International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

COLLABORATIVE MULTICLOUD DATA STORAGE USING BLOCKCHAIN WITH INTEGRITY VERIFICATION

Mr. D. Vijayakumar[1], *G. Aarthi*[2], *S. Abinaya*[3], *B. Priyadharshini*[4]

[1] Assistant Professor, Department of Information Technology, Dhanalakshmi Srinivasan Engineeringcollege (Autonomous), Perambalur, Tamil Nadu.

[2,3,4] UG-Department of Information Technology, Dhanalakshmi Srinivasan Engineering college(Autonomous), Perambalur, Tamil Nadu.

E. Mail: Vijaydsecit@gmail.com[1], aarthi.g1112@gmail.com[2], abia09219@gmail.com[3],dharshinibabu45@gmail.com[4]

ABSTRACT

Traditional centralized cloud storage systems often face vulnerabilities such as single points of failure, data breaches, and unauthorized access. To address these challenges, this study proposes a blockchain- based approach for secure data storage on the cloud while providing controlled data access. The proposed system leverages the decentralized and immutable nature of blockchain to ensure the integrity and security of stored data. Blockchain technology, known for its decentralized and immutable nature, can enhance the security and transparency of data storage. In this proposed approach, data is encrypted and distributed across multiple nodes in the cloud, eliminating the risk of a single point of failure. The data is then recorded as a series of tamper-proof blocks on a blockchain, ensuring data integrity and preventing unauthorized modifications. Each block includes a hash pointer that links it to the previous block, creating a chain of blocks that forms the blockchain. These independent entities perform regular audits on the stored data and verify its integrity against the hashes stored on the blockchain. The proposed system enhances the security of data storage using AES based encrypted data storage and eliminating single points of failure and preventing unauthorized modifications. By leveraging the decentralized and transparent nature of blockchain technology, this approach addresses the limitations of traditional cloud storage systems, providing enhanced security, data integrity, and controlled data access.

KEYWORDS: Blockchain verification, Data Auditing, Access Control, Blockchain Nodes, Tamper- Proof.

I.INTRODUCTION

In dynamic and distributed computing environments, organizations increasingly leverage multi-cloud architectures to enhance resilience, scalability, and resource flexibility. Multi-cloud replication emerges as a pivotal strategy, allowing data to be seamlessly distributed across multiple cloud service providers. This paradigm shift introduces a pressing need for robust data auditing mechanisms to ensure data integrity, compliance, and security across diverse cloud environments. The concept of multi-cloud replication-based data auditing revolves around the meticulous examination and verification of data replicas spread across different cloud infrastructures. By deploying replication strategies, organizations not only safeguard against potential data loss but also seek to address auditability challenges posed by the intricate nature of multi-cloud deployments. This approach facilitates comprehensive monitoring and tracking of data movements, modifications, and access events, enabling organizations to maintain a granular level of control over their distributed data assets. Key considerations in multi-cloud replication-based data auditing include the development of sophisticated audit trails, ensuring the consistency of replicated data, and implementing real-time monitoring mechanisms. These measures collectively empower organizations to detect unauthorized access, or data inconsistencies promptly.

PURPOSE

The purpose of this project is to revolutionize data storage practices by proposing a blockchain-based approach that addresses the vulnerabilities inherent in traditional centralized cloud storage systems. With a focus on enhancing security, data integrity, and controlled access, this project aims to mitigate risks such as single points of failure, data breaches, and unauthorized access. By leveraging the decentralized and immutable nature of blockchain technology, data is encrypted and distributed across multiple nodes in the cloud, eliminating the risk of a single point of failure. Furthermore, the use of tamper-proof blocks on a blockchain ensures the integrity of stored data, preventing unauthorized modifications and enhancing transparency. Through mechanisms for controlled access and auditing capabilities enabled by blockchain, this project seeks to provide a more secure, reliable, and transparent data storage solution, contributing to the development of trustworthiness in cloud storage infrastructures.

