SECURE AND FINE-GRAINED ACCESS ENFORCEMENT FOR MULTI-OWNER CLOUD DATA SHARING

[1]Anitha,[2]Swapna,[3]Nagrendra
[123]Students
Department of CSD

ABSTRACT

Cloud computing enables convenient and scalable data storage, but it introduces significant security challenges, especially in multi-owner environments where data is shared among various users with different access rights. This paper proposes a secure and fine-grained access enforcement mechanism for multi-owner cloud data sharing. The approach employs attribute-based encryption (ABE) to enforce access policies that are both flexible and scalable. Each data owner can independently define access conditions, while the cloud service remains untrusted and cannot access plaintext data. The system supports dynamic user revocation, multi-owner cooperation, and conditional sharing based on user attributes or roles. Security analysis and experimental evaluation confirm that the proposed scheme achieves confidentiality, policy compliance, and performance efficiency, making it suitable for secure collaborative environments such as e-health systems, enterprise data sharing, and academic cloud storage platforms.

I. INTRODUCTION

The widespread adoption of cloud computing has revolutionized data storage and sharing by offering high availability, scalability, and cost efficiency. In collaborative environments such as universities, enterprises, or healthcare systems, multi-owner cloud data sharing is a common scenario where different individuals or entities upload, access, and manage data concurrently. However, ensuring data confidentiality and precise access control in such scenarios remains a critical challenge, especially when relying on third-party cloud providers that may not be fully trusted.

Traditional encryption schemes are often insufficient for fine-grained access management, as they typically require sharing decryption keys manually or lack flexibility in policy enforcement. Furthermore, managing access control for multiple users across multiple data owners without compromising security or performance is complex. In response to these issues, attribute-based encryption (ABE) has emerged as a promising technique that allows encryption and access policies to be tightly coupled with user attributes such as roles, departments, or clearance levels.

This paper introduces a secure and fine-grained access control framework designed for multi-owner cloud systems. Each owner can define their access control policies independently using attribute-based encryption, ensuring that only authorized users can access specific subsets of encrypted data. The system supports dynamic user revocation and minimizes overhead, thereby preserving both data security and operational efficiency.

1.2LITERATURE SURVEY

As cloud computing grows, so does the need for secure and efficient data-sharing mechanisms, especially in multi-owner environments where data control is distributed across multiple parties. Research on cloud-based data sharing has focused on access control, data encryption, privacy preservation, and conditional dissemination. This literature survey reviews key contributions in these areas, providing an understanding of the evolution and current challenges of secure data sharing in multi-owner cloud environments.

Access Control Mechanisms: One of the primary research areas in secure data sharing is access control. Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) are widely used to manage permissions. Sandhu et al. (1996) introduced RBAC, which assigns permissions based on users' roles, while ABAC, as introduced by Jin et al. (2012), offers finer granularity by using a broader range of attributes to define access rights. However, both models encounter limitations in dynamic, multi-owner cloud settings where permission requirements can vary across owners and use cases.

Data Encryption Techniques: To enhance security, researchers have also explored encryption-based approaches. Traditional encryption methods often lack flexibility in multi-owner systems. Recently, Attribute-Based Encryption (ABE) has gained popularity for supporting fine-grained access control. Goyal et al. (2006) introduced ABE, enabling data owners to specify conditions for data access using attributes. Additionally, Key-Policy ABE (KP-ABE) by Sahai and Waters (2005) and Ciphertext-Policy ABE (CP-ABE) by Bethencourt et al. (2007) introduced alternative approaches for assigning encryption policies directly into the encryption process. These encryption models have become foundational in multi-owner cloud frameworks, though they often come with increased computational costs and complexity.

Conditional Data Dissemination: Conditional dissemination, which involves setting criteria that recipients must meet before accessing data, is a critical component in secure data-sharing frameworks. Yuan and Yu (2013) proposed a solution to enforce fine-grained access in cloud storage using CP-ABE, while Lin et al. (2018) enhanced these mechanisms with more adaptive and context-aware dissemination methods. These conditional models provide a solution for securely sharing data without compromising owners' control over dissemination conditions. However, existing frameworks often face scalability challenges as the number of users and conditions grows, making efficient dissemination techniques a crucial area of continued research.

