CRYPT-SECURE : CRYPTOGRAPHIC ENFORCEMENT OF DYNAMIC CLOUD ACCESS GOVERNANCE

Ch. Upendar Rao [1]
Department of Information Technology
MLR Institute of Technology
Hyderabad,India.
upendarcse@gmail.com

M.Deva Sandeep [2]
Department of Information Technology
MLR Institute of Technology
Hyderabad,India.
devasandeep2003@gmail.com

K.Harsha Vardhan [3]
Department of Information Technology
MLR Institute of Technology
Hyderabad,India.
harshakoturi@gmail.com

Dasi Joseph [4]
Department of Information Technology
MLR Institute of Technology
Hyderabad,India.
dasijoseph666@gmail.com

V.Bhavya Laxmi [5]
Department of Information Technology
MLR Institute of Technology
Hyderabad,India.
bhavyalaxmi86@gmail.com

Abstract- One of the main concerns in cloud computing is how to effectively manage access controls for data using cryptography. While challenging, cryptographic methods are an appealing solution that both individuals and businesses want to adopt. To address this issue, a potential solution called CryptSecure has been proposed in this study. The primary goal of CryptSecure is to enable dynamic access control through cryptography. To revoke access permissions, the encrypted data in the cloud is modified as directed by CryptSecure. This technique involves a symmetric code system consisting of file codes and revocation codes. When a revocation occurs and an authorized entity uploads a new revocation code to the cloud, the file is encrypted with an additional layer of security. This triggers a corresponding adjustment in the encrypted code system.

To reduce encryption layers and keys, CryptSecure uses three key techniques that address scalability concerns. This enables efficient dynamic access control without needing resource-intensive data transmission or decryption. Authorization to access can also be withdrawn quickly. The formal implementation of the system demonstrates CryptSecure's security and effectiveness in enabling efficient and secure dynamic access control for cloud-hosted data. This approach has proven invaluable for individuals and organizations to ensure remote data is accessible smoothly and securely.

Keywords: Cryptographic techniques, confidentiality, integrity, security, proxy re-encryption, centralized system, Revocation keys .

1.INTRODUCTION

Many companies are using cloud services because they make it easier to share and store data, due to the growing popularity of cloud computing. Companies like Amazon, Microsoft, and Apple offer a wide range of cloud-based services that can be used for personal or business purposes. However, recent security breaches where unauthorized people accessed and shared personal information have highlighted the privacy risks of storing data in the cloud. These incidents show that cloud service providers need to address security vulnerabilities and design flaws in their systems as soon as possible. They also emphasize the importance of having strong data access controls in potentially insecure cloud environments.

Researchers have developed various methods to reinforce access control systems on untrusted cloud platforms. These methods utilize cryptographic techniques to address security concerns. To enforce different access control models, such as attribute-based encryption (ABE) instead of the traditional attribute-based access control (ABAC) model, these techniques often employ complex cryptographic primitives. However, current solutions primarily target static scenarios where access policy changes are infrequent, resulting in significant overhead when actual policy updates are required. Dealing with access revocation can be tricky. One common approach is to update the encryption keys linked to the files. However, this isn't perfect as users might keep copies of the old keys, risking security. This means the data has to be encrypted again with new keys, requiring file owners to download, encrypt, and re-upload the files, which adds a lot of extra work. While dynamic access control has been studied before, delaying revocation until the next file modification

often leads to communication issues or security concerns. Overall, finding an effective solution for access revocation remains a challenge.

We introduce SecureAccess, a dynamic access strategy for untrusted cloud environments that uses cryptographic methods to address these challenges. When access is terminated, SecureAccess leaves the task of updating encrypted documents to the cloud. Specifically, documents are encrypted using a list of symmetric keys, which includes both document-specific keys and termination keys. When a termination event occurs, an authorized party uploads a new termination key to the cloud, triggering an additional layer of encryption for the document. We assume a reliable yet potentially intrusive cloud environment, where the cloud performs necessary functions but may inadvertently collect private information.

