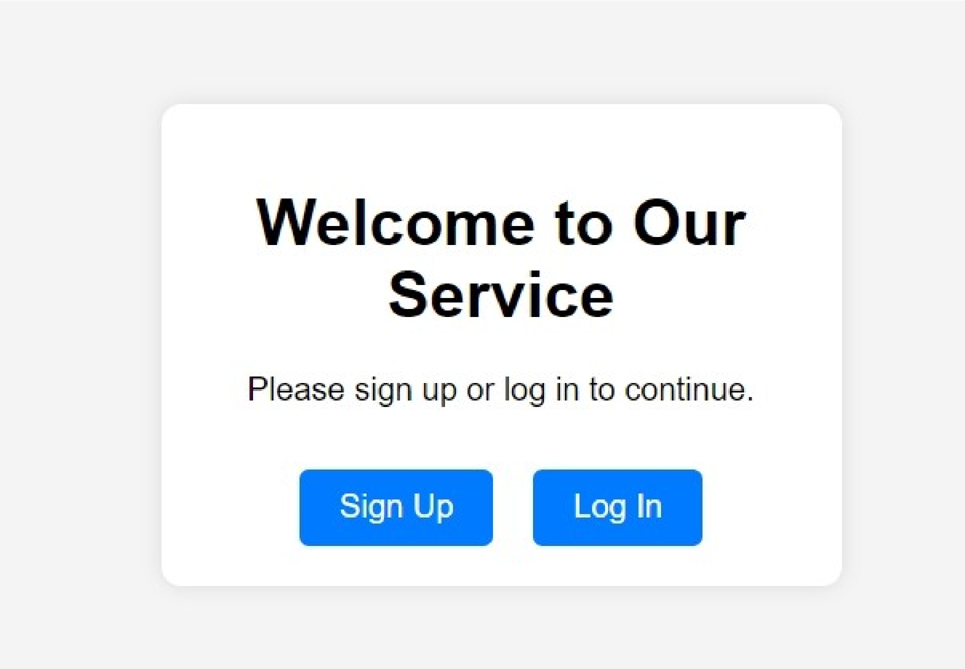
DESIGN, IMPLEMENTATION AND DOCUMENTATION OF THE SYSTEM

4.1 DESIGN OF THE SYSTEM

This is the computation of the particulars of a new system and the determination of what the new system would be and the function it is to perform. This may involve changing from one system to another or modifying the existing system operation. The most challenging phase of the system life cycle is the change from manual operation to a faster and more accurate one; system design stage covers the technical specifications that will be employed in the implementation of the new system in order to modify the previous system. Some factors are put in consideration. These factors include input design, output design, definitions file and procedure designs and other documentation.

4.1.1 OUTPUT DESIGN

This incorporates the objectives of solving the existing system problems and challenges. This involves the structuring of the desired information and also to enhance efficient and effective cloud storage security using blockchain technology. Things taken into consideration in determining the output are represented below:

