iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: IX Month of publication: September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74029

# Decentralized Cloud Storage Architecture Using Block Chain for Data Integrity

Miss. Tafeem[1], Mrs. Jennifer Mary S[2]
[1]*Department Of MCA, Ballari Institute Of Technology & Management, Ballari, Karnataka, India.*
[2]*Assistant Professor, Department Of MCA, Ballari Institute Of Technology & Management, Ballari, Karnataka, India.*

***Abstract: Cloud computing offers scalable storage but raises concerns over data integrity and trust due to centralized control. This project presents a decentralized cloud storage system using blockchain to ensure secure, transparent, and tamper-proofdata handling. By integrating cryptographic hashing, smart contracts, and audit logging, the system allows users to verify data integrity without third-party auditors. Implemented with ASP.NET and C#, the prototype demonstrates secure uploads, controlled access, and verifiable audit trails, forming a foundation for future blockchain-enabled cloud systems.***

## I. INTRODUCTION

Cloud computing has become a cornerstone of the digital transformation era, revolutionizing how data is stored, accessed, and processed. Its rise has been largely fueled by the need for scalable, cost-effective, and remotely accessible computing infrastructure.

By offloading storage and computation to centralized Cloud Service Providers (CSPs), organizations reduce capital expenditure and gain flexibility in managing workloads. As a result, industries ranging from healthcare to banking, education, and government have shifted critical operations to the cloud. Users must trust that the CSP will up hold confidentiality, integrity, and availability, often without any verifiable guarantees.

This trust-based model is fundamentally flawed in environments where data sensitivity, regulatory compliance, and cyber threats are high. Reports of large-scale data breaches, insider threats, and unauthorized surveillance have highlighted the vulnerabilities in the centralized storage architectures. Traditional solutions such as symmetric encryption, authentication tokens, and access control mechanisms offer a degree of protection, but they fail to provide auditability or tamper-evidence.

Furthermore, these mechanisms are often opaque to the end-user, who has no way of verifying whether data has been accessed, altered, or deleted without consent.

Blockchain technology introduces a paradigm shift that addresses the limitations of conventional cloud storage systems. As a decentralized and immutable ledger, blockchain eliminates the need for blind trust by replacing it with mathematical proofs and consensus-driven validation. Every transaction recorded on a blockchain is time- stamped, cryptographically linked, and visible to all participants in the network. This creates an environment where data access and updates are not only traceable but permanently auditable. These capabilities make blockchain an ideal candidate for embedding trust and accountability directly into the fabric of cloud storage.

The importance of this integration extends beyond technical merit it aligns with emerging regulatory demands and the societal push toward data sovereignty and digital accountability. It not only addresses today’s challenges in cloud trust and transparency but also provides a foundation for future innovation in areas such as decentralized identity, federated cloud systems, and AI-driven anomaly detection.

## II. LITERATURE REVIEW

The limitations of traditional cloud storage systems have prompted extensive research into enhancing data integrity, privacy, and verifiability. One of the earliest and most cited works in this domain is by Q. Wang et al. [1], who proposed a public auditability mechanism that allows cloud users to verify the integrity of their stored data without retrieving the entire file. Their methodology introduced the concept of Third-Party Auditors(TPAs)that action behalf of users to perform audits. While this solution reduced communication overhead and improved efficiency, it inherently required users to trust the TPA, thereby reintroducing a centralized dependency that could itself become a point of failure or vulnerability.

The revolutionary work of S. Nakamoto [3] on Bitcoin laid the groundwork for blockchain technology a decentralized, immutable, and transparent ledger system. While initially intended for secure peer-to- peer currency exchange, its underlying principles have since been extended to data security and cloud auditing. Blockchain’s ability to eliminate centralized trust intermediaries made It a compelling foundation for building distributed auditing systems.

Expanding on this idea, X. Chen et al. [4] applied blockchain to multi-cloud storage environments, designing an integrity auditing framework that allowed dynamic user revocation and data updates. Their work utilized bilinear pairings to ensure secure proof generation and verification, and it highlighted the importance of traceability in distributed storage systems. Meanwhile, G. Ateniese et al. [7] introduced the concept of Provable Data Possession (PDP), where clients could verify that a cloud server possessed their data without retrieving it.

