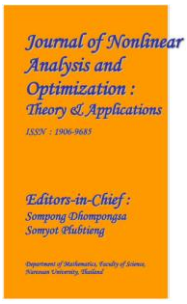
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



Paper ID: ICRTEM24_132 **ICRTEM-2024 Conference Paper**

UTILIZING BLOCKCHAIN TECHNOLOGY WITH CLOUD COMPUTING TO ENHANCE DOCUMENT SECURITY

[#1]RAMAKRISHNA VEMULA, *Research Scholar,*
[#2]Dr. ANOOP SHARMA, *Guide,*
[#3]Dr.KISHOR KUMAR GAJULA, *Co-Guide,*
Department of Computer Science & Engineering,
UNIVERSITY OF TECHNOLOGY, JAIPUR, RAJASTHAN
Corresponding Author: *Ramakrishna Vemula,* vemula.ramakrishna@yahoo.com

ABSTRACT: Blockchain-based cloud computing blends blockchain technology with cloud computing infrastructure to enhance data security and privacy. Cloud computing allows data to be stored, processed, and accessed online, but blockchain technology provides a secure and decentralized approach for data management. Combining blockchain with cloud computing can improve data security, transparency, and reduce the risk of data breaches. Blockchain-based cloud computing provides a distributed and secure platform for storing and managing information. Blockchain maintains data on a decentralized network of nodes, which improves security by making it difficult for unauthorized parties to access or modify the data. Furthermore, blockchain technology can provide an immutable audit record of transactions, making it easier to monitor and authenticate data. Blockchain-based cloud computing provides substantial benefits in terms of data privacy. Blockchain technology provides a decentralized and secure platform for storing and managing data, thereby lowering the risk of data breaches and hacking. Furthermore, blockchain technology can facilitate secure and secret communication among users, hence boosting data privacy. Blockchain technology combined with cloud computing infrastructure has the potential to alter data storage, processing, and access. Blockchain-based cloud computing improves data security, transparency, and privacy by providing a secure and decentralized platform for data management.

Keywords: *Blockchain, Cloud Computing, Centralized, Decentralized.*

I. INTRODUCTION

Blockchain technology is a decentralized mechanism for recording information that eliminates intermediaries such as banks and governments while ensuring transaction security and transparency. Its decentralized, transparent, and secure features have the potential to transform many industries. Cloud computing entails delivering computer services such as servers, storage, databases, networking, software, analytics, and intelligence via the internet. Businesses can quickly modify their capacity in response to changing demand by having flexible and on-demand access to a shared pool of computer resources. Blockchain technology improves the security of cloud documents by

providing an additional layer of protection. It prevents unwanted access, alteration, or deletion by keeping an immutable record of transactions. Blockchain technology mixed with cloud computing improves traceability, accountability, and transparency. Users can analyze transaction history to ensure accountability for all parties involved. The decentralized nature of blockchain technology may improve the dependability of cloud services. A decentralized network of nodes works together to verify and authenticate transactions, eliminating the need for a single authority to manage and secure data. This prevents malicious users from taking advantage of the system. Integrating blockchain technology into cloud computing may result in a more secure and efficient method to data management and storage. It has the potential to reduce the dangers associated with traditional cloud storage while also expanding organizations' data management options.

Background and Context

As cloud computing becomes more widespread for data processing and storage, there are growing concerns regarding the security and privacy of sensitive data. Cloud computing provides benefits such as cost-effectiveness, scalability, and flexibility, but it also introduces security threats such as data breaches, cyber assaults, and unauthorized access. It is critical to have a secure and reliable cloud data processing and storage solution..

Problem Statement

Cloud computing Centralized data storage makes consumers more vulnerable to security threats such as hacking, data breaches, and unauthorized access. The centralized system makes it difficult to monitor data changes, leaving it prone to fraud and corruption. A secure and transparent system is critical for ensuring the security and integrity of data stored in the cloud.

Objectives

The initiative's objectives are the following:

- To research increasing document security by combining blockchain technology and cloud computing.
- To determine the benefits and drawbacks of using blockchain technology to improve document security in cloud computing.
- by developing a cloud computing solution that incorporates blockchain technology for document security.
- Evaluate the document security capabilities of the blockchain-based cloud computing architecture.