Multi-Owner Data Sharing: Multi-owner data sharing is particularly complex due to varying ownership rights and the need for unified access control. Yang et al. (2015) proposed a model allowing owners to retain independent control while still collaborating within the cloud environment. Similarly, Liu et al. (2019) introduced a decentralized model using blockchain for multi-owner data management, providing traceability and ownership verification in a secure, transparent manner. These models improve collaborative security but may introduce computational overhead and latency.

Privacy and Security Challenges: Data privacy in cloud-based sharing systems remains a prominent concern. Works by Liu et al. (2014) emphasize the importance of privacy-preserving methods that protect data even from the cloud provider itself. Homomorphic encryption and secure multi-party computation (SMC) have been proposed as potential solutions, allowing data processing without compromising privacy. However, these methods are still computationally intensive and may affect system scalability.

Ethical and Regulatory Considerations: Studies by Metcalf and Crawford (2016) and Shokri et al. (2011) discuss the ethical implications of cloud data sharing, particularly around privacy laws such as GDPR and HIPAA. Ensuring compliance with these regulations is especially challenging in multi-owner environments, where ownership and control are distributed.

The literature demonstrates significant progress in secure multi-owner data sharing, but challenges remain in achieving a balance between security, efficiency, and usability. This survey highlights the potential of combining access control, encryption, conditional dissemination, and privacy-preserving techniques to build a robust data-sharing framework for multi-owner cloud environments. The findings underscore the need for solutions that support dynamic access control and efficient dissemination, ensuring that security is not compromised as data sharing continues to evolve in the cloud.

2 OVERVIEW OF THE PROPOSED SYSTEM

INTRODUCTION:

The wellbeing of ladies as well as product conditions will be only a tick away at less expensive rate by machine and utilizing our normal framework The gadget will be set off over the tapping button during crisis circumstance. A section physically getting to the application this frenzy switch can likewise be utilized. During the frenzy circumstance the current area will be shipped off companions, family and furthermore to cops.

2.1 ARCHITECTURE OF THE PROPOSED SYSTEM:

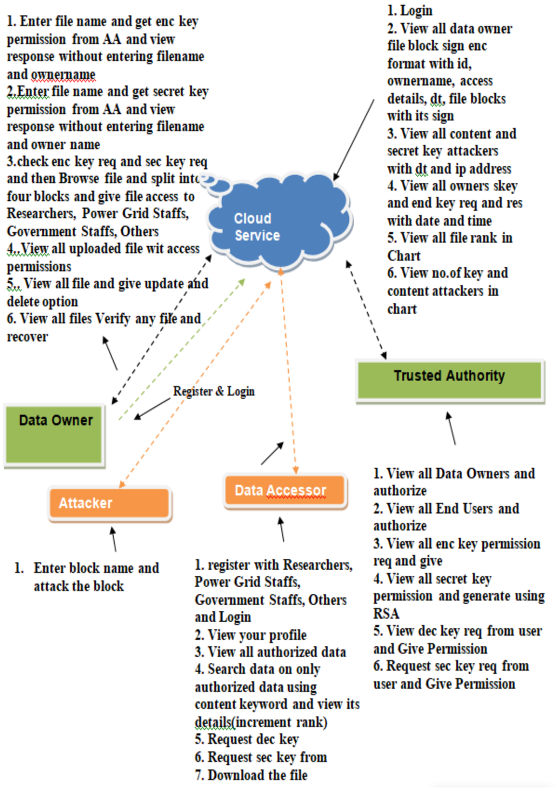
1. Enter file name and get enc key permission from AA and view response without entering filename and ownername
2.Enter file name and get secret key permission from AA and view response without entering filename and owner name
3.check enc key req and sec key req and then Browse file and split into four blocks and give file access to Researchers, Power Grid Staffs, Government Staffs, Others
4,.View all uploaded file wit access permissions
5,. View all file and give update and delete option
6. View all files Verify any file and recover
Cloud Service
1. Login
2. View all data owner file block sign enc format with id, ownername, access details, dt, file blocks with its sign
3. View all content and secret key attackers with dt and ip address
4. View all owners skey and end key req and res with date and time
5. View all file rank in Chart
6. View no.of key and content attackers in chart
Trusted Authority
Register & Login
Data Owner
Attacker
Data Accessor
1. Enter block name and attack the block
1. register with Researchers, Power Grid Staffs, Government Staffs, Others and Login
2. View your profile
3. View all authorized data
4. Search data on only authorized data using content keyword and view its details(increment rank)
5. Request dec key
6. Request sec key from
7. Download the file
1. View all Data Owners and authorize
2. View all End Users and authorize
3. View all enc key permission req and give
4. View all secret key permission and generate using RSA
5. View dec key req from user and Give Permission
6. Request sec key req from user and Give Permission

