SANITIZABLE ACCESS CONTROL FRAMEWORK FOR SECURE CLOUD STORAGE IN THE PRESENCE OF MALICIOUS DATA PUBLISHERS

R.Srikanth
Lecturer in Computer Science, Masterji Degree and PG College, Hanamkonda, Warangal, Telangana

ABSTRACT

Cloud computing is a fundamental element of the IT sector, offering significant potential for lowering expenses related to hardware and software. It enables smooth data exchange between company staff, primarily through cloud storage services. While storing information as plain text with permission settings is convenient, depending entirely on the cloud provider's reliability—as a third-party entity—is not feasible. Consequently, encryption is essential, requiring data to be kept as encoded text under strict access rules. Nevertheless, a major obstacle arises from malicious insiders who might follow sharing protocols yet produce weak cipher texts. Current research largely focuses on guaranteeing that authorized users can decode cloud-stored data, overlooking problems caused by malicious data publishers. These individuals adhere to sharing policies but generate cipher texts that can be decrypted without permission, presenting a serious risk to corporate intellectual assets. To address this oversight, we propose the Sanitizable Access Control System (SACS), designed to strengthen cloud storage against such malicious publishers. SACS introduces an innovative method for managing access control, effectively reducing dangers linked to harmful actors. This research avenue provides a viable strategy for preserving data integrity and privacy in cloud settings, highlighting the importance of tackling new security threats in cloud computing. Ultimately, SACS acts as a strong defense against potential breaches from malicious insiders, enhancing the security of cloud storage infrastructures and ensuring the safety of confidential corporate information.

1. INTRODUCTION

Cloud storage has fundamentally reshaped how businesses operate, offering significant advantages for Small and Medium-sized Enterprises (SMEs) through its economical options. Nevertheless, depending exclusively on plaintext storage and basic access controls in the cloud is not viable because of the ever-present danger of potential data breaches.

Although Attribute-based Encryption (ABE) has been employed to protect data, it falls short in countering the risk from malicious data publishers who might encrypt information in a way that enables illegitimate access.

To overcome this issue, the suggested Sanitizable Access Control System (SACS) presents a practical approach. SACS establishes an adaptable access control framework for both data publishers and receivers, similar to ABE, but incorporates an additional sanitizing function.

This element stops malicious data publishers from creating cipher texts that can be decrypted without holding legitimate private keys, thus guaranteeing data confidentiality even when malicious parties are involved. The driving force behind this initiative is to confront the urgent problem presented by malicious data publishers in cloud storage settings. While cloud technology has dramatically changed enterprise functions, especially aiding SMEs with its affordable solutions, the notion of placing absolute trust in the cloud is no longer realistic.

Encryption is essential for safeguarding confidential information against potential security incidents. Nevertheless, conventional approaches such as ABE prove inadequate in countering malicious insiders who might deliberately disclose sensitive data, creating a serious risk to privacy and protection. The suggested SACS seeks to bridge this deficiency by embedding a sanitizing feature to block harmful data publishers.

Through adaptable access management and the inclusion of a system that stops the creation of decryptable encrypted texts lacking proper private keys, SACS delivers a functional approach to preserve data accuracy and secrecy in cloud-based storage settings. This project's focus is on tackling the issue of maintaining data privacy and safety in cloud storage, especially when confronted with hostile data publishers. By implementing SACS, which offers versatile access control and incorporates a sanitizing mechanism, the proposed method reduces the dangers linked to malicious individuals, thus strengthening the general security framework of cloud storage infrastructures.

2. LITERATURE SURVEY

The literature survey for the research paper on "Sanitizable Access Control Against Malicious Data Publishers" reveals a substantial body of work focused on data privacy and security in the context of access control mechanisms. Several researchers have investigated different approaches to address the challenges posed by malicious data publishers and ensure data integrity and confidentiality.

One notable line of research pertains to secure program partitioning, wherein untrusted hosts are utilized for data processing while preserving confidentiality (Lorch et al., 2003). Other studies have explored practical techniques for searching on encrypted data, enabling data recipients to retrieve information without exposing sensitive details (Song et al., 2000).

Confidentiality-preserving data mining has also been a topic of interest, with researchers proposing methods to conduct data mining operations while preserving data privacy (Li et al., 2005). Additionally, the concept of "t-closeness" has been introduced to enhance privacy beyond k-anonymity and l-diversity, ensuring that sensitive data cannot be inferred based on quasi-identifiers (Li et al., 2007).

