International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

Blockchain-Based Secure Data Storage Framework for Cloud Computing

Subasri E[1] , **Dr. B. Leelavathi** [2]

1. Student Department of Computer Technology, Dr. N.G.P. Arts and Science College, Coimbatore, India, Email: 231ct157@drnpasc.ac.in
2. Professor Department of Computer Technology, Dr. N.G.P. Arts and Science College, Coimbatore, India, Email: get2leelavathi@gmail.com

https://doi.org/10.55041/ijsmt.v2i3.101

Cite this Article: E, S. (2026). Blockchain-Based Secure Data Storage Framework for Cloud Computing. International Journal of Science, Strategic Management and Technology, *02*(03). https://doi.org/10.55041/ijsmt.v2i3.101

Abstract

Data storage has been transformed by cloud computing, which offers scalable, flexible, and affordable services. Centralized cloud architectures are still susceptible to insider threats, data manipulation, integrity breaches, and a lack of transparency, though. In cloud systems, ensuring data integrity and trust has emerged as a significant research topic. In order to provide a decentralized and impenetrable verification method, this study suggests a Blockchain-Based Secure Data Storage Framework that combines blockchain technology with cloud computing.

The Advanced Encryption Standard (AES) is used in the suggested method to encrypt files prior to cloud storage. Smart contracts are used to create and store a SHA-256 cryptographic hash of the encrypted file on the blockchain.

The hybrid design uses blockchain's immutability for secure integrity verification while ensuring scalability using off-chain cloud storage. In order to identify any unauthorized changes, the system recalculates the file hash during data retrieval and compares it with the blockchain record. The suggested approach guarantees safe data verification in cloud contexts, increases transparency, strengthens auditability, and does away with centralized trust dependency.In comparison to conventional cloud storage systems, experimental study shows enhanced security and dependable tamper detection

Keywords

Blockchain, AES encryption, SHA-256, cloud computing, data integrity, smart contracts, decentralized storage, tamper detection, secure cloud framework, and cryptographic hashing.

1.Introduction

One of the most revolutionary technologies in contemporary information systems is cloud computing. Instead of using local storage devices, it allows businesses and people to store, manage, and process data via remote servers.

Large cloud service providers with scalable infrastructure, high availability, and affordable storage options include Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform. These benefits have made cloud computing a crucial platform for government agencies, enterprises, healthcare systems, and educational institutions.

Cloud computing has serious security issues despite its advantages. Conventional cloud storage systems use a centralized architecture, giving the cloud service provider complete control over the data they store. Potential hazards brought forth by this centralized paradigm include insider threats, illegal access, data breaches, and data manipulation.

Because the service provider frequently lacks visible procedures to confirm data integrity, users are forced to rely significantly on their reliability.

A crucial component of cloud security is data integrity. Throughout its existence, it guarantees that stored data is accurate, consistent, and unchanged. Current integrity verification methods frequently rely on centralized monitoring systems or independent auditors.

However, the system's overall dependability is impacted if the central authority is compromised. Blockchain technology presents a viable way to address these issues. Blockchain is a distributed, decentralized ledger system that guarantees tamper resistance, immutability, and transparency. It is feasible to establish a secure verification system without disclosing private information by storing cryptographic hash values on the blockchain rather than the real data.

This study suggests a Blockchain-Based Secure Data Storage Framework that combines cloud storage systems with blockchain technology, encryption, and cryptographic hashing. The framework seeks to improve transparency, remove reliance on centralized trust, and offer trustworthy tamper detection.

The suggested solution guarantees scalability and security in cloud computing environments by fusing on-chain hash verification with off-chain cloud storage.

2.Literature Review

Despite significant advancements in blockchain, cryptographic verification, and cloud securitytechnologies, several challenges remain, including scalability, real-time monitoring, and efficient integration of security mechanisms into distributed storage systems. These limitations highlight the need for advanced secure cloud storage frameworks that combine blockchain technology, cryptographic verification, and intelligent security mechanisms to ensure reliable and trustworthy data management..

3.Problem Statement

Cyber threat identification has become more difficult and sophisticated due to the quick rise in network traffic and digital communication. Conventional intrusion detection systems rely on static, signature-based techniques that are only able to detect known attacks; they are unable to detect evolving hostile activity and zero-day attacks.

Additionally, these solutions are not flexible enough to adjust to changing network settings, which leads to increased vulnerability and delayed detection.
Furthermore, a lot of current security solutions lack integrated alarm systems, intelligent prediction, and real-time monitoring inside a single framework. High false positive rates might lead to alert fatigue and further reduce efficiency.

