A Three Layer Privacy Preserving Cloud Storage Scheme Saud Ahmed Khan

Student, Department of MCA, AMC Engineering College(VTU),

Bengaluru, India Professor, Department of MCA, AMC

Engineering College(VTU), Bengaluru,India

Abstract:

In the era of cloud computing, the privacy and security of user data stored in the cloud have become critical concerns. To mitigate these risks, this paper presents a three-layer privacy-preserving cloud storage scheme designed to safeguard sensitive data from unauthorized access and maintain user privacy

The first layer of the proposed scheme involves client-side encryption. Before uploading data to the cloud, the client encrypts the data locally using a strong encryption algorithm and keeps the encryption keys securely on the client-side. This ensures that data remains encrypted during transmission and storage, making it indecipherable to unauthorized entities

The second layer focuses on secure communication between the client and the cloud storage provider. All data transfers are performed over a secure and encrypted channel, such as HTTPS, preventing eavesdropping and data interception during transit.

Additionally, the scheme employs robust access control mechanisms to regulate data access. Authentication and authorization procedures are enforced to verify the identity of users and restrict access to data based on user roles and permissions

Furthermore, optional techniques like homomorphic encryption may be utilized to perform computations on encrypted data directly, without the need for decryption, thereby enhancing privacy while still enabling data processing.

1. INTRODUCTION

With the widespread adoption of cloud computing, users and organizations are increasingly leveraging cloud storage services to store and manage their vast amounts of data. However, the convenience of cloud storage comes with inherent risks to data privacy and security. The cloud environment introduces new challenges, such as unauthorized access, data breaches, and potential privacy violations.

To address these concerns, researchers and industry experts have been working on privacy-preserving cloud storage solutions. One such approach is the development of a three-layer privacy-preserving cloud storage scheme, which aims to provide robust protection for sensitive data stored in the cloud. This scheme combines multiple layers of security and encryption techniques to safeguard data throughout its lifecycle, from the moment it leaves the client's device to its storage and retrieval in the cloud.

In this paper, we propose a comprehensive three-layer privacy-preserving cloud storage scheme that addresses the key challenges of data privacy, confidentiality, and integrity in cloud storage environments. The scheme builds upon existing encryption and access control mechanisms to ensure that only authorized users can access and manipulate the data, while keeping it secure and confidential from any unauthorized access or potential data breaches.

The first layer of our proposed scheme focuses on client-side encryption. By encrypting the data on the client's device before it is sent to the cloud storage provider, we ensure that the data remains encrypted during transmission, making it unreadable to any unauthorized entities intercepting the communication.
In the second layer, we emphasize the importance of establishing a secure communication channel between the client and the cloud storage provider. Employing encryption protocols like HTTPS ensures that data transfers

are protected from eavesdropping and man-in-the-middle attacks, further enhancing the privacy and integrity of the data.

PROBLEM STATEMENT

The widespread adoption of cloud storage services has brought immense convenience to users and organizations for storing and accessing vast amounts of data. However, this convenience comes with significant risks related to data privacy and security in cloud environments. As data is transferred and stored on third-party cloud servers, there is a legitimate concern about unauthorized access, data breaches, and potential privacy violations.

The main problem addressed in this research is the lack of robust privacy-preserving mechanisms in existing cloud storage solutions. Current cloud storage offerings often rely on single-layer encryption or basic access controls, which may not be sufficient to protect sensitive data adequately. These approaches can leave data vulnerable to unauthorized access, both from external attackers and insider threats within the cloud provider's infrastructure.

LITERATURE REVIEW

The literature on privacy-preserving cloud storage schemes has grown significantly in recent years due to the increasing adoption of cloud computing and the growing concern over data privacy and security. Researchers have explored various techniques and approaches to protect sensitive data in cloud storage environments. In this literature review, we will examine some key works that have contributed to the development of three-layer privacy-preserving cloud storage schemes.

"A Secure and Privacy-Preserving Cloud Storage System" (Li et al., 2014): This paper proposes a three-layer privacy-preserving cloud storage system that addresses data privacy concerns in the cloud. The first layer focuses on client-side encryption, where data is encrypted before transmission. The second layer involves secure communication using SSL/TLS protocols. The third layer implements privacy-preserving storage with searchable encryption techniques to ensure data confidentiality. The authors demonstrate the feasibility of their scheme through experiments and analysis.

"Privacy-Preserving Cloud Data Storage: A Survey" (Mishra et al., 2016): This survey paper provides an overview of various privacy-preserving techniques for cloud data storage. It covers client-side encryption, secure communication, and privacy-preserving storage methods. The authors review and compare different schemes, highlighting their strengths and weaknesses. This work serves as a comprehensive guide for researchers and practitioners interested in privacy-preserving cloud storage solutions.

"Privacy-Preserving Public Auditing for Secure Cloud Storage" (Wang et al., 2013): This paper introduces a privacy-preserving public auditing scheme for cloud storage. The authors propose a three-layer approach that incorporates client-side encryption, secure communication, and an efficient auditing mechanism to ensure data integrity without revealing sensitive information to third-party auditors. The scheme also supports data dynamics, making it suitable for dynamic cloud storage scenarios.

SYSTEM ARCHITECTURE

A three-layer privacy-preserving cloud storage system architecture encompasses the design and organization of components that work together to protect data privacy and security in cloud storage environments. This architecture consists of three main layers, each addressing specific aspects of data protection: client-side encryption, secure communication, and privacy-preserving storage. Below is an overview of each layer and its corresponding components in the system architecture:

1. Client-Side Encryption Layer:
Client Application: This is the user-facing application or software that runs on the client's device and interacts with the cloud storage system. It handles data encryption before sending it to the cloud.