Scope and Limitations

This project aims to provide robust document security through the use of cloud computing and blockchain technologies. The project's goal is to create a blockchain-based cloud computing system that focuses on analyzing system performance and document security. The project's research and development of the blockchain-based cloud computing architecture is limited by time and funding constraints.

Methodology

The project will use the following processes in its methodology:

- An exploration of the use of blockchain and cloud computing to enhance document security.
- An analysis of current cloud computing models that use blockchain technology to improve document security.
- Creating a blockchain-based cloud computing system to increase document security.
- Simulation and testing are used to examine the efficiency of a blockchain-based cloud computing infrastructure.
- Comparing the findings to existing document security standards for blockchain-based cloud computing.
- The conclusion includes ideas for future research.
-

II. LITERATURE REVIEW

Integrating blockchain technology with cloud computing can improve data management and storage efficiency, security, and transparency. Blockchain technology's decentralized and secure ledger maintains data integrity, while cloud computing offers benefits such as cost-

effectiveness, scalability, and flexibility for data processing and retrieval. When blockchain technology is used with cloud computing, document management and storage can become more secure and efficient, reducing reliance on centralized institutions.

Blockchain Technology

1. Definition and Characteristics:

Blockchain technology is an independent, decentralized ledger that operates without the need for a central authority. It allows users to validate and preserve data in a visible and unchangeable format. A decentralized database can be created by using encryption to connect data pieces. Decentralized data storage system prohibits unwanted data modifications by demanding network-wide clearance.

The following are the primary properties of blockchain technology:

Decentralization: The blockchain functions independently of a centralized regulatory body. Data that is saved and confirmed by multiple people is less likely to be tampered with, making it more secure.

Transparency: Transparency and accountability are assured because every transaction is visible to all blockchain network participants.

Security: Cryptography ensures data security on the blockchain network, making it very impossible for unauthorized parties to change or tamper with the data.

2. Blockchain Types:

There are three basic categories of blockchain networks:

Public Blockchain: Everyone is invited to participate and use the network. Two examples are Bitcoin and Ethereum.Private Blockchain: Data access is limited to a specific set of authorized users. Two examples are Hyperledger Fabric and Corda.

Hybrid Blockchain: The public and private blockchain networks have been integrated. It allows specified users to use the network while maintaining the confidentiality of their information.

3. Blockchain Security Features:

Here are the main security features of blockchain technology:

Consensus: Consensus is used in blockchain networks to ensure that all members agree on the data they exchange with the network.

Cryptography: Hashing and digital signatures are cryptographic methods for securing data on the blockchain network.

Immutable Ledger: When data is posted to the blockchain, it becomes immutable and tamper-proof, guaranteeing its accuracy permanently..

Distributed Storage: Decentralized data storage on a computer network improves data security by making data alteration and hacking more difficult.

4. Blockchain Applications in Different Domains:

Blockchain technology has proved utility in a variety of industries.

Financial Services: Blockchain technology is used in the financial industry to ensure secure and transparent transactions, digital identity verification, and automated contract execution.

Supply Chain Management: Blockchain tracks the flow of goods across the supply chain, ensuring openness and accountability.Blockchain allows for the rapid and safe transport and storage of patient data while maintaining privacy and security.

Real Estate: Land registries, property ownership information, and real estate smart contracts are all managed using blockchain technology.

Government: The government uses blockchain technology to protect document management, identity management, and voting systems.

Cloud Computing

1. Definition and Characteristics:

Cloud computing is a paradigm in which computer resources are delivered digitally and instantly when requested. It enables consumers to access a shared pool of computer resources, such as servers, storage, and applications, without requiring on-site equipment. Key characteristics of cloud computing include:

On-demand self-service: Users can access computer resources quickly and autonomously, without requiring human intervention.

Broad network access: Cloud computing resources are accessible from any device via the internet..

Resource pooling: Resource pooling optimizes resource use by dividing cloud computing resources across multiple consumers.

Rapid elasticity: Rapid elasticity refers to the seamless adaptation of cloud computing resources to changing client needs.

Measured service: Billing and resource utilization in the cloud are based on actual consumption.

2. Cloud Computing Models

There are three basic cloud computing models:

Infrastructure as a Service (IaaS): Users gain access to computational resources via Infrastructure as a Service (IaaS), which comprises servers, storage, and networking components.

