SECURE DATA GROUP SHARING AND CONDITIONAL DISSEMINATION WITH MULTI-OWNER IN CLOUD COMPUTING

[1]Dr.S.V Sonekar,[2]Swati Raut,[3]Niket Farfad,[4]Ankit Bhandarkar
[1]Professor,[2]Assistant Professor,[34]Research Scholar
Department Of CSE
J D College of Engineering & Management, Nagpur

ABSTRACT

With the rapid development of cloud services, huge volume of data is shared via cloud computing. Although cryptographic techniques have been utilized to provide data confidentiality in cloud computing, current mechanisms cannot enforce privacy concerns over cipher text associated with multiple owners, which makes co-owners unable to appropriately control whether data disseminators can actually disseminate their data. In this paper, we propose a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing, in which data owner can share private data with a group of users via the cloud in a secure way, and data disseminator can disseminate the data to a new group of users if the attributes satisfy the access policies in the cipher text. We further present a multiparty access control mechanism over the disseminated cipher text, in which the data co-owners can append new access policies to the cipher text due to their privacy preferences. Moreover, three policy aggregation strategies, including full permit, owner priority and majority permit, are provided to solve the privacy conflicts problem caused by different access policies. The security analysis and experimental results show our scheme is practical and efficient for secure data sharing with multi-owner in cloud computing.

1.1INTRODUCTION

The popularity of cloud computing is obtained from the benefits of rich storage resources and instant access [1]. It aggregates the resources of computing infrastructure, and then provides on-demand services over the Internet. Many famous companies are now providing public cloud services, such as Amazon, Google, Alibaba.

These services allow individual users and enterprise users to upload data (e.g. photos, videos and documents) to cloud service provider (CSP), for the purpose of accessing the data at any time anywhere and sharing the data with others. In order to protect the privacy of users, most cloud services achieve access control by maintaining access control list (ACL). In this way, users can choose to either publish their data to anyone or grant access rights merely to their approved people. However, the security risks have

raised concerns in people, due to the data is stored in plaintext form by the CSP. Once the data is posted to the CSP, it is out of the data owner's control [2]. Unfortunately, the CSP is usually a semi-trusted server which honestly follows the designated protocol, but might collect the users' data and even use them for benefits without users' consents. On the other hand, the data has tremendous usages by various data consumers to learn the behavior of users [3]. These security issues motivate the effective solutions to protect data confidentiality. It is essential to adopt

access control mechanisms to achieve secure data sharing in cloud computing [4] . Currently, cryptographic mechanisms such as attribute-based encryption (ABE) [5], identity- based broadcast encryption (IBBE) [6], and remote attestation [7] have been exploited to settle these security and privacy problems. ABE is one of the new cryptographic mechanisms used in cloud computing to reach secure and fine-grained data sharing [8]. It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among decryption keys and cipher texts. As long as the attribute set satisfies the access policy that the cipher text can be decrypted. IBBE is another prevalent technique employed in cloud computing [9],[10], in which users could share their encrypted data with multiple receivers at one time and the public key of the receiver can be regarded as any valid strings, such as unique identity and email. In fact, IBBE can be seen as a special case of ABE for policies consisting of an OR gate. Compared to ABE in which the secret key and cipher text are both correspond to a set of attributes, IBBE incurs low-cost key management and small constant policy sizes, which is more suitable for securely broadcasting data to specific receivers in cloud computing.

Hence, by using identities, data owner can share data with a group of users in a secure and efficient manner, which motivates more users to share their private data via cloud. Actually, these encryption techniques can prevent unauthorized entities (e.g. semi-trusted CSP and malicious users) from accessing the data, but it may not consider data dissemination in cloud computing. In the cloud collaboration scenario such as Box [11] and One Drive [12], the data disseminators (e.g. editor and collaborator) may share the documents with new users even those outside the organization. However, once the data is encrypted with the above techniques, data disseminators are not able to modify the cipher text uploaded by data owners [13]. Proxy re-encryption (PRE) scheme [14] is employed to achieve secure data dissemination in cloud computing by delegating a re-encryption key associated with the new receivers to the CSP. However, the data disseminator can disseminate all of the data owner's data to others with this re-encryption key, which may not meet the practical requirement since the data owner may only permit the data disseminator to disseminate a particular document.

