Journal of Cardiovascular Disease Research

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

SECURE AND CONDITIONAL DATA DISSEMINATION FOR MULTI-OWNER SYSTEMS IN THE CLOUD

[1] Dr.Ayesha Banu,[2] MEKALA SUNILKUMAR,[3] RAYYAN MOHAMMAD

[1]Associate Professor,[23]Students

Department of CSD

Vaagdevi College of Engineering, Warangal, Telangana

ABSTRACT

With the rapid adoption of cloud computing, secure data sharing among multiple users and owners has become a critical aspect of data management, particularly when privacy and conditional access control are required. This paper presents a framework for secure group data sharing and conditional dissemination in a multi-owner cloud environment, addressing key challenges such as data privacy, access control, and ownership integrity. The proposed model leverages advanced encryption techniques and access control policies to ensure that only authorized users can access and disseminate shared data based on predefined conditions. By implementing a multi-owner setting, the framework allows multiple data owners to collaboratively manage and control data access, without compromising the security or privacy of individual contributions. Additionally, a conditional dissemination mechanism ensures data is only distributed to eligible recipients based on dynamically adjustable criteria, further strengthening data security in sensitive cloud applications. Through performance evaluation and security analysis, this approach demonstrates efficiency, scalability, and resilience against unauthorized access, providing a robust solution for secure multi-owner data sharing in cloud computing.

1.1INTRODUCTION

Here's an introduction for "Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing":

Cloud computing has transformed data storage and sharing by providing scalable, cost-effective solutions for both individuals and organizations. As data sharing becomes increasingly prevalent in cloud environments, ensuring data security, privacy, and proper access control remains a complex challenge—particularly in scenarios involving multiple data owners and group sharing. Traditional cloud storage models are often centralized and do not fully address the need for fine-grained access control in multi-owner settings, where each owner may have distinct access permissions and dissemination conditions for shared data. Without adequate security measures, cloud-stored data is vulnerable to unauthorized access, data breaches, and potential privacy violations.

This paper introduces a secure framework for group data sharing and conditional dissemination in a multi-owner cloud environment. The proposed solution focuses on enabling multiple data owners to jointly manage and control data access, allowing each owner to establish individual access policies for their data while maintaining security and privacy standards across the cloud platform. This

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

approach utilizes encryption and access control mechanisms to enforce conditional dissemination, ensuring that data is only accessible to authorized users who meet specific criteria defined by the owners. In contrast to conventional models, this framework supports dynamic access control and ownership verification, providing each owner with assurance over the security and integrity of their contributions.

The need for secure, conditional data dissemination is especially relevant in fields such as healthcare, finance, and collaborative research, where sensitive information must be shared selectively among authorized parties while protecting individual privacy and ownership rights. By addressing both technical and policy-related challenges, this research seeks to enhance secure cloud data sharing practices, providing a scalable and efficient solution for multi-owner environments. Through this approach, we aim to establish a more secure and collaborative data sharing model, leveraging cloud technology to foster information exchange without compromising the principles of confidentiality, integrity, and availability.

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

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

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.

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

2.1 ARCHITECTURE OF THE PROPOSED SYSTEM:

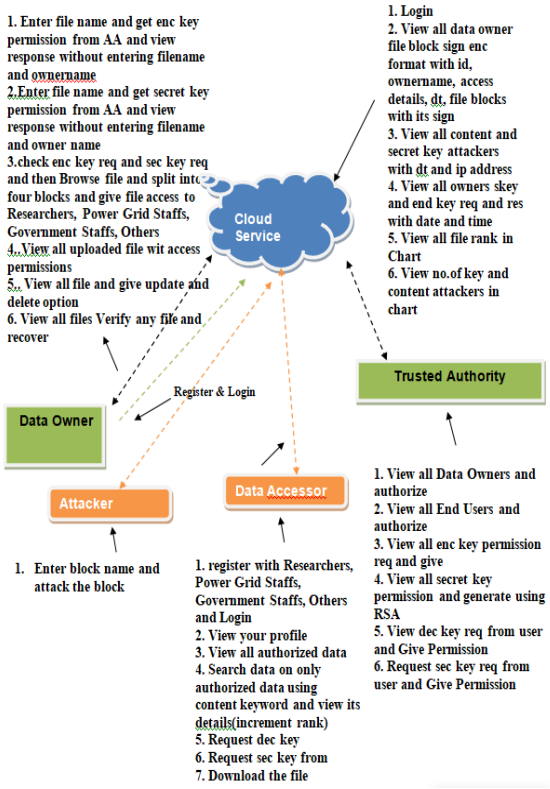

Figure: Architecture diagram

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

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

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.