OBJECTIVES

Ensure the integrity of data stored in the cloud by leveraging blockchain's decentralized and tamper-resistant nature. Distribute data storage across multiple nodes in a decentralized network to eliminate single points of failure and enhance resilience against attacks or system failures.

EXISTING SYSTEM

Integrity auditing techniques are considered as an effective means to detect the integrity of cloud storage data. Considering that it is impractical to download the complete data for inspection, (provable data preserve) PDP was invented to take a sampling approach to indicate the data integrity with probability. A large number of PDP schemes have been proposed afterwards. The common way to this method is that the user divides the original file into data blocks before uploading, and generates a tag for each block, called homomorphic verifiable tag (HVT). The data blocks and tags are then outsourced to the CSP. When an audit is launched, a challenge containing a random index set and a random number set is sent to the CSP, then the CSP is required to generate a proof of data integrity based on the challenge. By verifying this proof, it can be known whether the outsourced data is intact or not with high probability. Later, in order to free data owners from heavy audit tasks and to alleviate the disputes between data owners and CSPs over audit results, third-party auditors (TPAs) were introduced to carry out audits instead. In public verification schemes, after data outsourcing, the user sets a verification period (i.e., the frequency at which the auditor performs the verification). Then the auditor verifies the outsourced data integrity at the corresponding time. In practice, the auditor generates a verification report containing multiple verification results. If in any period the verification result is “Reject”, it means that the data may be corrupted and the auditor needs to inform the user at once. Otherwise, the auditor generates a verification log and provides the user with the log at the end of each epoch. Since the auditor is able to verify the data integrity without the user’s participation, the user can assign the auditor to perform the verification with any period as needed.

DISADVANTAGES

- Cannot resist a procrastinating auditor who may not perform the data integrity verification on schedule
- Deviate from the original objective of public verification schemes.
- It might be too late to recover the data loss or damage if the auditor procrastinates on the verification.
- The procrastinating auditor also cannot be detected in the public verification schemes, even though malicious auditors can be detected there.

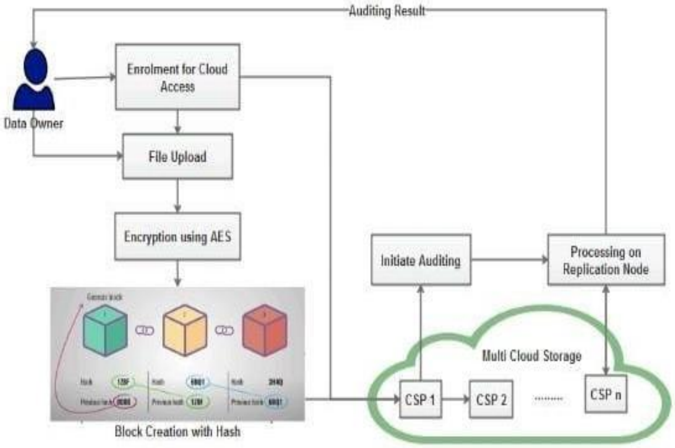
PROPOSED SYSTEM

In proposed work, implement a new model for remote data integrity auditing called CIA (Collaborative Integrity Auditing). Integrate a blockchain-based cloud storage data auditing scheme to protect the integrity of outsourced data and accurately identify the malicious CSP or organizer. Here use the verifiable tags to design a network storage service verification mechanism in a cloud system, which supports users to verify the integrity of outsourced data in batches, thus reducing the overhead during the service verification phase. Here also introduce blockchain technology to enable trusted public audits. The user outsources his data to multiple CSPs. To improve the data storage security, here utilizing Advanced Encryption Standard (AES) algorithm. AES is a symmetric based encryption algorithm that provides simple structure for encryption and decryption process. In addition to the reduction in computational overhead, the proposed scheme provides unprecedented support for free data blocking. Multiple replicas are one of the most common approaches to achieve data redundancy. The user generates multiple replicas of a data file, which are then outsourced to multiple CSPs. If a corruption of one replica on a CSP occurs, the user can recover it with other intact replicas on other CSPs. Collaborative integrity auditing among CSPs allows a CSP to act as auditor.