Platform as a Service (PaaS): offers users a platform for developing, testing, and deploying applications.

Software as a Service (SaaS): provides clients with online access to software packages..

3. **Cloud Computing Security Issues:**

security challenges that must be addressed, including:

Data Security: fundamental concern in cloud computing due to the storage and processing of sensitive data.

Data Privacy: creates privacy concerns because data is processed and stored in third-party data centers.

Cloud Provider Security: Cyberattacks can compromise sensitive data, placing cloud providers at risk of being targeted.

Compliance: Compliance issues may arise with cloud computing, particularly in sectors such as finance and healthcare.

4. Cloud Computing Applications in Different Domains:

Cloud computing has a wide range of applications across industries, including:

E-commerce: Cloud computing enables the creation of safe and scalable e-commerce platforms..

Healthcare: Cloud computing allows for the processing and storage of medical records, as well as remote patient monitoring.

Education: Cloud computing can be used to develop collaborative learning environments and distribute instructional content.

Finance: Online banking and trading platforms are just two examples of scalable and secure financial services that can be provided through cloud computing.

III. BLOCKCHAIN IN CLOUD COMPUTING

1. Definition and Characteristics:

Blockchain technology provides a transparent, decentralized ledger that cannot be manipulated and can be used in cloud computing to improve security and privacy.

The following are some of the primary characteristics of blockchain in cloud computing:

Decentralization: Blockchain technology allows data to be processed and stored on a network of nodes rather than in a centralized data center, thereby decentralizing cloud computing.

Security: Blockchain technology allows for the creation of a visible and unchangeable ledger that may be used to certify the authenticity and integrity of cloud-based data.

Privacy: Blockchain technology can be used to provide secure cloud computing, allowing users to keep their information and actions private.

2. Blockchain-based Cloud Computing Architecture:

A decentralized network of nodes processes and stores data in a cloud computing architecture based on blockchain technology. Each node in the network stores a copy of the blockchain ledger, which contains a record of all transactions. A user sends a calculation request via the network, and the nodes collaborate to process it. The result is added to the blockchain ledger as soon as the calculation is completed, ensuring its transparency and immutability.

3. Advantages and Disadvantages of Using Blockchain in Cloud Computing:

Some advantages of implementing blockchain technology in cloud computing are as follows:
Decentralization: Blockchain technology allows for decentralized cloud computing, which reduces the risk of data loss or outages.
Security: Cloud data can be protected via blockchain technology, which provides a secure record that is impenetrable to alteration.
Privacy: Blockchain technology can be used to facilitate cloud computing, which protects user privacy from prying eyes by hiding user data and actions. Some disadvantages of employing blockchain technology in cloud computing are as follows:
Scalability: Scaling blockchain technology is tough due to its high latency and resource needs.
Complexity: Many organizations struggle to implement blockchain technology due to its complexity and particular knowledge needs.
Cost: Implementing a blockchain-based cloud computing architecture might be costly due to the significant investment required in hardware, software, and infrastructure.

4. Blockchain-based Cloud Computing Applications:

Blockchain technology can be used in cloud computing for private and secure purposes, such as:
Decentralized cloud storage: Blockchain technology allows you to create decentralized cloud storage solutions that are resistant to data loss and tampering..
Privacy-preserving cloud computing: Blockchain technology, which enables private and secure cloud computing, can protect user data and activities from prying eyes.
Decentralized applications (DApps): Building decentralized applications (DApps) with blockchain technology can provide increased security and transparency.

IV. PROPOSED WORK

1. Cloud Documents Encryption

To ensure the security of data transmitted via the cloud, utilize the AES (Advanced Encryption Standard) approach with a 256-bit key. AES is a common symmetric encryption method noted for its user-friendliness. The substitution-permutation network is used as an alternative to the Feistel cipher. AES calculates a plaintext segment as either 128 bits or 16 bytes. The binary layout consists of a 4x4 matrix. Before storing the data in the cloud, the server encrypts it with a randomly generated key.

2. Secret Key Management

Our plans include a mechanism for storing incomplete keys. During runtime, the system creates a random alphanumeric secret key, which is subsequently converted into a 32-byte encryption key. The blockchain securely stores the secret alphanumeric key required for encryption and decoding in encrypted form. Hackers cannot decrypt the entire key if a piece of it is encrypted using alphanumeric characters.