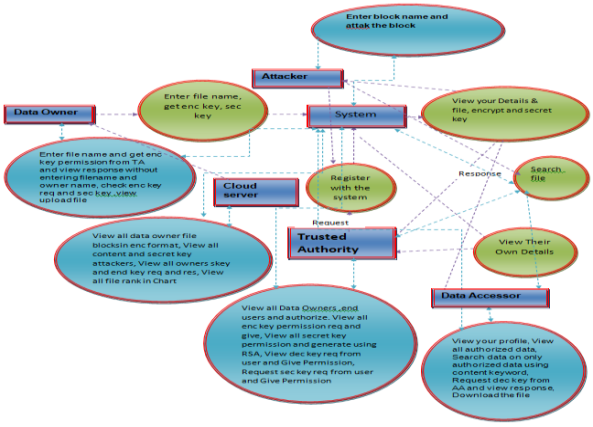

Figure: Data flow block diagram

4 SYSTEM TESTING

4.1 TESTING METHODOLOGIES

The following are the Testing Methodologies:

• Unit Testing.
• Integration Testing.
• User Acceptance Testing.
• Output Testing.
• Validation Testing.

The following are the types of Integration Testing:

4.2 Top down Integration

This method is an incremental approach to the construction of program structure. Modules are integrated by moving downward through the control hierarchy, beginning with the main program module. The module subordinates to the main program module are incorporated into the structure in either a depth first or breadth first manner.

In this method, the software is tested from main module and individual stubs are replaced when the test proceeds downwards.

4.3 Bottom-up Integration

This method begins the construction and testing with the modules at the lowest level in the program structure. Since the modules are integrated from the bottom up, processing required for modules subordinate to a given level is always available and the need for stubs is eliminated. The bottom up integration strategy may be implemented with the following steps:

• The low-level modules are combined into clusters into clusters that perform a specific Software sub-function.

• A driver (i.e.) the control program for testing is written to coordinate test case input and output.

• The cluster is tested.

• Drivers are removed and clusters are combined moving upward in the program structure

The bottom up approaches tests each module individually and then each module is module is integrated with a main module and tested for functionality.

4.4 User Acceptance Testing

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

User Acceptance of a system is the key factor for the success of any system. The system under consideration is tested for user acceptance by constantly keeping in touch with the prospective system users at the time of developing and making changes wherever required. The system developed provides a friendly user interface that can easily be understood even by a person who is new to the system.

4.5 Output Testing

After performing the validation testing, the next step is output testing of the proposed system, since no system could be useful if it does not produce the required output in the specified format. Asking the users about the format required by them tests the outputs generated or displayed by the system under consideration. Hence the output format is considered in 2 ways – one is on screen and another in printed format.

4.6 Validation Checking

Validation checks are performed on the following fields.

Text Field:

The text field can contain only the number of characters lesser than or equal to its size. The text fields are alphanumeric in some tables and alphabetic in other tables. Incorrect entry always flashes and error message.

5 CONCLUSIONS

The growing reliance on cloud computing for data storage and collaboration has made secure multi-owner data sharing a critical area of research. This study has presented a framework that addresses essential challenges in multi-owner environments, including data privacy, conditional dissemination, and access control. By utilizing advanced encryption techniques and customizable access policies, this framework allows multiple owners to share data securely while maintaining control over dissemination conditions. This approach enables fine-grained access management, ensuring that data is only accessible to users who meet the criteria defined by the owners.

Through analysis and practical examples, this framework demonstrates its effectiveness in balancing security and usability, providing a viable solution for fields that require sensitive data management, such as healthcare, finance, and collaborative research. The inclusion of conditional dissemination further strengthens data security, supporting selective sharing that adapts to dynamic user requirements and ownership rights.

Despite the advancements achieved, challenges remain in ensuring scalability and minimizing computational costs in large-scale cloud applications. Future research could explore optimization methods, such as integrating machine learning for dynamic policy adjustment, to enhance the framework's adaptability and efficiency. Ultimately, this work contributes to a more secure and collaborative cloud computing environment, enabling efficient, conditional, and secure data sharing among multiple owners while upholding privacy and data integrity.

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

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

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.

[16] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption

ISSN:0975 -3583,0976-2833 VOL 11, ISSUE 11, 2020

for cloud storage," *IEEE Access*, vol. 5, pp. 13336 – 13345, 2017.