The Crypt approach introduces three essential methods to maximize security and performance. First, it encrypts key lists in a compact way using a delegation-aware encryption method. This eliminates the need for users to download and decrypt large keys to access files. Administrators can also set size limits for acceptable files using a customized layered encryption technique. This balances security and effectiveness by restricting the number of encryption layers. Lastly, a delayed decryption method ensures quick access while maintaining security standards. This is done by regularly updating lists of symmetric keys and removing capped encryption layers during writing.

Experiments on Alicloud show that Crypt-DAC provides immediate access revocation, and significantly improves efficiency in access revocation and file access, compared to previous solutions.

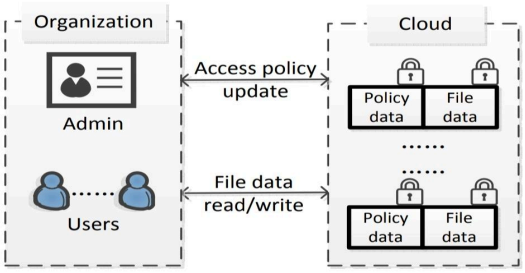


Figure-1: System General Overview

II. LITERATURE SURVEY

The literature review highlights the crucial role of cryptographic techniques in strengthening dynamic access control in cloud systems. Each study offers unique perspectives on critical issues like efficiency, security, and scalability, making them valuable contributions to the development of access control solutions such as Crypt-DAC. However, the conclusion could be strengthened by emphasizing the need for further research to address emerging concerns like interoperability, regulatory compliance, and adaptability to diverse cloud architectures. Additionally, incorporating advancements in cryptographic methods and protocols may enhance the effectiveness and robustness of cloud-based dynamic access control systems. This comprehensive approach underscores the ongoing need for innovation and research in this vital area, while also supporting the conclusions of the existing literature.

Title: "Fuzzy Identity-Based Encryption"

Citation: A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Advances in Cryptology – EUROCRYPT 2005.

Brief: presents a method of cryptography that enables adjustable access control by using identities as public keys.

Title:" DACC: Distributed Access Control in Clouds"

Citation: S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds."

Brief: suggests a way to improve data security and integrity in remote cloud systems by controlling access control.

Title: "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation"

Citation: S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation."

Brief: outlines a system that uses encryption techniques to manage access to social network data, with a focus on effective revocation processes.

Title: "Ciphertext-Policy Attribute-Based Encryption"

Citation: J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption" in IEEE 2007.

Brief: presents an encryption technique that allows for fine-grained access control over encrypted data by expressing access policies as characteristics.

Title: "Attribute Based Encryption with Revocation for Secure Data Sharing in Cloud Storage"

Citation: M. A. Salahuddin, M. F. A. Rasid, and N. H. Saad, "Attribute Based Encryption with Revocation for Secure Data Sharing in Cloud Storage."

Brief: explains how attribute-based encryption can be used to securely share data in cloud storage systems while allowing for quick and easy access right revocation.

III. PROPOSED SCHEME

Addressing the complex issues around implementing effective cryptographic access control in the cloud requires a thoughtful solution. By combining various approaches and encryption algorithms, Crypt-DAC offers a practical way to enforce dynamic access control for data stored in untrusted cloud environments. The system aims to enable cryptographically enforced access control, ensuring only authorized users can access the data.

The core of our suggested system is the symmetric key inventory, a vital part that keeps track of the access key and recently revoked keys. The file key is used to encrypt the file, and the revocation keys are essential for making it easier to remove access rights. If someone needs to have their access to a file revoked, a designated manager uploads a new revoked key to the cloud platform. The cloud platform then adds an extra layer of encryption to the file and updates the encrypted key list in response to the introduction of the revocation key. This straightforward process ensures that access permissions can be quickly and effectively revoked. Combining revocation keys with symmetric encryption guarantees that no one else can access the file without authorization, and makes it easy to grant or revoke access when needed.

This system boosts efficiency and security by skipping resource-heavy processes like decryption and re-encryption. It uses three key strategies to manage encryption layers and key lists. Data stored in the cloud is further protected by cryptographic dynamic access control and instant permission revocation, which quickly block unauthorized users. The system's real-world viability is validated through formal framework testing and implementation, proving its ability to safely enforce dynamic access control in untrusted cloud environments.