Further contributions by M.Lietal.[9]and

H. Tian et al. [16] focused on privacy- preserving models in sensitive domains such as healthcare. Their frameworks implemented fine-grained access controls and patient-centric policies using attribute- based encryption and dynamic audit logging. These solutions emphasized the critical need for customizable and context-aware access control mechanisms, particularly in environments handling confidential or regulated information.

## III. METHODOLOGY

The proposed decentralized cloud storage system is designed around a modular, layered architecture that integrates blockchain technology to ensure data confidentiality, integrity, and verifiability. Unlike centralized models, where control and verification are delegated to third parties, this system emphasizes trustless verification, cryptographic proof, and autonomous access control using smart contracts.

The entire architecture assegmented into five interdependent modules:User Authentication, File Management, Blockchain Ledger, Smart Contract Controller, and Audit Logging. Each module is functionally independent yet collaboratively orchestrated to ensure the secure lifecycle management of digital files in a simulated cloud environment.

### *A. User Authentication Module*

User interaction begins with authentication via secure registration and login processes. This module validates user credentials using secure hash functions, preventing unauthorized access. It establishes the identity layer critical to implementing subsequent access control and audit logging. The authentication logic is implemented in ASP.NET Identity and integrated with backend session management in C#.

### *B. File Management Module*

Once authenticated, users can perform upload, download, or share operations. Files are encrypted client-side using AES-256, a symmetric encryption algorithm known for its computational efficiency and high through SHA-256 hashing.

### *C. Blockchain Ledger Module*

A simulated block chain modules as the system's tamper-proof transaction log, preserving all file-related events such as upload, download, and share actions. Each operation is converted into a cryptographically linked block, appended to the chain in chronological order. The structure ensures immutability, providing a traceable history of user actions without dependence on a centralized database or audit authority.

### *D. Smart Contract Module*

File sharing is managed through simulated smart contracts, implemented in C#. These contracts automate access validation, permission checks, and activity logging.

When a user attempts to share a file, the smart contract cross-verifies the recipient’s role and permissions. If verified, access is granted and the event is committed to the blockchain ledger. This automation eliminates the need for manual access provisioning and enhances security through code-driven enforcement.

### *E. Audit Logging Module*

The Audit Log tracks all critical user activities across the system, Including logins, file uploads/downloads, and share events. Each action is linked with a block chain entry, forming a transparent and traceable audit trail. Users can view these logs through a frontend interface, which also flags suspicious patterns such as multiple failed login attempts or unauthorized file access attempts.

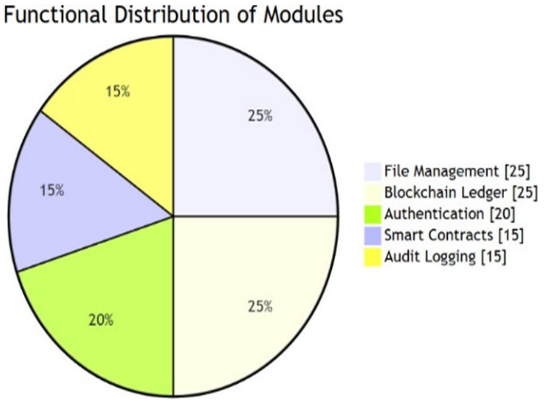

Fig1: Component-wise Logic Distribution

## IV. EVALUATION&RESULTS

The implementation of the evaluation of the proposed decentralized cloud storage architecture is conducted by analyzing its performance against multiple critical metrics that reflect the system's core objectives: data integrity, security, transparency, access control, and operational efficiency.

### *A. Data Integrity Verification Accuracy*

A central metric used to evaluate the effectiveness of the system is hash-based file integrity verification accuracy. Every file uploaded is hashed using SHA-256, and the same hash is re-evaluated during download to confirm that he file remains unaltered. In all tested scenarios, the verification returned 100% hash match accuracy, confirming the system's ability to detect tampering or corruption reliably.

### *B. Access Control Effective ness*

The smart contract enforcement of file sharing permissions was evaluated by simulating multiple user roles (owner, authorized user, unauthorized user). The smart contract logic correctly allowed or blocked access based on role validation rules.

