Decentralized Multi-Layer Security Framework for Cloud Storage Using Hyperledger Fabric and Homomorphic Encryption

Arvind Panwar[1], Tarun Kumar[2], Shobhit Sharma[3], Prince Garg[4], Ritik Kumar[5]
[1]*Assistant Professor, arvind.cs@rdec.in, Department of CSE, R.D. Engineering College*
[2345]*Department of CSE, R.D. Engineering College, Uttar Pradesh, India*

Abstract: **Cloud storage has become an important part of modern data management, but security and privacy concerns remain critical challenges. Traditional cloud security mechanisms rely on centralized models, making them vulnerable to single points of failure, insider attacks, and unauthorized access. To address these challenges, this paper present a Decentralized Multi-layer Security Framework that integrates Hyperledger Fabric and Homomorphic Encryption to enhance the confidentiality, integrity, and availability of cloud-stored data.**

The proposed framework leverages Hyperledger Fabric, a permissioned blockchain, to decentralize access control, enforce security policies through smart contracts, and ensure tamper-proof auditability. Simultaneously, Homomorphic Encryption allowing computation on encrypted data without decryption, preserving data privacy even during processing. The multilayer security approach combines blockchain-based identity management, cryptographic access control, and encrypted computation to mitigate risks such as unauthorized data breaches, collusion attacks, and malicious modifications. Experimental results demonstrate the framework's efficiency in reducing latency while maintaining high security standards. Performance evaluations show that the approach outperforms conventional cloud security models in terms of data confidentiality, integrity verification, and resistance to insider threats. The proposed solution provides a scalable and practical safety model for safe cloud storage in domains like healthcare, finance, and IoT.

Keywords: **Blockchain, Cloud Security, Homomorphic Encryption, Hyperledger Fabric, Decentralization, Smart Contracts.**

1. INTRODUCTION

Cloud storage has emerged as a fundamental part of modern digital infrastructure, providing organizations and individuals with scalable, cost-effective, and on-demand data storage solutions. Concerns about data privacy, security and integrity are only getting worse as more and more companies turn to cloud-based architectures. Traditional cloud storage systems rely on centralized trust models, where data is managed and controlled by cloud service providers (CSPs). While this model offers convenience and efficiency, it introduces several vulnerabilities such as unauthorized access, single points of failure, insider threats, and data breaches. Moreover, users must place complete trust in third-party cloud providers to enforce security policies and maintain data confidentiality, which raises concerns regarding data misuse and adherence to legal frameworks like the CCPA, GDPR, and HIPAA.

2. CHALLENGES IN CLOUD STORAGE SECURITY

One of the standard primary security challenges in cloud storage is unauthorized access, where malicious actors exploit weak authentication mechanisms or compromised credentials to gain control over sensitive data. Additionally, data integrity threats arise due to possible tampering or corruption of stored information, either by external attackers or untrusted cloud providers. Another critical issue is privacy leakage, as traditional encryption methods protect data in idle and in transit but require decryption during processing, exposing plaintext information to potential breaches.

Furthermore, insider threats are a serious concern because CSP administrators or employees may have privileged access to data that has been stored, which could lead to data manipulation or theft. Denial-of-service (DoS) attacks can also impact cloud storage services, leading to service unavailability and data inaccessibility. These challenges necessitate a robust and decentralized security framework that minimizes reliance on centralized cloud providers while

ensuring confidentiality, integrity, and availability of stored data.

2.1 Blockchain and Cryptographic Advancements

Blockchain technology has been emerged as a promising solution for addressing cloud security challenges due to its decentralized, transparent, and tamper-resistant nature. Unlike traditional cloud storage, which depends on a single trusted authority, blockchain-based solutions distribute trust among multiple entities, reducing the risk of single points of failure. Hyperledger Fabric, a permissioned blockchain framework, is particularly well-suited for cloud security applications, as it enables identity management, role-based access control, and verifiable audit logs through smart contracts. Unlike public blockchains such as Bitcoin or Ethereum, Hyperledger Fabric provides a controlled and efficient blockchain environment, making it an ideal choice for enterprise-grade cloud security solutions. By combining Homomorphic Encryption with a blockchain-based security framework, cloud storage systems can achieve a multi-layered security model that simultaneously enforces decentralized access control, cryptographic confidentiality, and tamper-proof auditability.