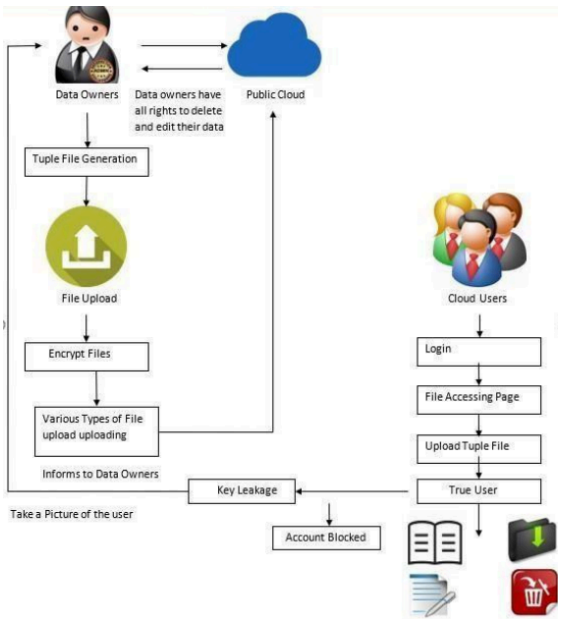


Figure-2: System Architecture

Typically, the Crypt-DAC system involves a number of entities or roles, each of which is essential to its use and efficacy:

- **Administrators:** The people responsible for managing the access control rules that regulate the data stored on cloud servers are the administrators. Their job is to manage permissions, allowing or denying access to sensitive data. They also have the duty of uploading revocation keys as needed to properly implement access control mechanisms.

- **End User:** The end users in this architecture are the individuals or organizations that require access to the data stored in the cloud. They submit requests to access specific data sets, subject to the restriction regulations of Crypt-DAC. End users must follow the established policies because their access rights may change or be canceled based on organizational needs.

- **Cloud Service Providers:** These companies offer the services and tools needed to store data in the cloud. Cloud providers maintain the necessary infrastructure and system setup, which is crucial for the smooth operation of Crypt-DAC. They also implement security measures to protect the hosted data and ensure compliance with Crypt-DAC's access control protocols.

- **Security Experts:** Specialists in access control, encryption, and cybersecurity are essential members of the Crypt-DAC network. To ensure Crypt-DAC maintains robust data protection protocols, security experts contribute their knowledge. By providing valuable insights on the most effective ways to implement and operate the system securely, they enhance its overall security posture.

Cooperation between different parties is crucial to optimize the Crypt-DAC system's ability to provide safe and effective access control for data stored in the cloud. By leveraging their specialized knowledge and positions, they help ensure the smooth functioning and implementation of access control measures, which ultimately enhances the security of data in cloud environments.

IV. METHODOLOGY

The Crypt-revocation encryption technique combines cryptographic methods and access control approaches to offer flexible and secure data access options in cloud environments that are not fully trustworthy. The standard operation of the Crypt-DAC system is outlined below:

Policy Establishment for Access Control: Data administrators define the rules that control who can access data and under what conditions. These policies outline the specific user rights and situations where data can be accessed. The policies specify which users or user groups have particular access privileges.

Data Encryption Protocol: Before data is uploaded to the cloud, it goes through an encryption process. Crypt-DAC employs encryption methods to safeguard the data when it's not in use, ensuring that only authorized individuals with the proper decryption keys can access it.

Secure Key Management: The crypto-revocation approach uses robust management procedures to ensure the security of the keys. This includes creating the keys, distributing them to authorized users, and regularly updating the keys to maintain data security.

Authentication and Authorization Process: When someone asks to see certain data, Crypt-DAC checks if they have permission to access it. The system compares the user's credentials to the access control rules. Only authorized people can get into the data because of this authentication process.

Dynamic Access Control Mechanisms: Real-time adjustments to access permissions are simplified with Crypt-DAC. Data administrators can respond promptly to evolving access needs by swiftly updating access control policies to accommodate changes in user requirements, providing flexibility.

Revocation Protocol: Crypt-DAC provides a way to revoke access if needed for an authorized user, such as when their role changes or security issues arise. Uploading revocation keys helps strengthen data security by preventing unwanted access if access changes occur.

