Two-Level Access Control for Cloud-Based Data Exchange and Storage

Mahalakshmi K
Department of CSE
Kalaignar Karunanidhi Institute
of Technology,
Coimbatore, Tamil Nadu, India

Vidhya Bharathi R
Department of CSE
KalaignarKarunanidhi Institute
of Technology,
Coimbatore, Tamil Nadu, India

Abstract **–** Distributed computing has emerged as a transformative breakthrough, offering an efficient solution to the persistent challenge of information storage and retrieval. This paper introduces a novel approach to address the critical concern of security in distributed computing by presenting a secure admission control architecture. Utilizing a progressive structure and employing a clock-based mechanism, this architecture enhances access control granularity, ensuring secure operations such as transmission, download, and deletion of documents within the cloud environment. Key terms associated with this research include Access Control, Cloud Computing, and Cloud Privacy, as highlighted by the National Institute of Standards and Technology. Furthermore, the paper delves into the realm of secure distributed storage, an evolving facet of cloud services designed to safeguard outsourced data confidentiality while ensuring flexible access for cloud users. Cipher text- policy Attribute-Based Encryption (CP-ABE) is acknowledged as a promising method for certification verification in this context. However, the inherent "win big or bust" decryption feature of CP-ABE may lead to potential security breaches. This paper explores two instances of access credential abuse, addressing concerns both on the semi-trusted authority side and the cloud user side. To mitigate these issues, the paper proposes CryptCloud+, a secure distributed storage system based on the main responsible authority and revocable CP- ABE, incorporating white-box traceability and auditing features. A comprehensive security analysis is presented, demonstrating the effectiveness of CryptCloud+ through empirical investigations. This research contributes to enhancing the security and utility of distributed computing in the context of secure admission control and encrypted data storage.

Keywords: Attribute-Based Encryption, Cloud-based Data Sharing, CryptCloud+, Access Control, Secure Distributed Storage, Cloud Storage Service, EDoS, ECC, Ciphertext

I. INTRODUCTION

In recent years, there has been a significant focus from both academia and industry on the utilization of cloud-based storage services. These services offer advantages such as flexibility in access and the elimination of local data management, making them popular for various Internet-based commercial applications like Apple iCloud. Many individuals and businesses now prefer outsourcing their data to remote clouds to avoid expenses associated with upgrading local data management facilities and devices.

However, the widespread adoption of cloud-based storage services faces a major obstacle due to concerns about security breaches involving outsourced data. While cloud encryption is recommended to enhance data security and privacy, traditional methods may fall short in scenarios where data needs to be shared with unknown or dynamically changing users.

To address these challenges, a novel approach called dual access control is proposed in this paper. Attribute-based encryption (ABE), particularly Ciphertext-Policy ABE (CP-ABE), is considered a promising solution for protecting data in a cloud-based storage service. CP-ABE allows for fine-grained control over outsourced data and the specification of access policies for potential data receivers.

Nevertheless, merely relying on CP-ABE is deemed insufficient for an effective mechanism that ensures control over both data access and download requests. The paper introduces the concept of using dummy ciphertexts to verify the decryption rights of data receivers. While this approach provides a solution, it comes with drawbacks such as computational overhead for data owners, increased network bandwidth consumption, and additional decoding costs for users.

The central question posed in the paper is whether there exists a cloud-based mechanism that enables dual access control, covering both download requests and fine-grained data access, without compromising efficiency or security.

II. LITERATURE SURVEY

1] Existing Access Control Strategies

In the realm of distributed computing access control, various strategies have been proposed by different researchers. FADE, introduced by Y. Tang and colleagues [5], offers fine-grained admission control and guaranteed erasure, but may not be necessary when data owners and specialized cooperatives are in the same location. HASBE [2], presented by Z. Wan, J. Liu, and R. H. Deng, provides another access control plan with the main drawback of limited adaptability.

S. Yu and colleagues [10] propose a method utilizing KPABE and PRE, which, while effective, faces challenges due to the increasing complexity of encryption and decoding. Additionally, Y. Zhu and colleagues [6] present a temporary access approach suitable only for systems where data owners and specialized cooperatives share the same trusted space. M. Li and his group [4] put forward a somewhat expensive access control plan, and M. Zhou and colleagues [9] propose a privacy-preserving access control solution with certain drawbacks in terms of adaptation and versatility.

