Self-Destructing Data Vault Using Cloud and KP-TSABE

An Easy-to-Understand Academic Report

1. Introduction

Cloud storage services like Google Drive, Dropbox, and SharePoint are widely used for storing and sharing files. While they offer convenience, sharing sensitive or personal data introduces security and privacy challenges. Traditional cloud storage does not provide automatic mechanisms to delete files after a specific period, which can lead to unauthorized access or data misuse. This project proposes a system that allows users to upload, share, and set an expiration time for files, ensuring secure, automatic deletion after the expiry period.

2. Problem Statement

Users often face difficulties in controlling the privacy of their data on cloud platforms. Once data is shared, it may be copied, downloaded, or misused by unauthorized users. There is no standard mechanism to automatically delete files from cloud storage after a specific time, leading to security risks and privacy violations.

3. Objectives

1. Provide secure cloud storage with user-defined expiration time for files.
2. Enable automatic self-destruction of files after expiry to prevent unauthorized access.
3. Implement fine-grained access control using KP-TSABE (Key-Policy Time-Specified Attribute-Based Encryption).
4. Develop a user-friendly system for managing secure file sharing.

4. Proposed System

The proposed system uses the KP-TSABE scheme to provide time-based access control for shared files. Each file is encrypted and associated with a time interval. Users with valid keys can access the file only within the specified time. After the expiration, the file automatically becomes inaccessible and is securely deleted from the storage.

5. Working & Features

1. Upload: Users upload files and set an expiration time. 2. Encryption: Files are encrypted using KP-TSABE, linking attributes with time intervals. 3. Sharing: Encrypted files are shared with users who have corresponding decryption keys. 4. Access Control: Users can access files only during the valid time interval. 5. Self-Destruction: Once the time expires, files are automatically and securely deleted. 6. Security: Ensures that data cannot be recovered after deletion, protecting privacy.

6. System Architecture

The system consists of three main components: 1. Client/User: Uploads files, sets expiry, and accesses shared files. 2. Cloud Server: Stores encrypted files, enforces access control, and triggers secure deletion after expiry. 3. Key Management Authority: Issues KP-TSABE keys to users and manages time-based access policies. The workflow ensures secure upload, controlled access, and automatic deletion without requiring constant user intervention.

7. Project Ideas

Project 1: Self-Destructing Data Vault using KP-TSABE

A secure cloud storage system that allows users to share files with time-limited access. Files self-destruct after the user-defined expiry period, ensuring privacy.
Novelty: Time-controlled access and automatic data destruction using KP-TSABE.
Future Scope: Extend to multi-user sharing and integrate AES encryption.

Project 2: Blockchain-Based File Deletion Verification System

Integrates blockchain with cloud storage to record file access and deletion events immutably, ensuring transparency and accountability.
Novelty: Uses blockchain for proof-of-deletion and audit verification.
Future Scope: Combine with KP-TSABE for hybrid secure access and user dashboards.

Project 3: AI-Driven Access Policy Manager for Cloud Security

An AI-powered manager that adapts access policies based on user behavior, automatically updating permissions or revoking rights to prevent unauthorized data use.
Novelty: Machine learning-based adaptive access control for enhanced cloud security.
Future Scope: Integrate with KP-TSABE and AES for multi-layered security.

8. Novelty of the Project

The project introduces a unique combination of KP-TSABE encryption and timed self-destruction of files, allowing secure file sharing in cloud environments. Unlike traditional cloud storage systems, this approach provides automatic, irreversible deletion of files and fine-grained time-based access control.

9. Conclusion and Future Scope

The proposed system addresses major challenges in cloud file security by implementing time-controlled access and automatic deletion using KP-TSABE. Users can securely share files with confidence that their data will not remain accessible indefinitely. Future work includes enabling multi-user sharing, integrating advanced encryption like AES, adding user-friendly interfaces, and exploring blockchain for audit and verification.

10. References

1. 1. Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute-Based Encryption. IEEE Symposium on Security and Privacy.
2. 2. Yang, K., Xue, Y., Li, K., & Ma, J. (2014). Time-Specified Attribute-Based Encryption for Secure Data Sharing. Journal of Information Security.
3. 3. Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. ACM CCS.
4. 4. Zhang, R., Liu, X., & Chen, Y. (2018). Secure Cloud Data Deletion Techniques: A Survey. International Journal of Cloud Computing.