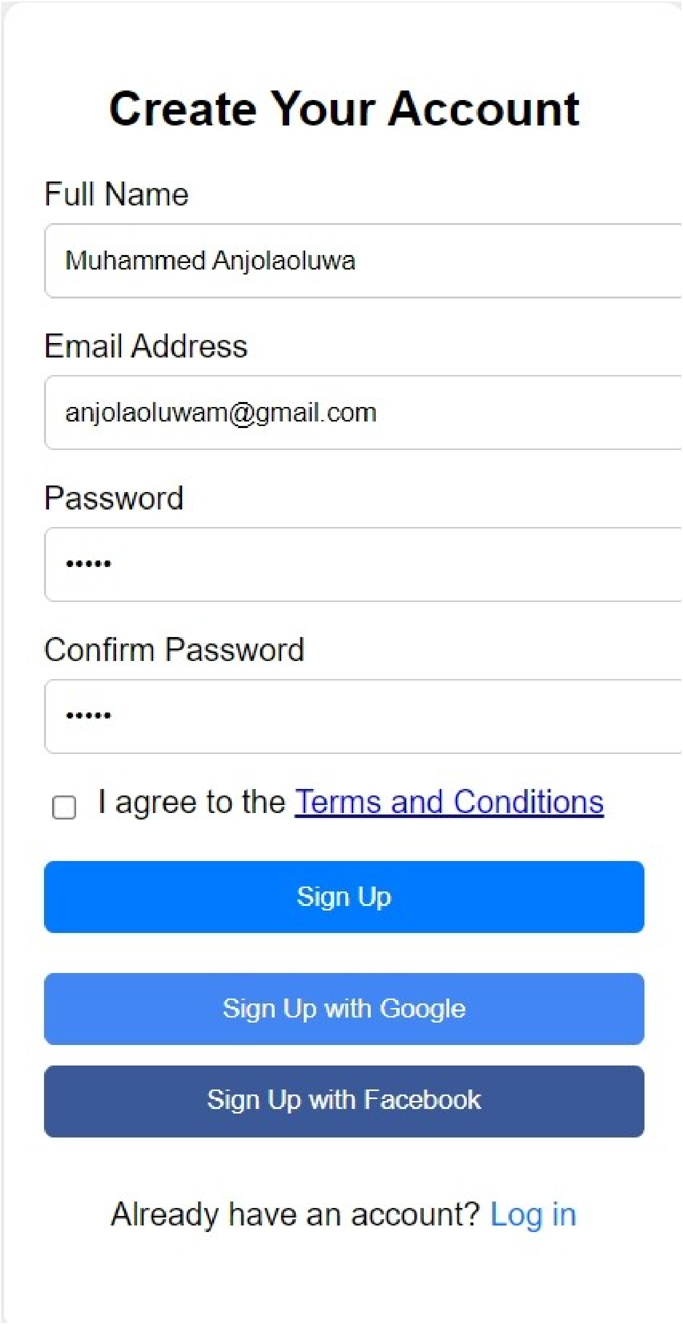


Welcome to Our Service

Please sign up or log in to continue.

Figure 4.1: Index Page

This interface above shows where a user can sign up or login to the system developed.



Create Your Account

Full Name

Muhammed Anjolaoluwa

Email Address

anjolaoluwam@gmail.com

Password

•••••

Confirm Password

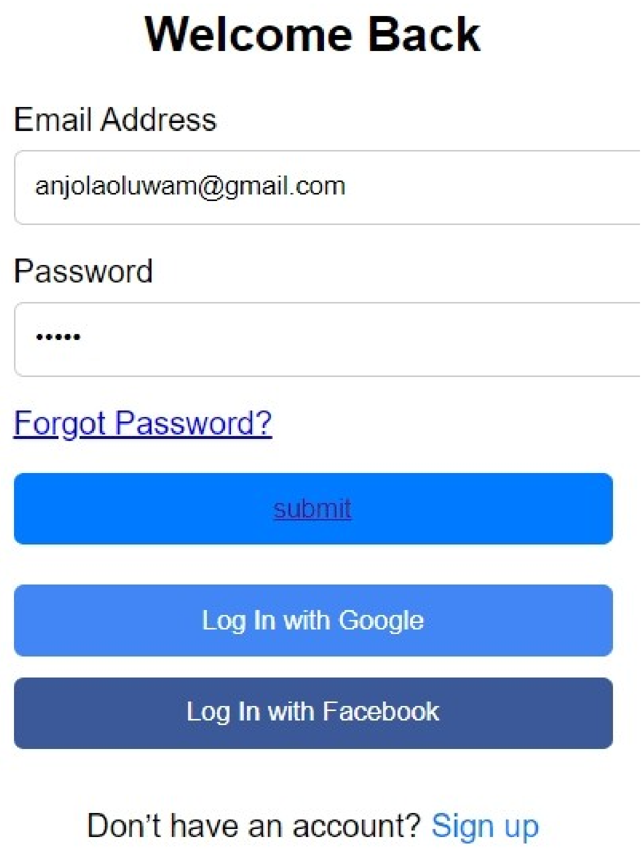
•••••

□ I agree to the Terms and Conditions

Already have an account? Log in

Figure 4.2: Signup Page

This interface allows new user to register their information for them to have access to the system.