Figure: Architecture diagram

2.2 MODULES:

Data Owners (DO)

DO decide the access policy and encrypt the data with CP-ABE. The encrypted data will be uploaded to the Cloud Servers. DO are assumed to be honest in the system.

Data Requester/Receivers (DR)

DR sends the decryption request to Cloud and obtain the ciphertexts over the internet. Only when their attributes satisfy the access policies of the ciphertext, can they get access to the plaintexts. Data requester/receivers may collude to access the data that is otherwise not accessible individually.

Cloud Servers (CS)

CS are responsible for storing a massive volume of data. They cannot be trusted by DO. Hence, it is necessary for DO to define the access policy to ensure the data confidentiality. CS are assumed not to collude with DR.

Trusted Authority (TA)

AA is responsible for registering users, evaluating their attributes and generating their secret key SK accordingly. It runs the Setup algorithm, and issues public key PK and master key MK to each DO. It is considered as fully trusted.

3 PROPOSED SYSTEM

- The proposed system introduces a solution to achieve cipher text group sharing among multiple users, and capture the core feature of multiparty authorization requirements. The contributions of our scheme are as follows:
- The system achieves fine-grained conditional dissemination over the cipher text in cloud computing with attribute based CPRE. The cipher text is firstly deployed with an initial access policy customized by data owner. Our proposed multiparty access control mechanism allows the data co-owners to append new access policies to the cipher text due to their privacy preferences. Hence, the cipher text can be re-encrypted by the data disseminator only if the attributes satisfy enough access policies.
- The system provides three strategies including full permit, owner priority and majority permit to solve the privacy conflicts problem. Specially, in full permit strategy, data disseminator must satisfy all the access policies defined by data owner and co-owners. With the majority permit strategy, data owner can firstly choose a threshold value for data co-owners, and the cipher text can be disseminated if and only if the sum of the access policies satisfied by data disseminator's attributes is greater than or equal to this fixed threshold.
- The system proves the correctness of our scheme, and conduct experiments to evaluate the performance at each phase to indicate the effectiveness of our scheme.

Advantages

- The Data security is more since data co-owners can renew the cipher texts by appending their access policies as the dissemination conditions.
- The system is more secured due to Continuous policy enforcement in which the data owner's access policy is enforced in the initial cipher text as well as the renewed cipher text.

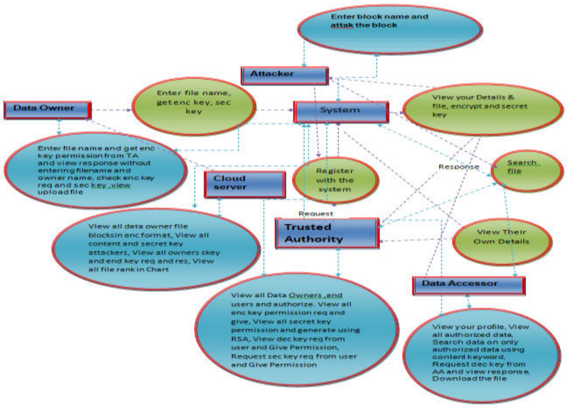
Enter block name and attak the block
Attacker
Data Owner
Enter file name, getenc key, sec key
System
View your Details & file, encrypt and secret key
Enter file name and get enc key permission from TA and view response without entering filename and owner name, check enc key req and sec key ,view upload file
Cloud server
Register with the system
Response
Search file
Request
Trusted Authority
View all data owner file blocksin enc format, View all content and secret key attackers, View all owners skey and end key req and res, View all file rank in Chart
View Their Own Details
Data Accessor
View all Data Owners ,end users and authorize, View all enc key permission req and give, View all secret key permission and generate using RSA, View dec key req from user and Give Permission, Request sec key req from user and Give Permission
View your profile, View all authorized data, Search data on only authorized data using content keyword, Request dec key from AA and view response, Download the file

Figure: Data flow block diagram

4. CONCLUSIONS

This work presents a robust and scalable solution for secure data sharing in multi-owner cloud environments through fine-grained access control using attribute-based encryption. The proposed framework empowers data owners to specify detailed access policies while maintaining data confidentiality in an untrusted cloud infrastructure. The system not only facilitates secure and conditional data dissemination but also supports user revocation and policy updates without compromising efficiency.