3. RELATED WORK

Security and privacy issues in cloud storage have been studied carefully in recent years, leading to the development of various frameworks and models that aim to enhance data protection. Traditional cloud security mechanisms rely on centralized encryption models, access control mechanisms, and third-party trusted authorities. However, these models introduce vulnerabilities such as single point of failure, insider attacks, and unauthorized data access. To avoid these risks, researchers have explored the integration of blockchain technology, cryptographic techniques, and decentralized architectures to improve security in cloud storage. This section studies existing work related to cloud security, blockchain-based cloud frameworks, and homomorphic encryption-based privacy preservation.

3.1 Traditional Security Mechanisms for Cloud Storage

Traditional cloud storage security mechanisms primarily rely on data encryption, access control policies, and authentication protocols. Techniques such as Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), and Attribute-Based Encryption (ABE) has been widely used to secure data at rest and in transit. However, these techniques face the following challenges:

a) Data Exposure during Processing: Traditional encryption methods require decryption before data can be processed, exposing plaintext information to potential threats.
b) Centralized Trust Model: Cloud providers control the storage and management of encryption keys, leading to an one point of failure.
c) Inefficiency in Fine-Grained Access Control: Role-based and attribute-based access control methods often fail to efficiently support decentralized environments.

To overcome these challenges, researchers have turned to blockchain and cryptographic techniques such as Homomorphic Encryption to enhance cloud security.

3.2 Blockchain-based Security Models for Cloud Storage

Researchers have proposed several blockchain-based frameworks that leverage decentralized identity management, smart contracts and distributed access control to enhance cloud security.

a) Sharma et al. (2023) provides a blockchain based c loud storage system that combines intelligent security contracts, encryption and integrity confirmation mechanisms for confidentiality.[1]
b) Yang et al. (2022) Introduces a distributed access control model using blockchain technology and attribute-based encryption (ABE) to improve data security and data protection in cloud environments.[2]
c) Desai et al. (2019) presents a secure multi-user access control model system that uses blockchain technology for data integrity and can only be available for certified users using encryption keys.[3]

3.3 Homomorphic Encryption for Secure Cloud Computing

Homomorphic Encryption (HE) allows computation on encrypted data without requiring decryption, thereby preserving data privacy even during processing. This makes it a best solution for securing cloud storage. There are various homomorphic encryption schemes proposed:

a) Partially Homomorphic Encryption (PHE) – Supports only one operation (addition or

multiplication). Examples include RSA and ElGamal encryption.

b) Somewhat Homomorphic Encryption (SHE) – Allows limited computation on encrypted data but is inefficient for large-scale applications.
c) Fully Homomorphic Encryption (FHE) – Supports arbitrary calculations on encrypted data but requires high computational resources. Examples include Gentry's FHE scheme (2009) and BFV (Brakerski-Fan-Vercauteren) encryption.

Various research studies have explored the integration of Homomorphic Encryption with cloud storage: Iti Sharma, C. P. Gupta (2015) offers a complete homomorphic encryption system with symmetric keys. This allows secure calculation of encrypted data in a cloud environment.[4]

a) Benzekki et al. (2016) presents a multi-cloud architecture that enables fully approximate encryption (FHE), encrypting calculations and maintaining security at the same time.[5]
b) Biksham & Vasumathi (2016) discuss different encryption methods for secure query-based computations on encrypted cloud data.[6]

3.4 Comparison of Existing Works

Paper	Approach	Key Features	Limitations
Sharma et al. (2023)	Blockchain-based storage with smart contracts and integrity checks.	Encrypted storage, optimized failure repair.	High computation cost, limited scalability.
Yang et al. (2022)	Decentralized access control using blockchain & ABE.	Fine-grained access, smart contract verification.	Encryption overhead, latency issues.
Desai et al. (2019)	Multi-user blockchain access control ensuring data integrity.	Cryptographic access, immutable storage.	Key management challenges, security risks.
Sharma & Gupta (2015)	FHE with symmetric keys for secure computation.	Low cost, multi-user support.	Key size growth, limited real use.
Benzekki et al. (2016)	Multi-cloud FHE for encrypted data processing.	Secure computing, redundancy.	High complexity, costly setup.
Biksham & Vasumathi (2016)	SHE & FHE for query-based computations.	Privacy-preserving arithmetic.	Performance overhead, SHE limits.