3. Keyword Management

The process involves encrypting and extracting data from documents. Keywords are identified in the collected text using several ways. A popular method for keyword extraction consists of three major components:Candidate Selection Process: The keywords for the task are chosen based on their potential effectiveness as words, phrases, sentences, or concepts.
The likelihood of a candidate becoming a keyword is estimated using their properties. A candidate that appears in the title of a book is more likely to be a keyword.
Machine learning techniques or a formula must be used to examine the candidate's characteristics and calculate the likelihood of their selection as a keyword. The amount of keywords utilized in the final keyword collection is limited.Encrypted keywords are used to access documents. The extracted keywords are encrypted again using the Caesar method. The Caesar cipher is a basic substitution encryption algorithm that moves each letter in the plaintext by a predetermined number of alphabetic positions. Unencoded keywords are translated into a readable format with little material.Our technology provides blockchain-powered transaction management for getting documents via key storage. The blockchain stores transaction data that is captured

and saved when a user subscribes to certain content. These transaction data are available for review by authorized users.

V. SYSTEM DESIGN

This architecture comprises a universal cloud server designed specifically for document storage. It enables users and researchers to register and publish their research findings or documents, which can subsequently be shared with others. The framework ensures the secure storage of documents and their associated keywords on the cloud server. End users can find documents by entering a search query. The system will then locate and display the relevant papers on the screen. Users must subscribe to a document by following the administrator's instructions or using a specific transaction method, such as a bitcoin transaction. The blockchain will record and monitor all transactions. Only authorized users will be able to access the transaction records. An architectural diagram is shown below.

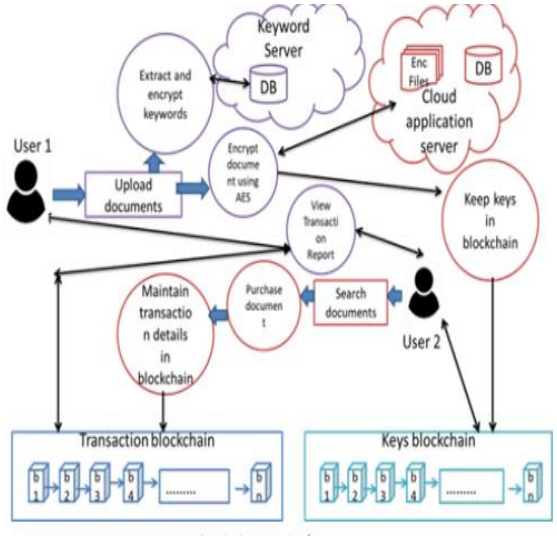


Fig -1: System Architecture

1**. Algorithm and Mathematical Model**

- Cloud servers use the Advanced Encryption Standard (AES) algorithm to encrypt data.
- Directions: Derive the round keys from the ciphertext.
- Revise the state array to include the block data in plaintext.
- Merge the initial state array with the first round key.
- Perform nine state modification iterations.
- Complete the tenth and last round of state manipulation.
- Create the ciphertext by using the final state array.

2. Algorithm for encrypting document keywords: Caesar Algorithm: Steps

- Analyze the entire text, focusing on each character individually.
- Alter each character according to a specified rule, taking into account whether the text is encrypted or decoded.

V. IMPLEMENTATION

We are using an innovative strategy in this project by storing the papers on a cloud server and the keywords on a separate key server to ensure that they are up to date. We distribute keys through blockchain technology. We will track blockchain transactions in addition to keys. This project uses both distributed and centralized storage methods. We advocated using the AES method to encrypt documents. The papers are encrypted using a symmetric key using the AES algorithm.