In order to improve proactive network security, a scalable and adaptable system that continually analyzes live network traffic, employs machine learning to identify and anticipate cyber threats in real time, and produces timely alerts is required.

4. Objectives

This project's primary goal is to use blockchain technology to provide a safe, decentralized, and impenetrable data storage architecture for cloud computing. The approach seeks to decrease reliance on centralized cloud security methods while improving data integrity, openness, and trust.

4.1 Secure Data Storage in Cloud

To design a system that securely stores user data in the cloud using encryption techniques to prevent unauthorized access and data breaches.

4.2 Blockchain Integration for Data Integrity

To incorporate blockchain technology to preserve unchangeable recordings of data that has been stored. To guarantee tamper-proof verification, every data transaction or update will be documented as a block.

4.3 Decentralized Verification Mechanism

To do away with the need for centralized control by putting in place a decentralized validation system that uses blockchain consensus techniques to confirm data integrity.

4.4 Data Tampering Detection

To create a system that compares current data hashes with blockchain-stored hashes in order to identify any unauthorized changes in cloud-stored data.

International Journal of Science, Strategic Management and Technology
Volume **02** Issue **03** March-**2026** | ISSN: **3108-1762 (Online)** | Impact Factor: 3.8
An International, Peer-Reviewed, Open Access Scholarly Journal Indexed in recognized academic databases

4.5 Transparency and Auditability

To provide transparent and traceable data access logs, enabling users to audit and verify all storage and retrieval operations securely.

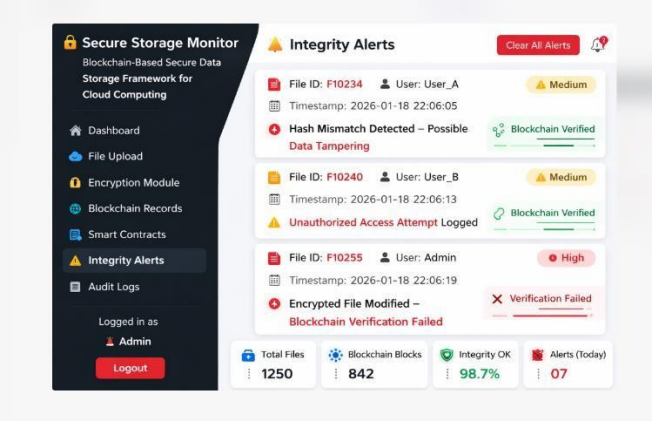

Fig 1: Secure Cloud Data Integrity Monitoring Interface

5. Methodology

To guarantee safe and impenetrable cloud storage, the suggested Blockchain-Based Secure Data Storage Framework for Cloud Computing adheres to a methodical procedure. Before being stored in the cloud, user data is first uploaded and encrypted.

To guarantee immutability, a cryptographic hash of the file is created and stored on the blockchain using smart contracts. To ensure data integrity, the system recalculates the hash each time the file is viewed and compares it with the blockchain record. An alert is produced if a mismatch is found. The technology guarantees safe, transparent, and dependable cloud data storage by combining encryption, blockchain verification, and audit logging.

5.1 Data Collection

In this system, data collecting entails obtaining crucial information about file activity and cloudstorage transactions. Information like user ID, file ID, timestamps, hash values, and transaction status are all recorded by the system.

The blockchain network and cloud storage technology are used to gather this data. These documents support data integrity verification, file modification tracking, unauthorized access detection, and storage operations transparency.

Attribute Name	Description
timestamp	Time when the file was uploaded, accessed, or modified
user_id	Identity of the user performing the operation
file_id	Unique identifier of the stored file
file_hash	Cryptographic hash value of the file
blockchain_txn_id	Transaction ID generated in blockchain
status	Verification result (Verified / Tampered)
description	Summary of storage or integrity event

Table.1 Dataset Description

5.2 Data Storage and Preprocessing

User data is uploaded to the cloud storage system during the initial phase. To maintain confidentiality, the file is encrypted before being stored. To produce a distinct digital fingerprint of the file, a cryptographic hash (such SHA-256) is created.

Duplicate records are eliminated, missing values are addressed, and transaction data is appropriately arranged during preparation. A smart contract is then used to store the hash value on the blockchain. This guarantees immutability and keeps stored records from being altered without authorization.