2] Recent Research Contributions:

2.1) DaSCE: Data Security for Cloud Environment with Semi-Trusted Third Party (Authors: Ali, M., Malik, S., and Khan, S.): DaSCE addresses security concerns associated with outsourcing data to a third-party administrative control in a cloud environment. It provides file assured deletion, key management, and access control. The key management employs Shamir's (k, n) threshold scheme, enhancing security by requiring multiple shares to generate the key. DaSCE's operation is verified using SMT-Lib and the Z3 solver, and its performance is evaluated based on time consumption for various operations, demonstrating its effectiveness in protecting outsourced data.

2.2) Control Cloud Data Access Privilege and Anonymity With Fully Anonymous Attribute-Based Encryption (Authors: Jung, T., Li, X. Y., Wan, Z., and Wan, M.):
This research focuses on privacy concerns related to cloud servers storing data and presents AnonyControl, a semi-anonymous privilege control method. AnonyControl decentralizes authority to prevent identity leaks, achieving semi-anonymity. Furthermore, AnonyControl-F is introduced, providing complete anonymity and preventing identity leakage. The performance evaluation demonstrates the viability of these schemes, and security analysis confirms their security under the DBDH assumption.

III. EXISTING SYSTEM

In the current system, although CP-ABE plays a role in preventing security breaches from external attackers, it presents challenges when addressing potential threats from insiders within an organization. Specifically, if an insider is suspected of participating in unauthorized activities, such as sharing decryption rights or divulging client information for unlawful financial gains, it becomes essential to conclusively establish the guilt of the insider. Moreover, is there a mechanism in place to revoke compromised access privileges In addition to these inquiries, there is an additional concern related to the key generation authority. Ordinarily, a cloud user's access credentials, such as decryption keys, are issued by a partially trusted authority based on the user's attributes. How can we ensure that this specific authority will not distribute the generated access credentials to unauthorized parties

IV. PROPOSED SYSTEM

Implementing a Digital Signature-based Trio Access Control with Key Shares for Enhanced Security:

1. Digital Signature Generation (utilizing ECC – Elliptic Curve Cryptography algorithm) – Mitigating network-based attacks and URL attacks.
2. Key Shares – The encryption key is partitioned into two shares, with one share allocated to the cloud server and the other to the data client. During the decryption and downloading process, these two shares are combined into a unified key. The client is required to provide their key share for verification, ensuring secure file decryption and download.
3. Access control for the owner (with digital signature) – Guarding against Insider Attacks.
4. User Request handling by the cloud server (with digital signature) - Counteracting Economic Denial of Sustainability (EDoS) attacks.

Advantages:

✓ The implementation of ECC in this cloud system protects against network and URL-based attacks.

✓ The concept of key shares effectively prevents key stealing attacks.

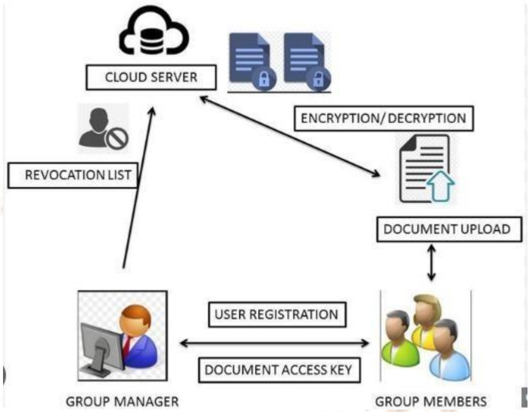


Figure 1: Proposed System

Module descriptions:

1) User Interface Administration

The User Interface Administration module is designed to cater to the specific needs of project participants, providing a tailored login page for both data owners and users. Upon logging in, data owners can seamlessly upload files, while users can input decryption keys and attributes to retrieve specific files, ensuring a user-friendly and secure experience.

2) File Encryption and Uploading

To access files within the system, users are required to register. Each file undergoes encryption with a unique encryption key before being uploaded to the storage system, ensuring data security. This module streamlines the process of safeguarding and transferring sensitive information.