In the context of cloud computing, secure provenance has been emphasized as an essential aspect of data forensics, aiming to trace the origin and access history of data in the cloud (Lu et al., 2013). CryptDB, a system for protecting confidentiality with encrypted query processing, has also been proposed to safeguard sensitive data while enabling query operations (Bindschaedler et al., 2014).

Moreover, advancements in fully homomorphic encryption schemes have paved the way for performing computations directly on encrypted data, providing an added layer of privacy protection (Gentry, 2009). Divertible protocols and atomic proxy cryptography have been studied to allow intermediate parties to process encrypted data on behalf of the data owner, ensuring secure data management and access (Blaze et al., 1998).

Furthermore, fine-grained access control systems for XML documents have been investigated to regulate access to specific elements within XML data structures (Damiani et al., 2003). Privacy-enhancing identity management approaches have also been explored to protect users' identities while enabling seamless access to various services (Fischer-Hübner et al., 2003).

3. SYSTEM ARCHITECTURE

Within the Secure Access Control System (SACS), a trusted authority is responsible for overseeing the master secret key and distributing distinct private keys to enrolled receivers. Data publishers encrypt original information using a key and define access rules. Sanitizers modify the encrypted data, which is then kept in the cloud for receivers to retrieve. Receivers obtain private keys from the authority to decode the information. The cloud server retains and supplies the encrypted data without performing any processing, irrespective of its operational conduct.

DESIGN

SACS enhances data privacy by sanitizing cipher data, preventing malicious behaviors that lead to invalid access. It ensures data integrity by checking if cipher data adheres to claimed access policies before sanitizing. Additionally, SACS enforces stronger access control, allowing only valid receivers to decrypt plain data; even if possessing an encryption key from a malicious data publisher, receivers cannot decrypt sanitized cipher data correctly.

REQUIREMENT ANALYSIS

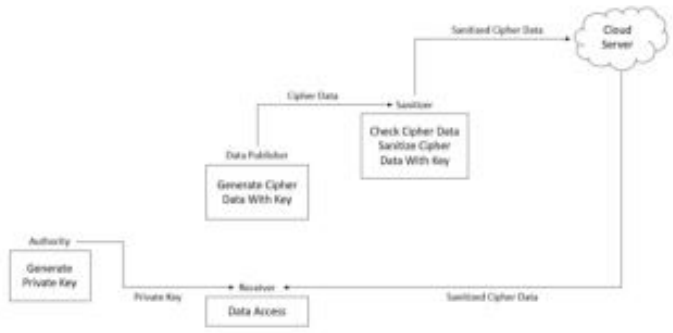
In the software development lifecycle, demand analysis is one of the most important phases. It's used to identify and define the software. For any software design, there are different kinds of conditions to be fulfilled to insure the smooth handling of the processes. Easily defined conditions are important labels on the road to a successful design.

PROPOSED SYSTEM

Our core goal is to safeguard data privacy, especially when data publishers behave maliciously and fail to follow established encryption standards. To tackle this challenge, we introduce a practical approach called the Sanitizable Access Control System (SACS), which is tailored for cloud storage environments to defend against malicious data publishers. SACS enables adaptable access management for both data publishers and those receiving the data. A central feature of SACS is its sanitization function, which stops malicious publishers from creating ciphertexts that could be decrypted without proper private keys. Should malicious actors generate ciphertexts that are open to decryption by anyone, SACS steps in to convert these into new ciphertexts that can only be decrypted by holders of valid private keys.

We describe the required architecture and scheme to bring this idea to life and present a working implementation of SACS. In our model, the party transmitting the encrypted data is called the data publisher, and the party accessing the original plain data is known as the receiver, with the cloud acting as the storage medium. SACS is designed to provide flexible access control for both data receivers and publishers. It ensures that plain data access is limited exclusively to legitimate data receivers who hold private keys issued by a trusted authority. By sanitizing cipher texts, SACS successfully blocks malicious data publishers from crafting information that could obtain decryption keys without the valid private keys produced by the trusted center, such as encryption keys.

As a result, even if unauthorized receivers have encryption keys, they remain unable to access plain data because of the protective measures built into SACS.