5.3 Blockchain-Based Integrity Verification Framework

Every time the file is read or downloaded, the system verifies its integrity after saving the encrypted file in

the cloud and its hash on the blockchain. The hash of the file is recalculated and compared to the hash kept in the blockchain ledger. The file is confirmed to be safe and legitimate if both hash values match. The system recognizes a discrepancy as possible data manipulation and sends out an alarm if it is found. Every action is recorded for transparency and auditing purposes.

In cloud computing contexts, this system guarantees decentralized verification, tamper detection, safe storage, and increased confidence.

6. Results and Discussion System Performance Evaluation

Data integrity verification, transaction processing efficiency, and system stability were used to assess the suggested blockchain-based framework. The findings demonstrate that by creating and storing cryptographic hash values on the blockchain, the system effectively protected data saved in the cloud. Accurate integrity verification was carried out without any data loss.

Tampering Detection Effectiveness

The system effectively detected unauthorized modifications by comparing recalculated file hashes with blockchain-stored hash values. Any mismatch was immediately identified as data tampering. This demonstrates the reliability of blockchain in ensuring immutability and trust.

Data Integrity and Transparency

Blockchain technology integration made storage activities transparent and traceable. To provide accountability and auditability in the cloud environment, every file upload, access, and update was documented as a blockchain transaction.

Security Enhancement over Traditional Cloud Storage

The suggested framework decreases reliance on third-party trust and does away with single-point failure, in contrast to conventional centralized cloud storage solutions. Data security and resistance to integrity assaults are greatly enhanced by the decentralized verification process.

System Reliability and Practical Applicability

It turned out to be an effective and scalable architecture that combined encryption, blockchain verification, smart contracts, and automated notifications. The findings verify that the suggested solution improves cloud computing environments' data security, transparency, and trust.

7. Conclusion

In order to improve data integrity, transparency, and confidence in cloud environments, this article proposed a Blockchain-Based Secure Data Storage Framework for Cloud Computing. Within a single architecture, the suggested system combines data encryption, cryptographic hash creation, blockchain-based verification, smart contracts, and automated integrity alarms. The solution guarantees immutability and stops unwanted data alteration by putting file hash values on the blockchain. Every time a file is accessed or altered, its integrity is confirmed by comparing the blockchain record with the recalculated hash. This system keeps trustworthy audit trails and successfully identifies efforts at manipulation.

The suggested approach improves security through decentralized verification and does away with single-point dependency, in contrast to conventional centralized cloud storage solutions. The outcomes show that the system offers a safe, transparent, scalable, and impenetrable way to safeguard private information in cloud computing settings.

8. Future Scope

By incorporating cutting-edge security features and scalable blockchain architectures, the suggested Blockchain-Based Secure Data Storage Framework for Cloud Computing can be further improved. Future developments could involve the use of consortium or hybrid blockchain architectures to save operating costs and increase transaction speed.

To improve data privacy while preserving verification capabilities, the system can also be expanded by including cutting-edge cryptographic techniques like homomorphic encryption and zero- knowledge proofs. Security can be further

strengthened by putting role-based access restriction and multi-factor authentication into practice.

The framework can be used in large-scale cloud systems in the future to provide enterprise-level data storage with improved performance optimization and scalability. Decentralized storage efficiency can be increased by integrating with cutting-edge technologies like edge computing and the InterPlanetary File System (IPFS). Enhancing smart contract security, streamlining consensus processes, and lowering blockchain latency might be the main topics of future study. These improvements will improve secure cloud storage systems' scalability, performance, and general dependability.

9. References

[1] S. Nakamoto, *"Bitcoin: A Peer-to-Peer Electronic Cash System,"* 2008.

[2] V. Buterin, *"A Next-Generation Smart Contract and Decentralized Application Platform,"* Ethereum Whitepaper, 2014.

[3] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI)*, 1999.

[4] L. Lamport, R. Shostak, and M. Pease, "The Byzantine Generals Problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[5] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 5, pp. 847–859, 2011.

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," *IEEE International Conference on Quality of Service (IWQoS)*, 2009.

[7] H. Shacham and B. Waters, "Compact Proofs of Retrievability," *ASIACRYPT 2008 – Advances in Cryptology*, Springer, 2008.

[8] National Institute of Standards and Technology (NIST), *"Advanced Encryption Standard (AES),"* FIPS PUB 197, 2001.

[9] B. Leelavathi, "An Efficient Worm Detection System Using Multi Feature Analysis and Classification Techniques," *Springer Nature Link,* vol. pp 1054–1064, 2019