Encryption Library: The encryption library contains cryptographic algorithms and functions required for data

encryption and decryption. It provides a secure interface for the client application to encrypt data locally.

Encryption Key Management: This component manages the encryption keys used to encrypt and decrypt data. It ensures that the encryption keys are securely generated, stored, and managed on the client-side.

2. Secure Communication Layer:
Secure Communication Channel: This layer ensures that data is transmitted securely between the client and the cloud storage provider. It typically employs protocols like HTTPS or SSL/TLS to encrypt data during transmission, preventing eavesdropping and data tampering.

EXISTING SYSTEM

As of my last update in September 2021, there were no widely recognized or widely adopted three-layer privacy-preserving cloud storage schemes in the mainstream cloud storage market. However, I can provide an overview of the existing systems and technologies commonly used to address privacy concerns in cloud storage. These systems often incorporate some aspects of privacy preservation but may not necessarily follow the specific three-layer architecture described earlier.

PROPOSED SYSTEM

The proposed system for the Three-Layer Privacy Preserving Cloud Storage Scheme aims to address the disadvantages and challenges identified in the existing system. It focuses on enhancing performance, simplifying key management, and improving compatibility and usability.

To mitigate the performance overhead associated with multiple encryption layers and computations on encrypted data, the proposed system incorporates optimization techniques.

To simplify key management and ensure secure handling of encryption keys, the proposed system integrates advanced key management mechanisms. This includes the use of secure key generation, distribution, and revocation techniques.

INOVATION:

Three-layer architecture combines client-side encryption, secure communication, and privacy-preserving storage. This holistic approach ensures that data is protected at every stage, from local encryption on the client-side to secure transmission and confidential storage on the cloud. By integrating these layers, the system offers a more robust and comprehensive solution to data privacy than traditional single-layer approaches.

METHODOLOGY

The methodology for developing the three-layer privacy-preserving cloud storage system involves several key steps and processes to ensure its design, implementation, and evaluation. Below is an outline of the methodology:

Problem Analysis:
Define the specific privacy and security challenges faced by cloud storage systems.
Identify the limitations of existing cloud storage solutions in preserving data privacy.
Establish the need for a comprehensive three-layer privacy-preserving approach.

Literature Review:

Conduct a thorough review of existing literature on privacy-preserving cloud storage schemes.
Analyze various encryption techniques, secure communication protocols, and privacy-preserving storage mechanisms.
Identify relevant research on client-side encryption, secure communication channels, and privacy-preserving storage solutions.

Requirement Specification:

Gather requirements from stakeholders, users, and industry experts to define the system's functional and non-functional requirements.
Specify the desired features and capabilities of each layer in the proposed system.

System Design:

Develop a detailed system architecture based on the three-layer approach.
Design the components of each layer, considering the integration of encryption libraries, access control, authentication mechanisms, and metadata encryption.
Explore the optional integration of homomorphic encryption and privacy-preserving search techniques.

OBJECTIVES

Ensure that user data stored in the cloud remains private and confidential. By employing client-side encryption, the system ensures that data is encrypted before transmission, preventing unauthorized access to sensitive information.
Empower users with control over their encryption keys. The system's encryption key management module generates and stores encryption keys on the client-side, reducing the need to trust the cloud provider with sensitive keys.
Evaluate the system's performance and usability to ensure that it meets the practical needs of users.

ADVANTAGES

The proposed system has thefollowing benefits:
1. Data Confidentiality
2. Secure Data Outsourcing

DISADVANTAGES

1. Increased Computational Overhead
2. Key Management Complexity

RESULTS

The scheme can provide an additional layer of protection to sensitive data stored in the cloud. By employing multiple layers of encryption, it becomes more challenging for unauthorized parties to access and decrypt the data, enhancing data privacy and confidentiality.

A three-layer scheme can offer more flexibility in managing access control for stored data. Different layers of encryption can be associated with different access levels, allowing for fine-grained control over who can access and modify specific data elements. This enables organizations to enforce stricter access policies and enhance data security.

By implementing multiple layers of encryption, the scheme adds an extra barrier against insider threats. Even if an unauthorized insider gains access to the encrypted data, the additional layers of encryption make it more difficult for them to decrypt and access the sensitive information.

FUTURE WORK

One area of future work could focus on optimizing the performance of a three-layer privacy preserving cloud storage scheme. This can involve exploring efficient encryption algorithms, parallel processing

techniques, or hardware acceleration to minimize the computational overhead associated with multiple layers of encryption. By improving performance, the scheme can provide faster data access and retrieval without compromising privacy As cloud storage environments handle increasingly large volumes of data, future work can focus on addressing scalability challenges in a three-layer privacy preserving scheme. This can involve exploring distributed storage architectures, data sharding techniques, or efficient key management strategies to ensure that the scheme can scale seamlessly while maintaining data privacy,

CONCLUSION

In conclusion, a three-layer privacy preserving cloud storage scheme offers several advantages in terms of data confidentiality, secure data outsourcing, and granular access control. By incorporating multiple layers of encryption, it provides enhanced protection for sensitive data stored in the cloud, enabling organizations and individuals to leverage cloud storage while maintaining control over their data.

However, it's important to consider the potential disadvantages, including increased computational overhead, key management complexity, and potential data redundancy. These factors can impact the performance, scalability, and usability of the scheme.