Email Address: anjolaoluwam@gmail.com

Password: •••••

Figure 4.3: Login Page.

This interface is where user will enter their email and password to login on the system.

Figure 4.4: Barcode Authentication

This is the page where users will have to scan the barcode in other to have access to the cloud storage environment.

4.1.2 **INPUT DESIGN**

The input to run this software is obtained from the blockchain technology. The administrator is expected to register any user information. He can achieve this by typing via the keyboard. The input required from the Users is their personal data and providing the login details to be used. It can serve as the various input layouts from the various modules first from the collection of data and module then from the assessment module and input from User respectively.

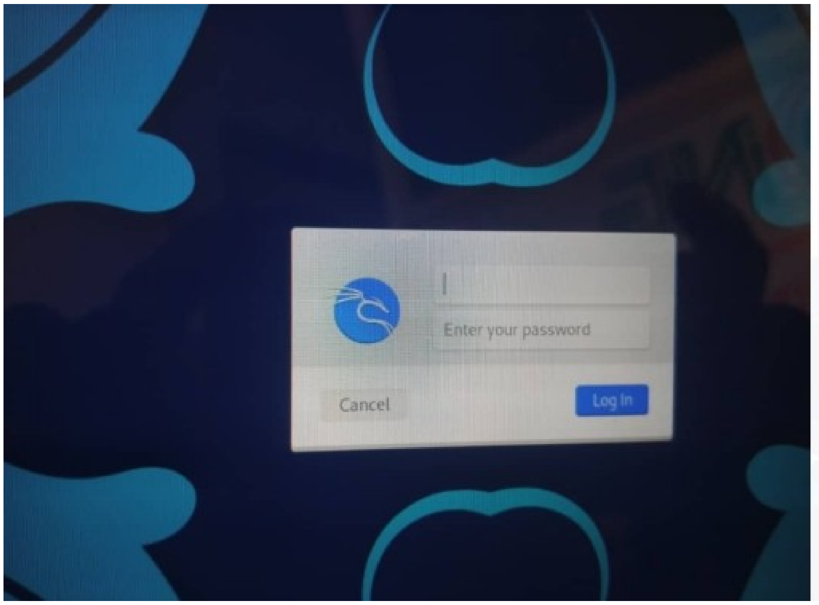
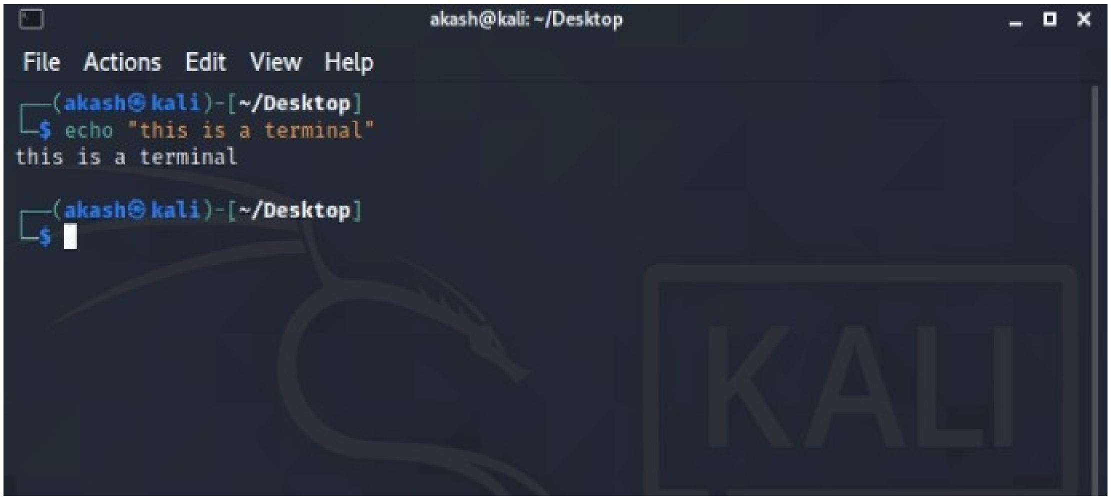