ADVANTAGES

- With the use of blockchain technology data cannot be altered or tampered with without detection.
- The proposed system can handle large volumes of data efficiently.
- The communication and computation overhead should be as efficient as possible.
- Collusion between any two participants cannot break the security of the proposed scheme.

SYSTEM ARCHITECTURE



FUTURE ENHANCEMENT

Future system focus on implement continuous monitoring, logging, and real-time notifications empower data owners with the tools needed to proactively manage and secure their data assets. As cloud technologies continue to evolve, this integrated approach positions itself as a forward-thinking solution, contributing to the resilience and trustworthiness of data management practices in the digital era.

CONCLUSION

In conclusion, the integration of AES-based encrypted data storage within a blockchain network, coupled with multi-cloud replication- based data auditing, presents a sophisticated and comprehensive solution for ensuring the security, integrity, and auditability of data in dynamic cloud environments. The use of blockchain technology as a decentralized and tamper-resistant ledger, combined with smart contracts and AES encryption, establishes a robust foundation for protecting sensitive information.

REFERENCE

[1] Xu, Yang, Cheng Zhang, Guojun Wang, Zheng Qin, and Quanrun Zeng. "A blockchain-enabled deduplicatable data auditing mechanism for network storage services." IEEE Transactions on Emerging Topics in Computing 9, no. 3 (2020): 1421-1432.

[2] Shen, Wenting, Jing Qin, Jia Yu, Rong Hao, Jiankun Hu, and Jixin Ma. "Data integrity auditing without private key storage for secure cloud storage." IEEE Transactions on Cloud Computing 9, no. 4 (2019): 1408-1421.

[3] Xu, Yang, Ju Ren, Yan Zhang, Cheng Zhang, Bo Shen, and Yaoxue Zhang. "Blockchain empowered arbitrable data auditing scheme for network storage as a service." IEEE Transactions on Services Computing 13, no. 2 (2019): 289-300.

[4] Yang, Xiaodong, Xizhen Pei, Meiding Wang, Ting Li, and Caifen Wang. "Multi-replica and multi- cloud data public audit scheme based on blockchain." IEEE Access 8 (2020): 144809-144822.

[5] Xue, Jingting, Chunxiang Xu, Jining Zhao, and Jianfeng Ma. "Identity-based public auditing for cloud storage systems against malicious auditors via blockchain." Science China Information Sciences 62 (2019): 1-16.

[6] Zhang, Yuan, Chunxiang Xu, Xiaodong Lin, and Xuemin Shen. "Blockchain-based public integrity verification for cloud storage against procrastinating auditors." IEEE Transactions on Cloud Computing 9, no. 3 (2019): 923-937.

[7] Li, Jiguo, Hao Yan, and Yichen Zhang. "Efficient identity-based provable multi-copy data possession in multi-cloud storage." IEEE Transactions on Cloud Computing 10, no. 1 (2019): 356- 365.

[8] Tian, Hui, Fulin Nan, Hong Jiang, Chin-Chen Chang, Jianting Ning, and Yongfeng Huang. "Public auditing for shared cloud data with efficient and secure group management." Information Sciences 472 (2019): 107-125.

[9] Li, Jiaxing, Jigang Wu, Guiyuan Jiang, and Thambipillai Srikanthan. "Blockchain-based public auditing for big data in cloud storage." Information Processing & Management 57, no. 6 (2020): 102382.

[10] Rajput, Ahmed Raza, Qianmu Li, and Milad Taleby Ahvanooey. "A blockchain-based secret- data sharing framework for personal health records in emergency condition." In Healthcare, vol. 9, no. 2, p. 206. MDPI, 2021.