A refined concept referred to as on additional PRE (CPRE) [15], [16] could address this issue, in which data owner can enforce re-encryption control over the initial cipher texts and only the cipher texts satisfying specific condition can be re-encrypted with corresponding re encryption key. However, traditional CPRE schemes only support simple keyword conditions, so they cannot match complex situations in cloud computing well. In order to support expressive conditions rather than keywords, attribute-based CPRE is proposed [17], which deploys an access policy in the cipher text. The re-encryption key is associated with a set of attributes, thus the proxy can re encrypt the cipher text only when the re-encryption key matches the access policy. In this way, data owner can customize fine-grained dissemination condition for the shared data.

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:

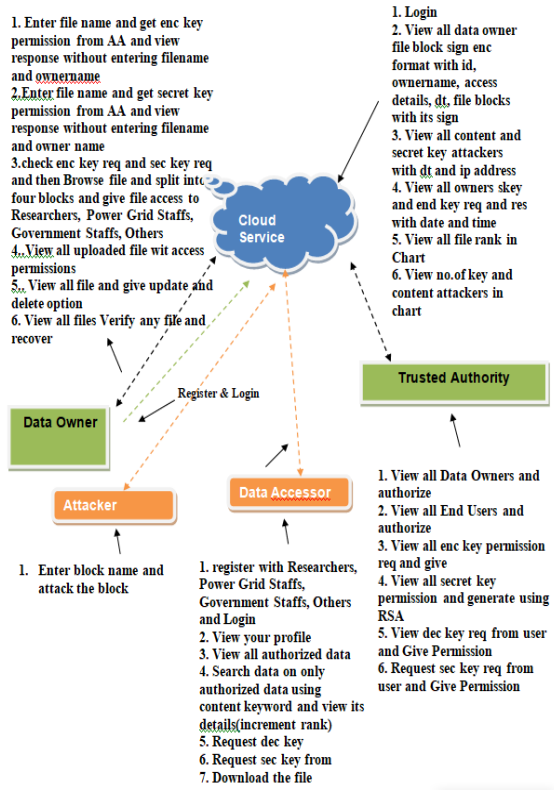

Figure: Architecture diagram

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.

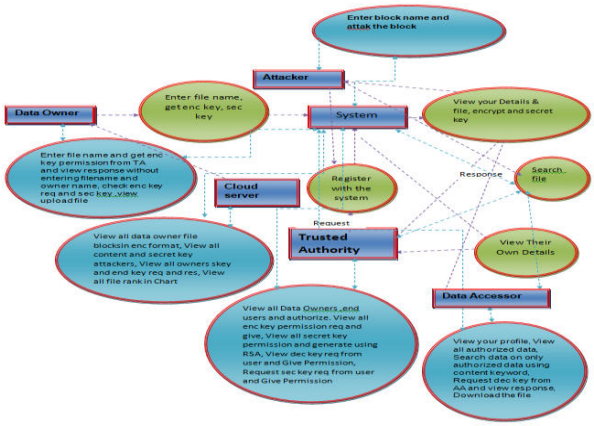

Figure: Data flow block diagram

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

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 data security and privacy is a concern for users in cloud computing. In particular, how to enforce privacy concerns of multiple owners and protect the data confidentiality becomes a challenge. In this paper, we present a secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. In our scheme, the data owner could encrypt her or his private data and share it with a group of data accessor at one time in a convenient way based on IBBE technique. Meanwhile, the data owner can specify fine-grained access policy to the cipher text based on attribute-based CPRE, thus the cipher text can only be re encrypted by data disseminator whose attributes satisfy the access policy in the cipher text. We further present a multiparty access control mechanism over the cipher text, which allows the data co-owners to append their access policies to the cipher text. Besides, we provide three policy aggregation strategies including full permit, owner priority and majority permit

to solve the problem of privacy conflicts. In the future, we will enhance our scheme by supporting keyword search over the cipher text [47, 48].

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.

[16] L. Jiang, and D. Guo "Dynamic encrypted data sharing scheme based on conditional proxy broadcast re-encryption for cloud storage," *IEEE Access*, vol. 5, pp. 13336 – 13345, 2017.