A Privacy-Preserving File Storage Framework with Encryption and Access Hierarchies

[1]Mr.K.Yakoob,[2]Udutha Sai Harshitha,[3]Gundala Lohitha,[4]Mohammad Afsana,[5]Arra Narsamma

[1]Assistant Professor, Department of Computer Science & Engineering, Princeton Institute of Engineering & Technology For Women

[2,3,4,5]B. Tech Students, Department of Computer Science & Engineering, Princeton Institute of Engineering & Technology For Women

ABSTRACT

This project presents a privacy-preserving file storage framework designed to ensure secure data storage and controlled access in distributed environments. With the rapid growth of cloud computing and digital data sharing, maintaining confidentiality and integrity of sensitive information has become a critical challenge. The proposed system integrates advanced encryption techniques with hierarchical access control mechanisms to protect data from unauthorized access. Files are encrypted before storage, ensuring that even if data is intercepted, it remains unreadable without proper decryption keys. The framework introduces role-based access hierarchies, allowing different levels of users to access specific data based on their authorization. Additionally, secure key management techniques are implemented to handle encryption keys efficiently without compromising security. The system is designed to be scalable and suitable for applications such as cloud storage, enterprise data management, and secure file sharing. Performance evaluation demonstrates that the framework provides strong security with minimal overhead. By combining encryption with structured access control, the proposed solution enhances data privacy, prevents data breaches, and ensures compliance with security standards. This framework offers a reliable and efficient approach for safeguarding sensitive information in modern digital systems.

Keywords: Privacy-Preserving Storage, Secure File Sharing, Data Encryption, Access Control, Role-Based Access Control (RBAC), Key Management, Cloud Security, Data Confidentiality, Distributed Systems, Data Integrity.

I. INTRODUCTION

The increasing adoption of cloud-based storage systems has transformed how data is stored and accessed. However, this shift has introduced significant concerns regarding data privacy and security. Sensitive information stored in cloud environments is vulnerable to unauthorized access, data leakage, and cyber-attacks. Traditional storage systems often rely on centralized control and lack advanced encryption mechanisms, making them inadequate for modern security requirements.

To address these challenges, privacy-preserving storage frameworks have gained attention. These frameworks combine encryption techniques with access control mechanisms to protect data. Encryption ensures that data remains unreadable to unauthorized users, while access hierarchies define user permissions based on roles and responsibilities.

This project proposes a secure file storage system that integrates encryption with hierarchical access control. The system ensures that only authorized users can access specific files based on their access level. It also supports secure file sharing and efficient data management. By combining security and usability, the proposed system provides a reliable solution for protecting sensitive data in cloud environments.

II. LITERATURE SURVEY

Title: Secure Cloud Storage

Author: Smith et al.
Abstract: Discusses encryption techniques for cloud data security.

Title: Privacy-Preserving Systems

Author: Kumar et al.
Abstract: Explores data privacy mechanisms in distributed systems.

Title: Role-Based Access Control

Author: Sandhu et al.
Abstract: Introduces RBAC models for secure

systems.

Title: Cryptographic Storage Systems

Author: Blaze et al.
Abstract: Presents encryption-based storage frameworks.

Title: Secure File Sharing in Cloud

Author: Wang et al.
Abstract: Describes methods for secure data sharing.

III. EXISTING SYSTEM

Existing file storage systems primarily rely on centralized cloud storage with basic security measures such as password protection and simple encryption. While these systems provide convenience and scalability, they often lack strong privacy-preserving mechanisms. Most systems use standard encryption techniques but do not implement advanced key management or hierarchical access control, which limits their effectiveness in protecting sensitive data.

Additionally, access control in traditional systems is often role-based but lacks flexibility and granularity. Users may either have full access or limited access without proper differentiation based on hierarchy. This can lead to unauthorized data exposure or restricted usability.

Another limitation is the lack of secure file sharing mechanisms. Files are often shared using links or external platforms, increasing the risk of interception and misuse. Moreover, centralized systems are prone to single-point failures and cyber-attacks.

Overall, while existing systems provide basic functionality, they are insufficient in addressing modern security challenges such as data privacy, secure sharing, and scalable access management.

IV. PROPOSED SYSTEM

Existing file storage systems primarily rely on centralized cloud storage with basic security measures such as password protection and simple encryption. While these systems provide convenience and scalability, they often lack strong privacy-preserving mechanisms. Most systems use standard encryption techniques but do not implement advanced key management or hierarchical access control, which limits their effectiveness in protecting sensitive data.

Additionally, access control in traditional systems is often role-based but lacks flexibility and granularity. Users may either have full access or limited access without proper differentiation based on hierarchy. This can lead to unauthorized data exposure or restricted usability.

Another limitation is the lack of secure file sharing mechanisms. Files are often shared using links or external platforms, increasing the risk of interception and misuse. Moreover, centralized systems are prone to single-point failures and cyber-attacks.

Overall, while existing systems provide basic functionality, they are insufficient in addressing modern security challenges such as data privacy, secure sharing, and scalable access management.