Audit Trail Functionality: The Crypt-DAC system could include an audit trail feature to monitor data access and usage patterns. This would allow tracking of access trends, detecting potential security issues, and ensuring compliance with regulations. The audit trail would provide visibility into how the data is being accessed and used, helping to maintain security and meet compliance requirements.

The Crypt-DAC system offers a strong foundation for enabling dynamic access control that is cryptographically enforced in cloud environments. By combining these components, this comprehensive approach enhances data security, safeguards privacy, and increases access control flexibility, making it well-suited for situations where sensitive data management and access need to be secure.

Crypt-DAC presents three essential methods for enhancing dynamic access control security and performance:

1. **Delegation-Aware Encryption Strategy :** The primary aim of this approach is to efficiently encrypt key lists. This reduces the need for users to download and decrypt lengthy key lists to access files. By decreasing the computational complexity associated with key list management, this solution enhances efficiency while preserving the security of encrypted data access.

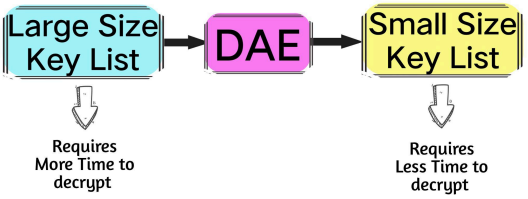


Figure-3: DAE strategy

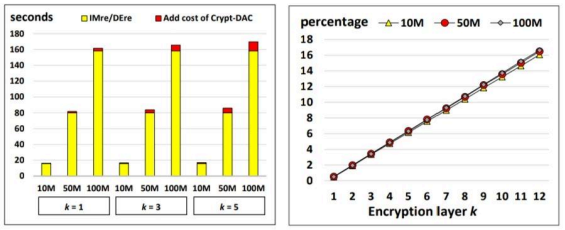
2. **Adjustable Onion Encryption Strategy :** Administrators can set limits on file sizes by using the configurable encryption approach implemented by Crypt-DAC. This feature allows them to control the number of encryption levels applied to files, balancing security and accessibility. By doing this, the system can customize its encryption strategy to meet the specific needs of the company or the data being protected.

3. **Delayed De-Onion Encryption Strategy:** This approach focuses on removing the encrypted layers during writing operations and regularly updating the lists of symmetric keys. By doing this, it ensures effective access through robust security measures by postponing the de-onion process until specific actions, like writing, instead of requiring it for every access attempt. This method reduces the performance impact.

V. RESULTS

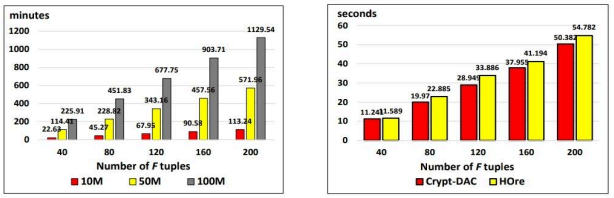
The adoption of Crypt-DAC represents a significant advancement in secure data management for cloud computing. Crypt-DAC offers a comprehensive method for implementing dynamic access control by combining modern access control techniques with cryptography. Its key strengths include encrypted data storage, real-time policy updates, and simplified access revocation. This ensures that only authorized personnel can access critical data, and gives managers the flexibility to quickly adjust access rights as needed. Additionally, Crypt-DAC's auditing features enable businesses to closely monitor data access and maintain regulatory compliance. Overall, Crypt-DAC provides a flexible and trustworthy framework for handling data in untrusted cloud environments, allowing enterprises to proactively reduce risks and protect their valuable information assets.

To simplify things, we'll refer to the two revocation techniques proposed in the cited study as immediate re-encryption (IMre) and postponed re-encryption (DEre). We'll also mention an additional revocation procedure called homomorphic re-encryption (HOre) from a different source. Next, we'll put IMre, DEre, HOre, and Crypt-DAC into practice.