3) Access Control on Upload Request

This module establishes robust access control mechanisms for upload requests, ensuring that only authorized data owners can upload and share data. The process involves the initiation of a call request by the owner, followed by meticulous processing of the request by the cloud server authority, enhancing the overall security of the system.

4) Key Share Generation

Key Share Generation involves the creation of a random secret key, K, by the Cloud Server (CS) for each data file. This key undergoes a two-step process to ensure randomness and is then divided into key shares for both CS and users in the group. These key shares play crucial roles in the encryption/decryption process, contributing to a secure and efficient system.

5) Access Control on Download Request

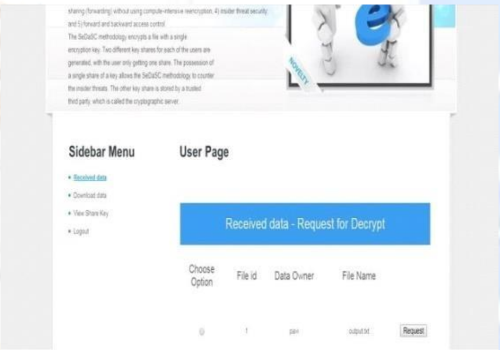
This module establishes access control for download requests, allowing only authorized users to download shared data. The process includes the initiation of a call request by the user, followed by careful processing by the cloud server authority. This ensures that data retrieval is restricted to authorized individuals, enhancing overall system integrity.

6) File Decryption and Download

Users seeking file access provide specific details, and the system responds with the encrypted file, preventing unauthorized access. Only recipients with the correct role and signature are able to decrypt the file, ensuring that information is accessed solely by authorized users and addressing concerns related to data privacy.

V. RESULTS AND DISCUSSIONS

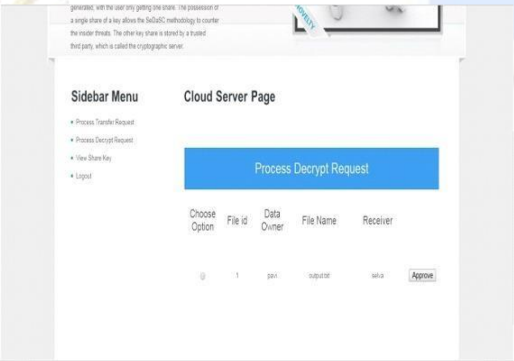
The decentralized multi-authority information access control framework employs credentials from diverse domains, managed by distinct authorities, facilitating data sharing through access policies defined with credentials from various sources. The system is developed using Java, and thorough testing is conducted by deploying each component on individual machines. Specifically, the cloud, owner, attribute authority (AA), certification authority (CA), and observer components operate on a machine featuring an Intel Core i3 processor and 4 GB RAM. The client system, utilizing an i3 processor with 2 GB RAM, interfaces with the deployed components. JRE-1.7 is universally installed across the system, while JDK 1.7, IDE: Netbeans 7.4, and Adrive Cloud are utilized for development purposes. MySQL 5.3 serves as the database for efficient data storage.



sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control
The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Choose Option	File id	Data Owner	File Name	
○	1	pavi	output.txt	Request

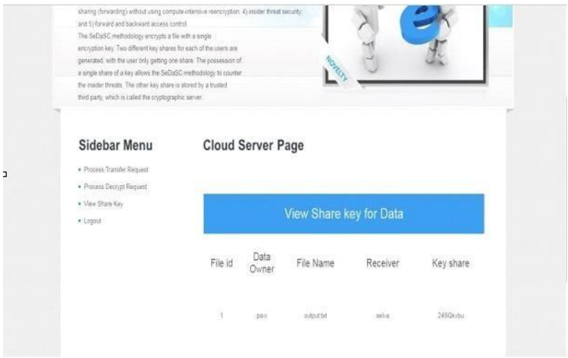
Figure 2: User Request Decrypt page



generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

Choose Option	File id	Data Owner	File Name	Receiver	
○	1	pavi	output.txt	selva	Approve