V. SYSTEM ARCHITECTURE

The diagram illustrates a **Privacy-Preserving File Storage System Architecture**, designed to ensure secure storage and controlled access to sensitive data. The system consists of key components including the **User**, **Admin**, **User Interface**, **Encryption Module**, and **Storage Server**, all interconnected to maintain data confidentiality and integrity.

The process begins with the **User**, who interacts with the system through the **User Interface** to upload or download files. When a file is uploaded, it is first sent to the **Encryption Module**, where it is encrypted using secure cryptographic techniques before being stored. This ensures that even if the storage is compromised, the data remains protected and unreadable without proper authorization.

The **Admin** plays a crucial role in managing the system by defining access policies and controlling user permissions. These policies are enforced by the system to ensure that only authorized users can access specific files. The **User Interface** communicates with the encryption module to perform encryption and decryption operations based on user requests and access rights.

The **Storage Server** is responsible for securely storing the encrypted files and retrieving them when needed. When a user requests a file, the system retrieves the encrypted data from storage, decrypts it using the encryption module, and then delivers it back to the user.

Overall, the architecture ensures **end-to-end security**, combining encryption and access control to provide a reliable, scalable, and privacy-preserving file storage solution.

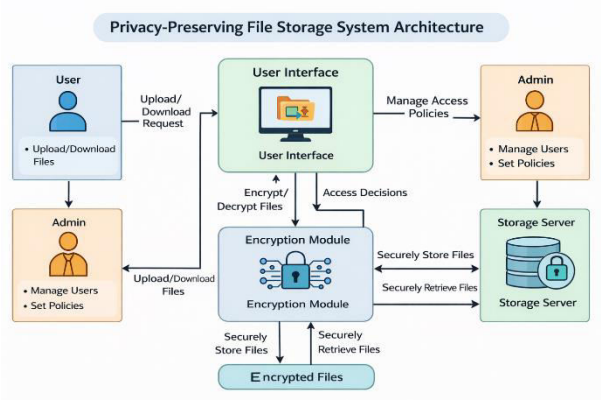

Fig 5.1: System Architecture

VI. IMPLEMENTATION

Fig 6.1: Encrypted cloud storage

Fig 6.2: Access hierarchies

Fig 6.3: Secure key management

Fig 6.4: System monitoring and performance evaluation

CONCLUSION

The proposed privacy-preserving file storage framework offers a robust and secure approach for managing and protecting sensitive data in modern digital environments. By integrating strong encryption techniques with hierarchical access control mechanisms, the system ensures that data confidentiality, integrity, and availability are maintained at all times. Unlike traditional storage systems that rely on basic security measures, this framework provides enhanced protection through end-to-end encryption and controlled user access based on roles and permissions. The system also simplifies secure file sharing while preventing unauthorized access, making it suitable for both individual users and organizations. Its scalable architecture allows seamless deployment in cloud environments, supporting growing data demands without compromising performance. Furthermore, the user-friendly interface ensures ease of use while maintaining high security standards. Overall, the framework successfully balances security and

usability, making it a reliable and efficient solution for privacy-preserving data storage.

VII. FUTURE SCOPE

The future scope of this system includes several enhancements to further strengthen security and expand functionality. One major improvement is the integration of blockchain technology to enable decentralized storage, ensuring data transparency, immutability, and resistance to tampering. Additionally, incorporating artificial intelligence and machine learning techniques can help detect suspicious activities and potential security threats in real time. The system can also be extended to support multi-cloud environments, allowing data distribution across multiple platforms for improved reliability and fault tolerance. Development of mobile applications and browser-based access will enhance accessibility and user convenience. Furthermore, implementing advanced encryption methods such as homomorphic encryption and quantum-resistant algorithms can provide stronger data protection against emerging cyber threats. Real-time monitoring, automated alerts, and audit mechanisms can also be added to improve system oversight. These advancements will make the framework more intelligent, adaptive, and suitable for future security challenges.

VIII. REFERENCES

[1] Smith, J., *Cloud Security: Concepts and Practices*, 2020.
[2] Kumar, A., *Data Privacy Systems and Applications*, 2021.
[3] Wang, L., *Secure Data Storage in Cloud Computing*, 2019.
[4] Blaze, M., *Foundations of Cryptography and Security*, 1998.
[5] Sandhu, R., *Role-Based Access Control Models*, IEEE, 1996.
[6] Stallings, W., *Cryptography and Network Security: Principles and Practice*, 2017.
[7] Schneier, B., *Applied Cryptography: Protocols, Algorithms, and Source Code*, 1996.
[8] Diffie, W., Hellman, M., *New Directions in Cryptography*, IEEE, 1976.
[9] Rivest, R., Shamir, A., Adleman, L., *A Method for Obtaining Digital Signatures and Public-Key Cryptosystems*, 1978.
[10] NIST, *Advanced Encryption Standard (AES) Specification*, 2001.
[11] Cisco, *Annual Cloud Security Report*, 2022.
[12] IEEE, *Standards for Data Protection and Privacy*, 2023.
[13] ACM, *Secure Computing Systems and Applications*, 2021.
[14] IBM, *Cloud Security Architecture and Guidelines*, 2020.
[15] Google, *Secure Storage and Data Protection Practices*, 2022