Figure 4.5: Login Interface

This interface allows the user to enter/supply his/her login credentials.



```
┌──(akash㉿kali)-[~/Desktop]
└─$ echo "this is a terminal"
this is a terminal

┌──(akash㉿kali)-[~/Desktop]
└─$ █
```

Figure 4.6: Linux Terminal Interface

This is where user will enter commands for program execution.

4.1.3 PROCEDURE DESIGN

These are the steps involved in unifying the whole process to produce the desired output. It involves computer procedures which start from the original input lessons to the output result file. This allows the processing of user information and result to be possible. Menu is provided to aid user in the processing of the output file.

4.2 IMPLEMENTATION OF THE SYSTEM

This entails the choice of the programming language employed to implement the software which should-be suitable for cloud storage security using blockchain technology. The software is designed for the use of cloud storage security using block chain technology which should serve as an assistant. The cloud storage security admin will prepare data base while the admin will provide personal data about the user.

4.2.1 IMPLEMENTATION OF THE SYSTEM

The Application was developed in a net {dot net} integrated development environment {.net IDE}. The Application IDE is chosen following the fact that extracted information needs to be presented in an enhanced pictorial/graphical format and easy communication with database for program flexibility in linux platform

4.2.2 HARDWARE REQUIREMENT

These are the hardware requirements of the system.

i. 500 Hz minimum with CD ROM drive etc.

ii. Hard disk of capacity 10GB Minimum

iii. 126-512 megabyte of RAM

iv. An Uninterrupted power supply (UPS)

v. A voltage stabilizer

vi. A power generating set and so on.

4.2.3 SOFTWARE REQUIREMENT

i. Linux operating system

ii. Dream Weaver

iii. Linux Command Prompt

iii. Server Query Language (SQL).

4.3 DOCUMENTATION OF THE SYSTEM

4.3.1 PROGRAM DOCUMENTATION

The program is packaged for use in any system that runs on Linux operating system. After the developing of the program in linux, there is a facility provided in Linux that is used in applications packaging and deployment.

4.3.2 MAINTAINING OF THE SYSTEM

The system maintenance refers to making modification to an already existing application/program without necessarily re-writing everything from start. Program maintenance of a program includes modification of the program to meet-up with certain requirements of the Users. In this course, additional features can be added, errors corrected, ambiguous interfaces redesigned to eliminate confusions and unnecessary features removed.

Maintaining this program can be done in a Linux operating system. Any future modification can be by re-running the program source code in a command prompt environment making necessary changes and updates and recompile the application into an upgrade version of the existing version of the mini word processing application. Further versions of this program can be named following their year of release or it can be given a different version number.

CHAPTER FIVE

SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 SUMMARY

The design and implementation of a cloud storage security using blockchain technology offer a transformative approach to addressing the inherent vulnerabilities and limitations of traditional centralized systems. By leveraging blockchain's decentralized architecture, immutability, and transparency, organizations can significantly enhance the security, integrity, and trustworthiness of their cloud infrastructure. This approach not only mitigates risks associated with data breaches and unauthorized access but also fosters greater transparency and accountability, crucial for ensuring data privacy and regulatory compliance. However, successful implementation requires careful consideration of various factors, including consensus mechanisms, data encryption, scalability, interoperability, and regulatory compliance. By addressing these considerations, organizations can build a robust and resilient cloud infrastructure capable of meeting the evolving needs of modern businesses while maintaining the highest standards of security and integrity.