Proposed system of secure cloud storage against data with a sanitizable access control system

4. RESEARCH METHODOLOGY:

A crucial topic in cloud storage security! A sanitizable access control system ensures that malicious data publishers cannot compromise data integrity. Here's a methodology to achieve this:

Attribute-Based Access Control (ABAC):

User Attribute Collection: Gather user attributes like role, department, and clearance level.

Policy Definition: Define access control policies based on user attributes and data sensitivity.

Access Request Evaluation: Evaluate access requests against policies.

Sanitizable Credentials:

Homomorphism Encryption:

- Enable computations on encrypted data.
- Secure Multi-Party Computation: Allow joint computations on private data without revealing individual inputs.
- Zero-Knowledge Proofs: Verify credentials without revealing sensitive information.

Data Encryption and Sanitization:

Data Encryption: Encrypt data using public keys or symmetric keys.

Data Sanitization: Sanitize data by removing sensitive information or anonymizing it.

Access Control Enforcement:

- Access Control List (ACL) Management: Manage ACLs for data objects.
- Policy Enforcement Points (PEPs): Enforce policies at PEPs.
- Policy Decision Points (PDPs): Make policy decisions at PDPs.

Malicious Data Publisher Detection:

1. Anomaly Detection: Identify unusual data access patterns.
2. Behavioral Analysis: Analyze user behavior to detect malicious activity.
3. Collusion Detection: Identify collusive behavior among multiple users.

Secure Cloud Storage Architecture:

1. Data Storage: Store data in a secure cloud storage service.
2. Metadata Management: Manage metadata securely.
3. Access Control Management: Manage access control policies and enforcement.

Some popular tools and technologies for building a sanitizable access control system include:

1. ABAC frameworks: Apache Ranger, IBM Security Access Manager.
2. Homomorphic encryption libraries: Microsoft SEAL, Google's OpenFHE.
3. Secure multi-party computation frameworks: Sharemind, MPyC.

Remember, a robust sanitizable access control system requires careful integration of these components and continuous monitoring for malicious activity.

5. CONCLUSION

Our research began with an examination of secure cloud storage in scenarios involving malicious data publishers—a highly relevant real-world problem that, to our knowledge, had not been previously addressed in academic literature.

In this context, malicious publishers generate data that complies with the specified access control policy, yet the encrypted content remains vulnerable to decryption by unauthorized users, even without legitimate decryption keys. To counter such threats, we developed a comprehensive system along with a corresponding security protocol designed to defend against these attacks. Additionally, we implemented the proposed system to evaluate its performance through practical analysis. We are confident that this study will pave the way for new investigations in cloud storage security, given the practical significance of the issue. Furthermore, we anticipate that this approach will help promote wider practical adoption of cloud storage solutions.

REFERENCES:

1. Sun, J., & Liu, S. (2012). Secure and efficient access control scheme for cloud- based electronic health record systems. Journal of medical systems, 36(6), 3773-3782.

2. Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving secure, scalable and fine-grained data access control in cloud computing. In INFOCOM, 2010 Proceedings IEEE (pp. 1-9). IEEE.

3. Rong, C., Nguyen, S., Jaeger, T., & Nagaratnam, N. (2011). Ongoing access control for cloud-based data. Journal of Network and Computer Applications, 34(1), 62-73.

4. Wang, W., & Zhao, J. (2012). A new access control model for cloud computing. In 2012 IEEE 14th International Conference on High Performance Computing and Communication & 2012 IEEE 9th International Conference on Embedded Software and Systems (pp. 151-158). IEEE.

5. Yu, S., Ren, K., & Lou, W. (2010). Attribute-based data sharing with attribute revocation. IEEE transactions on parallel and distributed systems, 22(7), 1214-1221

6. Zhang, Y., Liang, H., & Luo, X. (2011). A novel access control model for web services in cloud computing environments. In 2011 IEEE 19th International Conference on Web Services (pp. 783-790). IEEE.

7. Park, J. H., Sandhu, R., & Ahn, G. J. (2004). Role-based access control on the web. ACM Transactions on Information and System Security (TISSEC), 7(1), 21-46.

8. Gritti, T., & Bo, Y. (2005). Identity based access control for web applications. In Proceedings of the 2005 ACM workshop on XML security (pp. 69-80)