4. PROPOSED FRAMEWORK

To address these security challenges associated with cloud storage, we propose a Decentralized Multi-layer Security Framework that integrates Hyperledger Fabric and Homomorphic Encryption. This framework enhances data confidentiality, privacy, integrity, access control and auditability while eliminating reliance on centralized cloud providers. By leveraging Hyperledger Fabric, we ensure decentralized identity management and access control, while Homomorphic Encryption provides secure data processing without decryption. This multi-layered approach protects against unauthorized access, insider threats, data breaches and tampering.

4.1 Framework Architecture

The proposed framework consists of the following key components:

a) User & Data Owner: Users upload encrypted data into the cloud and define access control regulations using blockchain-based identity management.
b) Cloud Storage Provider (CSP): A third-party service provider that stores encrypted data but has no access to plaintext data due to Homomorphic Encryption.
c) Hyperledger Fabric Blockchain: Implements decentralized identity management, smart contracts, and auditability for access control.
d) Homomorphic Encryption Module: Allows computation on encrypted data without the need of decryption, preserving privacy.
e) Access Control Layer: Uses smart contracts to verify user identities and enforce security policies.

f) Auditing & Integrity Verification: Blockchain stores logs of all access requests and data modifications, ensuring tamper-proof auditability.

4.2 Workflow of the Proposed Framework

Step 1: User Registration & Identity Management

a) A new user registers on the system and receives a blockchain-based identity.
b) The user generates a public-private key pair for secure authentication.

Step 2: Data Encryption & Storage

a) The user encrypts data by using Homomorphic Encryption (HE) before uploading it.
b) The encrypted data is stored on cloud servers.
c) A hash function of the data is generated and stored on the blockchain for integrity verification.

Step 3: Secure Access Control Using Smart Contracts

a) A requesting user sends an access request to the blockchain.
b) Smart contracts verify identity & access rights based on predefined policies.
c) If access is granted, the encrypted data is retrieved for computation.

Step 4: Privacy-Preserving Computation on Encrypted Data

a) The cloud server performs data processing on encrypted data using Homomorphic Encryption.
b) The results remain encrypted and sent back to the user.
c) The user decrypts the result using their private key.

Step 5: Audit Logging & Integrity Verification

a) All transactions (data access, modifications, and computations) are logged on the blockchain server.
b) Users or end users can verify the integrity of stored data by comparing blockchain records with stored hashes.

Below Figure 1 illustrates the sequence diagram between the interactions in this proposed security framework, depicting user authentication, encrypted data storage, blockchain-based access control, and privacy-preserving computation