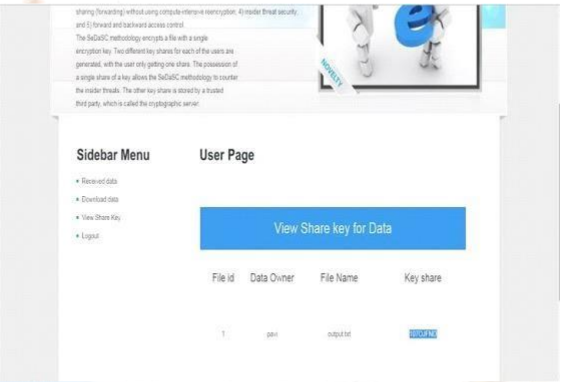
Figure 3: Cloud server approval



sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control
The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

File id	Data Owner	File Name	Receiver	Key share
1	pavi	output.txt	selva	24SQkvbu

Figure 4: Server share key page



sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control
The SeDaSC methodology encrypts a file with a single encryption key. Two different key shares for each of the users are generated, with the user only getting one share. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server.

File id	Data Owner	File Name	Key share
1	pavi	output.txt	[illegible]

Figure 5: User Download File

In essence, the result analysis emphasizes the robust architecture and compatibility of the system, ensuring effective deployment across varied machines. The utilization of Java, Netbeans, and MySQL underscores the versatility and reliability of the chosen technologies. The multi-authority approach facilitates secure data sharing with credentials from diverse authorities, contributing to the system's overall effectiveness. The thorough testing and deployment specifics affirm the system's operational integrity, setting the stage for a secure and efficient decentralized information access control framework.

VI. CONCLUSION

We addressed a compelling and reliable challenge in cloud-based information sharing by introducing two dual-access control systems. The proposed systems demonstrate resilience against DDoS/EDoS attacks. We assert that the approach employed to achieve control on download requests is "transplantable" to other CP-ABE developments. This revocable multi-authority information access scheme with evident re-encrypted decryption is secure and verifiable. In this enhanced system, we leverage the fact that the limited intelligence embedded in the domain cannot be extracted. Creating a dual access control system for cloud information sharing from a straightforward domain poses an intriguing challenge. In our future research, we aim to explore corresponding solutions to this challenge. Ensuring compatibility with existing ABE schemes and facilitating efficient user revocation will be considered in further developments.

VII. REFERENCES

[1] Mazhar Ali et al. presented Sedasc, a system ensuring secure data sharing in cloud environments, as detailed in their 2017 IEEE Systems Journal publication.

[2] Ming-Wei Shih, Sangho Lee, Taesoo Kim, and Marcus Peinado introduced T-sgx in NDSS 2017, aiming to eliminate controlled-channel attacks against enclave programs.

[3] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou, and Man Ho Allen Au explored enhancements in privacy and security for decentralized ciphertext-policy attribute-based encryption, as discussed in their 2015 IEEE Transactions on Information Forensics and Security article.

[4] Susilo Willy et al. addressed secure replication-based outsourced computation using smart contracts in their work published in IEEE Transactions on Services Computing in 2023.

[5] Shen Wenting et al. proposed an efficient identity-based data integrity auditing approach with key-exposure resistance for cloud storage in their work published in IEEE Transactions on Dependable and Secure Computing in 2022.

[6] Liu Jinlu et al. contributed to the field with their work on multi-keyword ranked searchable encryption with wildcard keywords for data sharing in cloud computing, expected to be published in 2023.

[7] Phillip Rogaway explored authenticated encryption with associated data, presenting findings in the Proceedings of the 9th ACM Conference on Computer and Communications Security in 2021.

[8] Amit Sahai and Brent Waters introduced fuzzy identity-based encryption in their work presented at Advances in Cryptology–EUROCRYPT 2005.

[9] Jianting Ning, Zhenfu Cao, Xiaolei Dong, and Lifei Wei proposed white-box traceable CP-ABE for cloud storage service, addressing the effective detection of individuals leaking their access credentials, as detailed in their 2018 IEEE Transactions on Dependable and Secure Computing publication.

[10] Jianting Ning, Zhenfu Cao, Xiaolei Dong, Kaitai Liang, Hui Ma, and Lifei Wei introduced auditable σ-time outsourced attribute-based encryption for access control in cloud computing in their 2018 IEEE Transactions on Information Forensics and Security article.