5.2 CONCLUSION

The design and implementation of a cloud storage security using blockchain techniques represent a paradigm shift in cloud computing, offering a decentralized and trust-based approach to security and data management. By decentralizing control and leveraging blockchain's inherent features, organizations can mitigate risks, enhance transparency, and improve the overall security posture of their cloud infrastructure. However, successful implementation requires careful planning, collaboration, and adherence to best practices in blockchain technology and cloud computing. With proper design and implementation, organizations can realize the full potential of blockchain in revolutionizing the way we secure and manage data in the cloud, paving the way for a more secure and trustworthy digital ecosystem.

5.3 RECOMMENDATIONS

Based on the findings of the research, the following are recommended:

i. Thorough Risk Assessment: a comprehensive risk assessment to identify potential security threats and vulnerabilities specific to the cloud environment and blockchain implementation should be conducted.

ii. Collaboration and Knowledge Sharing: Foster collaboration and knowledge sharing among stakeholders, including IT professionals, blockchain experts, and regulatory bodies, to ensure a holistic and informed approach to design and implementation.

iii. Continuous Monitoring and Evaluation: Implement robust monitoring and evaluation mechanisms to continuously assess the effectiveness and performance of the blockchain-based cloud environment and make necessary adjustments as needed.

iv. Adherence to Regulatory Compliance: Ensure compliance with relevant regulatory requirements and standards, such as GDPR for data privacy, to mitigate legal and regulatory risks associated with data management and storage.

References

Aishwarya Patil, and Others (2020) Blockchain based Cloud Data Storage System, International Research Journal of Engineering and Technology (IRJET), Vol. 7.

Project Pro. (2023). How big data analysis helped increase Walmarts Sales turnover? [Online]. Available: https://www.dezyre.com/article/how-big-data-analysis-helpedincrease-walmarts-sales-turnover/109 [2] S. Nakamoto. (2008). Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis,”A systematic literature review of blockchainbased applications:Current status,classification and open issues” , Elsevier, 2018.

Kranti Warke*1, Devika Mahindre*2, Vishakha Patil*3, Vaibhavi Shinde*4, Shrutika Hapse*5, Prof. V.A. Shevade*6 (2022), BLOCK CHAIN BASED SECURE DATA STORAGE ON CLOUD, International Research Journal of Modernization in Engineering Technology and Science.

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.-K.R. (2019). A systematic literature review of blockchain cyber security. Digital Communications and Networks, 6(2). doi:10.1016/j.dcan.2019.01.005

A. Sahai, “Fuzzy identity-based encryption,” in Lecture Notes in Computer Science, B. Waters, Ed., Springer, Berlin, Germany, pp. 457–473, 2005

J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” in Proceedings of the 2007 IEEE Symposium on Security and Privacy, pp. 321–334, Berkeley, CA, USA, May 2007.

Li C., J. He, L. Cheng, C. Guo, and K. Zhou, “Achieving privacy-preserving CP-ABE access control with multi-cloud,” in Proceedings of the 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), pp. 801–808, Melbourne, Australia, December 2018.

Kapadia A., P. P. Tsang, and Smith W. S., “ (2023) Attribute-based Publishing with Hidden Credentials and Hidden Policies,” in Proceedings of the Network And Distributed System Security Symposium, pp. 179–192, NDSS 2007, San Diego, CA, USA,

T. Nishide, K. Yoneyama, and K. Ohta, “Attribute-based Encryption with Partially Hidden Encryptor-Specified Access Structures,” in Proceedings of the International Conference on Applied Cryptography and Network Security, pp. 111–129, Springer, Berlin, Heidelberg, June 2008

Lai, R. H. Deng, and Y. Li, “Fully Secure Cipertext-Policy Hiding CP-ABE,” in Proceedings of the International Conference on Information Security Practice and Experience, pp. 24–39, Springer, Berlin, Heidelberg, May 2011.

] Hur. J, “Attribute-based secure data sharing with hidden policies in smart grid,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 11, pp. 2171–2180, 2018.