Security analysis demonstrates that the framework is resistant to unauthorized access, collusion attacks, and data leakage, while experimental results confirm its feasibility for real-world deployment in collaborative and sensitive data-sharing domains.

In conclusion, the proposed approach offers a flexible, secure, and efficient model for multi-owner data sharing in the cloud, paving the way for broader adoption of secure collaborative systems in healthcare, education, enterprise, and beyond.

REFERENCES

[1] Z. Yan, X. Li, M. Wang, and A. V. Vasilakos, “Flexible data access control based on trust and reputation in cloud computing,” *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 485-498, 2017.

[2] B. Lang, J. Wang, and Y. Liu, “Achieving flexible and self-contained data protection in cloud computing,” *IEEE Access*, vol. 5, pp. 1510- 1523, 2017.

[3] Q. Zhang, L. T. Yang, and Z. Chen, “Privacy preserving deep computation model on cloud for big data feature learning,” *IEEE Transactions on Computers*, vol. 65, no. 5, pp. 1351-1362, 2016.

[4] H. Cui, X. Yi, and S. Nepal, “Achieving scalable access control over encrypted data for edge computing networks,” *IEEE Access*, vol. 6, pp. 30049–30059, 2018.

[5] K. Xue, W. Chen, W. Li, J. Hong, and P. Hong, “Combining data owner-side and cloud-side access control for encrypted cloud storage,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2062–2074, 2018.

[6] C. Delerablée, “Identity-based broadcast encryption with constant size ciphertexts and private keys,” *Proc. International Conf. on the Theory and Application of Cryptology and Information Security (ASIACRYPT‘2007)*, pp. 200-215, 2007.

[7] N. Paladi, C. Gehrmann, and A. Michalas, “Providing user security guarantees in public infrastructure clouds,” *IEEE Transactions on Cloud Computing*, vol. 5, no. 3, pp. 405-419, 2017.

[8] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute based encryption,” *Proc. IEEE Symposium on Security and Privacy (SP‘07)*, pp. 321-334, 2007.

[9] L. Liu, Y. Zhang, and X. Li, “KeyD: secure key-deduplication with identity-based broadcast encryption,” *IEEE Transactions on Cloud Computing*, 2018, https://ieeexplore.ieee.org/document/8458136.

[10] Q. Huang, Y. Yang, and J. Fu, “Secure data group sharing and dissemination with attribute and time conditions in Public Clouds,” *IEEE Transactions on Services Computing*, 2018, https://ieeexplore.ieee.org/document/8395392.

[11] Box, “Understanding collaborator permission levels”, https://community. box.com/t5/Collaborate-By-Inviting-Others/Understanding-Collaborator-Permission-Levels/ta-p/144.

[12] Microsoft OneDrive, “Document collaboration and co-authoring”, https://support.office.com/en-us/article/document-collaborationand-co-authoring-ee1509b4-1f6e-401e-b04a-782d26f564a4.

[13] H. He, R. Li, X. Dong, and Z. Zhang, “Secure, efficient and finegrained data access control mechanism for P2P storage cloud,” *IEEE Transactions on Cloud Computing*, vol. 2, no. 4, pp. 471-484, 2014.

[14] Z. Qin, H. Xiong, S. Wu, and J. Batamuliza, “A survey of proxy reencryption for secure data sharing in cloud computing,” *IEEE Transactions on Services Computing*, 2018, https://ieeexplore.ieee.org/document/7448446.

[15] J. Son, D. Kim, R. Hussain, and H. Oh, “Conditional proxy reencryption for secure big data group sharing in cloud environment,” *Proc.* of *2014 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 541–546, 2014.