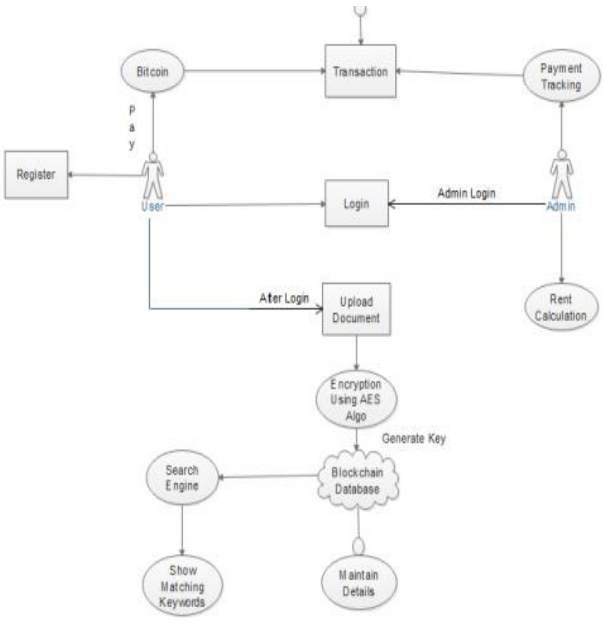


Fig -2: Data Flow

The diagram depicts an information flow chart that includes several processes, actions, users, and other factors. New users can submit papers and photographs, search for documents, purchase documents with bitcoin, register, log in, and perform other operations. The administrator can manage user service fees, payments, compute

rent, and log in. The user sends an encrypted document. Users can disseminate encrypted content for free or with a subscription fee..

VI. RESULT ANALYSIS

Users must register on the site before they can distribute or sell research papers in PDF format. Upon registration, they will receive login credentials via email. Upon logging in, users can select and upload research-related PDFs or files, which are securely saved. Unauthorized users or those who have not paid the subscription price will be unable to view the PDF. Common concerns in the present digital advertising sector include domain fraud, bot traffic, ambiguous payment methods, and a lack of transparency. Blockchain technology can address these concerns by limiting the number of viable firms that can thrive financially.

Fig -3: Document Upload

Fig -4: Service Charges

VII. CONCLUSION

This project uses strong encryption and blockchain key management technology to protect against external threats and cloud service provider document breaches. The solution demonstrates the secure use of blockchain technology for transaction processing and key management. The use of blockchain-based key storage effectively proves the system's security. Those looking for a safe and economical way to store and trade documents will find the recommended solution to be both secure and cost-effective.

REFERENCES

1. Smith, J. (2019). "Blockchain Applications in Cloud Computing." Journal of Cloud Computing, 7(1), 1-10. doi: 019-0130-7 on March 15, 2023.
2. Smith, J. (2022). "Securing Documents in Cloud Computing with Blockchain." Journal of Cloud Security,
3. "A Blockchain-based System for Secure Data Sharing in Cloud Computing Environments" by H. Su, M. Dong, and Y. Zhang. Published in IEEE Access in 2021. DOI: 10.1109/ACCESS.2021.3056381.
4. "Blockchain Technology for Securing Data in Cloud Computing Environments: A Review" by M. Ali, S. Ullah, and S. K. Bhatti. Published in Journal of Cloud Computing in 2020. DOI: 10.1186/s13677-020-00210-y.
5. "A Hybrid Cloud-Blockchain System for Secure Document Sharing and Access Control" by L. Yang and H. Li. Published in Future Internet in 2020. DOI: 10.3390/fi12020034.
6. "Blockchain-enabled Privacy-preserving Data Sharing in Cloud Computing" by Y. Chen, Z. Peng, and S. S. Iyengar. Published in IEEE Transactions on Services Computing in 2019. DOI:10.1109/TSC.2019.2923372.
7. F. Liu, Q. Xie, Z. Huang, J. Cai and H. Ma, "An Improved Blockchain-Based Cloud Storage and Sharing System," in IEEE Access, vol. 9, pp. 5291-5302, 2021, doi: 10.1109/ACCESS.2021.3042168.

8. S. Gaur, S. Kumar, V. Kumar and S. K. Singh, "Secured Data Sharing in Cloud Environment using Blockchain," in 2021 4th International Conference on Communication System, Computing and IT Applications (CSCITA), 2021, pp. 1-5, doi: 10.1109/CSCITA51990.2021.9461016.
9. X. Chen, Y. Liu and J. Zhang, "Blockchain-Based and Decentralized Document Management System with Fine-Grained Access Control in Cloud Computing," in IEEE Transactions on Services Computing, vol. 14, no. 2, pp. 232-245, 2021, doi: 10.1109/TSC.2020.3034126.
10. M. M. Rahman, M. N. Hasan and M. M. Hassan, "A Secure and Efficient Blockchain-Based Document Sharing System in Cloud Environment," in IEEE Access, vol. 8, pp. 192652-192662, 2020, doi: 10.1109/ACCESS.2020.3031638.