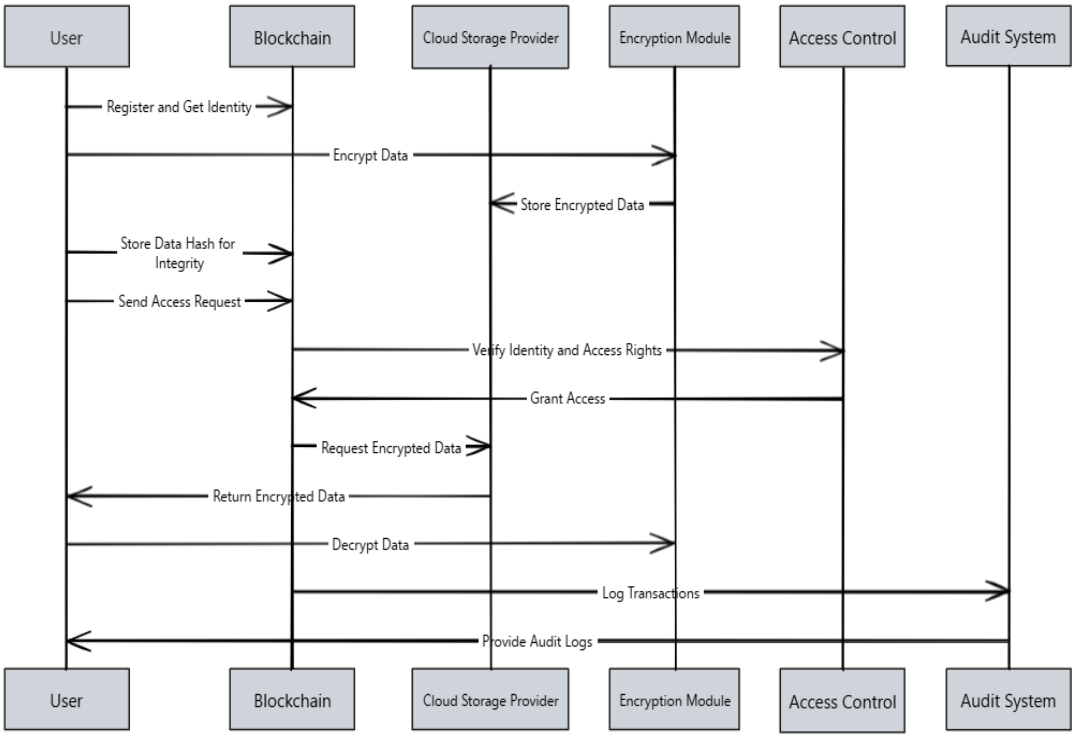

Figure 1: Sequence Diagram

5. CONCLUSION

Cloud storage has become crucial for modern data management, but security and privacy issues persist due to reliance on centralized models. This study presents a distributed multi-layer security framework that integrates Hyperledger fabric and homomorphic encryption (HE) to improve cloud security. By decentralizing identity management and access control through Hyperledger Fabric, the proposed

framework eliminates one point failure or single point of failures and reduces insider threats. Smart contracts enforce security guidelines and ensure operational checkability, but are homomorphic vulnerabilities in existing architectures. Encryption allows calculations on encrypted data without revealing the private information.

The experimental outcomes shows that this framework outperforms traditional cloud security models by improving data confidentiality, integrity, and resistance to unauthorized access. While HE introduces computational overhead, optimizations ensure that the system remains efficient and scalable. Despite some challenges, such as blockchain transaction latency and HE's computational cost, the proposed approach offers a significant advancement in cloud security. By combining distributed access control with data protection calculations, this study provides robust and scalable security solution for cloud memory. This takes into account the significant weaknesses of existing architectures.

REFERENCES

[1] Sharma, P., Namasudra, S., & Lorenz, P. (2023). Blockchain-Based Cloud Storage System with Enhanced Optimization and Integrity Preservation. *ICC 2023 - IEEE International Conference on Communications*, 3744-3749. https://doi.org/10.1109/ICC45041.2023.10279598.

[2] Yang, X., Chen, A., Wang, Z., & Li, S. (2022). Cloud Storage Data Access Control Scheme Based on Blockchain and Attribute-Based Encryption. *Security and Communication Networks*. https://doi.org/10.1155/2022/2204832.

[3] Desai, S., Deshmukh, O., Shelke, R., Choudhary, H., Sambhare, S., & Yadav, A. (2019). Blockchain based Secure Data Storage and Access Control System using Cloud. *2019 5th International Conference On Computing, Communication, Control And Automation (ICCUBEA)*, 1-6. https://doi.org/10.1109/ICCUBEA47591.2019.9129015.

[4] Sharma, I., & Gupta, C. (2015). Making data in cloud secure and usable: fully homomorphic encryption with symmetric keys. *Int. J. Commun. Networks Distributed Syst.*, 14, 379-399. https://doi.org/10.1504/IJCNDS.2015.069673.

[5] Benzekki, K., Fergougui, A., & Alaoui, A. (2016). A Secure Cloud Computing Architecture Using Homomorphic Encryption. *International Journal of Advanced Computer Science and Applications*, 7. https://doi.org/10.14569/IJACSA.2016.070241.

[6] Biksham, V., & Vasumathi, D. (2016). Query based computations on encrypted data through homomorphic encryption in cloud computing security. *2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT)*, 3820-3825. https://doi.org/10.1109/ICEEOT.2016.7755429.