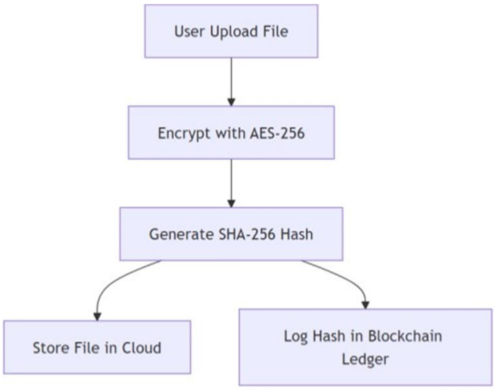

Fig2:FileUploadWorkflow

### *C. Audit Log Completeness and Traceability*

Each action upload, download, or share was logged into a simulated blockchain ledger. Evaluation confirmed that the audit trail captured 100% of operations, with accurate timestamps and user identification.

### *D. User Audit Accessibility and Alerts*

The audit log module includes a frontend interface that visualizes user activity logs. Test users wereable to retrieve their logs with zero failure. Additionally, alerts were triggered correctly during simulated integrity mismatches and unauthorized access attempts.

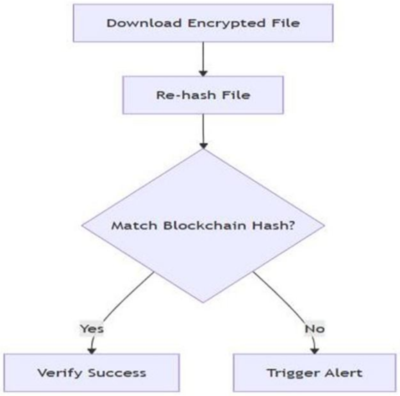

Fig3:FileDownloadVerification

## V. CONCLUSION

The proposed decentralized cloud storage architecture using blockchain effectively addresses critical challenges associated with centralized cloud systems, particularly those concerning data integrity, transparency, and access control. By integrating cryptographic hashing, AES-based encryption, and a simulated blockchain ledger, the system ensures that every file operation—whether upload, download, or sharing—is verifiable, immutable, and tamper-evident. The inclusion of role-based smart contract logic further strengthens data confidentiality by enforcing strict access policies without relying on third-party trust.

Through modular design, the framework enables secure user authentication, encrypted file management, decentralized audit logging, and automated permission handling. The evaluation metrics including hash verification accuracy, smart contract enforcement, audit traceability, and performance efficiency collectively demonstrate that the system meets its design goals.

The methodology not only reinforces user autonomy by eliminating reliance on centralized entities but also aligns with modern compliance demands for traceability and accountability.

## REFERENCES

[1] Y.Zhang,J.Liu,D.Guo,andD.Liu,"Secure and Efficient Public Integrity Auditing Scheme for Cloud Storage," IEEE Access, vol. 8, pp. 112536–112547, 2020.
[2] X.Chen,J.Li,X.Huang,J.Ma,andW.Lou,"New Public Integrity Auditing with Efficient User Revocation for Multi-Cloud Storage," IEEE TransactionsonComputers,vol.65,no.8,pp.2363–2375,2016.
[3] A.Dorri,M.Steger,S.S. Kanhere,andR.Jurdak, "Blockchain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119–125, 2017.
[4] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,"in IEEE International Congress on Big Data, 2017.
[5] R. Deng,R. Lu, C. Lai,T.H. Luan, and H. Liang, "Optimal Workload Allocation in Fog-Cloud Computing Toward Balanced Delay and Power Consumption," IEEE Internet of Things Journal, vol. 3, no. 6, 2016.
[6] L. Luu, D. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making Smart Contracts Smarter," in Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS), 2016.
[7] J.Li,Y.Shi,andY.Zhang, "Searchable Ciphertext- Policy Attribute-Based Encryption with Revocation in Cloud Storage," International Journal of Applied Cryptography, 2016.
[8] J. Yu, K. Ren, C. Wang, and V. Varadharajan, "Enabling Cloud Storage Auditing with Verifiable Outsourcing of Key Updates," IEEE Transactions on Information Forensics and Security ,vol.11,no.6,pp. 1362–1375, 2016.