(a) Performance of IMre/DEre and Crypt-DAC at user side (b) Performance of Crypt-DAC and HOre at user side

Figure-4: Performance at User Side



(a) Performance of IMre at administrator side (b) Performance of Crypt-DAC and HOre at administrator side

Figure-5: Performance at Administrator Side

TABLE I
PERFORMANCE OF CRYPT-DAC/HORE IN FILE READING

File size	Crypt-DAC	HOre	Cost of HOre
	Comp/Comm	Comp/Comm	Comp/Total
10 M	1.1/15.8 Sec	98.6/17.7 Sec	82.8/6.8 times
50 M	6.1/81.8 Sec	491.1/90.4 Sec	80.2/6.6 times
100 M	12.3/164.1 Sec	982.3/176.8 Sec	79.8/6.5 times

TABLE II
PERFORMANCE IN FILE WRITING

File size	Others	HOre	Cost of HOre
	Comp/Comm	Comp/Comm	Comp/Total
10 M	1.1/16.8 Sec	98.6/17 Sec	88.3/6.4 times
50 M	6.1/84.9 Sec	490.4/89.1 Sec	79.5/6.3 times
100 M	12.3/168 Sec	981.7/175.1 Sec	79.8/6.4 times

VI. CONCLUSION

Crypt-DAC is a creative solution to the complex challenges of secure data handling in cloud environments. It provides a comprehensive framework to enforce dynamic access control by seamlessly integrating sophisticated access control mechanisms with cryptographic techniques. Crypt-DAC's powerful features, such as encrypted data storage, real-time policy modifications, and effective access revocation methods, protect sensitive data from unauthorized access. Additionally, Crypt-DAC's auditing capabilities enable companies to closely monitor data access activities and comply with regulatory standards. This flexible and reliable technology helps organizations efficiently manage risks and safeguard their critical information assets in untrusted cloud settings. In an increasingly digital landscape, Crypt-DAC stands as an innovative beacon, assisting enterprises in navigating

the intricate domain of data security. It equips them with the confidence to effectively maintain the availability, integrity, and confidentiality of their data.

VII . ACKNOWLEDGEMENT

I am extremely grateful to the Department of Information Technology at MLRIT College for their invaluable support in completing my dissertation. Additionally, my sincere gratitude is also extended to our distinguished professors, friends, and project organizers for their advice and helpful criticism during the project.

VIII. REFERENCES

1. A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," in Advances in Cryptology – EUROCRYPT 2005.
2. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," .
3. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-Based Access Control in Social Networks with Efficient Revocation,"
4. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption " in IEEE 2007.
5. M. A. Salahuddin, M. F. A. Rasid, and N. H. Saad, "Attribute Based Encryption with Revocation for Secure Data Sharing in Cloud Storage,"
6. W. He, L. Chen, and Y. Wu, "CP-ABE with Constant-Size Ciphertexts for Secure Cloud Storage,"
7. R. Li et al., "A Secure and Efficient Dynamic Auditing Protocol for Data Storage in Cloud Computing,"
8. K. Ren, W. Lou, and Y. Zhang, "Multi-user Revocable Data Access Control for Cloud Storage,"
9. H. Jin et al., "Secure and Efficient Data Retrieval Scheme Based on CP-ABE in Cloud Storage," 2017.
10. D. Boneh, C. Gentry, B. Waters, "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys," in Advances in Cryptology – CRYPTO 2005, 2005.
11. L. Ibraimi et al., "MedSK: A Secure Key Management Scheme for Medical Applications of Wireless Sensor Networks," May 2011.
12. L. Nguyen, L. X. Bui, and C. D. Nguyen, "A Cryptographic Role-Based Access Control Model in the Cloud," in 2019 IEEE 11th International Conference on Knowledge and Systems Engineering (KSE), Oct. 2019.
13. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential Bread and Butter of Data Forensics in Cloud Computing," Jan. 2013.
14. C. Wang et al., "Toward Secure and Dependable Storage Services in Cloud Computing," in IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220-232, April-June 2012.
15. J. Zhao, Z. Cao, X. Su, and J. Liu, "Attribute-Based Proxy Re-encryption with Chosen-Ciphertext Security," 2017.
16. Y. Lu et al., "Secure and Efficient Fine-Grained Data Access Control Scheme in Cloud-Based Services," Jan.-March 2019.
17. K. Yang, X. Jia, K. Ren, and B. Zhang, "DR-ABE: Distributed Revocation in Attribute-Based Encryption for Secure Data Storage in Cloud Computing," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 1, pp. 190-199, Jan. 2015.