Secure Data Group Sharing and Conditional Dissemination with Multi-Owner in Cloud Computing

[1]K. Venkateswarlu [2V.] Manasa

[1] Assistant Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

[2] PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.

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 ciphertext associated with multiple owners, which makes co-owners unable to appropriately control whether data disseminators can actually disseminate their data. 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 ciphertext.

Keywords: Data Sharing, Conditional Proxy Re-Encryption, Attribute-Based Encryption, Privacy Conflict.

I. INTRODUCTION

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 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.
- 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 behaviour of users. 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. Currently, cryptographic mechanisms such as attribute-based encryption (ABE), identity-based broadcast encryption (IBBE), and remote attestation 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
- . It features a mechanism that enables an access control over encrypted data using access policies and ascribed attributes among decryption keys and ciphertexts.As long as the attribute set satisfies the access policy that the ciphertext can be decrypted.

II. BACKGROUND WORK

A series of unaddressed security and privacy issues emerge as important research topics in cloud computing. By utilizing the IBBE technique, Huang et al, Paranaiba et al. and Liu et al. proposed several private data sharing schemes in cloud computing.In these schemes, data owner outsources encrypted data to the CSP by defining a

list of receivers, thus only the intended users in the list can get the decryption key and further decrypt the private data.

ABE is another promising one-to-many cryptographic technique to realize data encryption and fine-grained access control in cloud computing [3, 4]. Specially, ciphertext-policy ABE (CP-ABE) is suited for access control in real world applications due to its expressiveness in describing the access policy of ciphertext [5]. Guo et al. [6] proposed a privacypreserving data dissemination scheme in mobile social networks based on CP-ABE. Teng et al. [7] proposed an efficient access control scheme with hierarchical CP-ABE to achieve privacy preservation in cloud storage systems.

Secure data dissemination is another important security requirement for data storage in cloud computing. The identity-based PRE [8] is a basic encryption algorithm to reach secure data dissemination in cloud computing, with which the data disseminators could send their reencryption keys to the semi-trusted proxy to transform data owner's ciphertext for new users [9].Yang et al. [10] proposed an attribute-based CPRE scheme by deploying an access policy in a ciphertext generated by public-key encryption. The reencryption key is generated by the secret key associated with a set of attributes, which allows the proxy to reencrypt the ciphertext only when these attributes satisfy the access policy. Wang et al. [11] proposed a preauthentication approach for sharing data in cloud, which achieves receiver's attribute authentication before the reencryption operation.

The multiparty privacy control among co-owners is indispensable in cloud computing. Thomas et al. [2] showed how Facebook's privacy model can be adopted to achieve multiparty privacy.Based on this multiparty privacy control model, Xu et al. [1] designed a mechanism to enable each user in a photo to participate in the decision of access control conditions of the photo. However, the above schemes may have privacy conflicts problem, which do not consider how users would actually achieve compromise [12].

To resolve the privacy conflicts among multiparty (negotiating users), Such et al. [13] proposed the first computational mechanism. The core idea is to estimate item sensitivity, relative importance and willingness for each conflicting negotiating users, and let the one who has less stringent privacy requirement compromise. Hu et al. [14] proposed a systematicapproach to enable privacy-preserving data sharing with multi-owner. This scheme introduces three strategies based on a voting mechanism to resolve the multiparty privacy conflicts. Unfortunately, this scheme only focuses on co-owner's access control over plaintext data, and ignores the data confidentiality towards semi-trusted CSP and malicious users.

III. PROPOSED WORK

We further present a multiparty access control mechanism over the disseminated ciphertext, in which the data co-owners can append new access policies to the ciphertext 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.

System Model:The system model consists of the following entities, as shown in Fig. 1

Data Owner: Decide the access policy and encrypt the data with CP-ABE. The encrypted data will be uploaded to the Cloud Servers. *Data Owners*are assumed to be honest in the system.

Data Requester/Receiver:Send 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 Server:are responsible for storing a massive volume of data. They cannot be trusted by Data Owners. Hence, it is necessary for Data Owners to define the access policy to ensure the data confidentiality.Cloud Servers are assumed not to collude with Data requester/receivers.

Trusted Authority: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 Data Owner. It is considered as fully trusted.

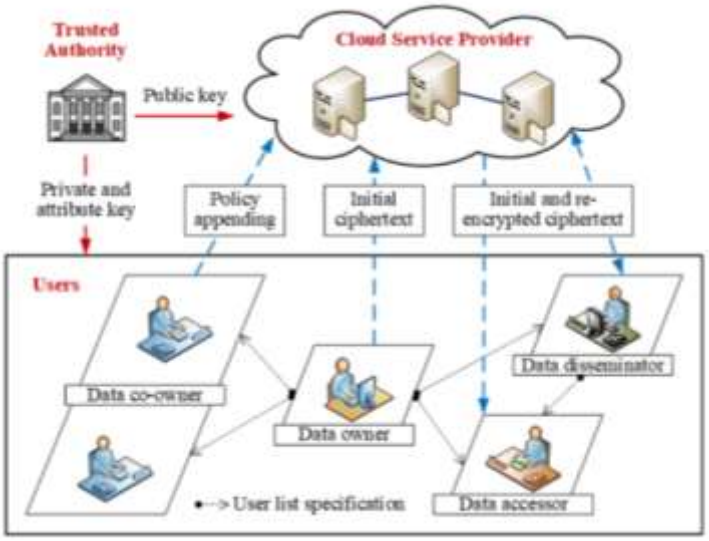

Fig. 1: System Overview

The contributions of our scheme are as follows:

(1) We achieve fine-grained conditional dissemination over the ciphertext in cloud computing with attribute based CPRE. The ciphertext 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 ciphertext due to their privacypreferences. Hence, the ciphertext can be re-encrypted by the data disseminator only if the attributes satisfy enough access policies.

(2) We provide 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 ciphertext 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.

(3) We prove the correctness of our scheme, and conduct experiments to evaluate the performance at each phase to indicate the effectiveness of our scheme.

IV. RESULTS AND DISCUSSION

To evaluate the efficiency of our proposed schemes,we conduct various experiments and chooses the Advanced Encryption Standard (AES) as the symmetric encryption scheme. The experimental results are the mean of 100 trials.

Fig. 2 shows the computation time of data encryption versus |U| under a fixed access policy with 5 attributes and 3 co-owners.

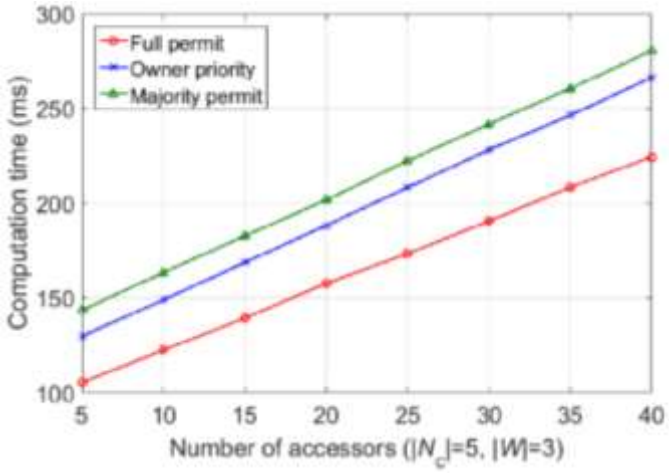

Fig. 2: Computation time versus users in encryption phase.

Fig. 3 shows the computation cost of reencryption in each strategy versus the number of attributes. In the owner priority strategy.

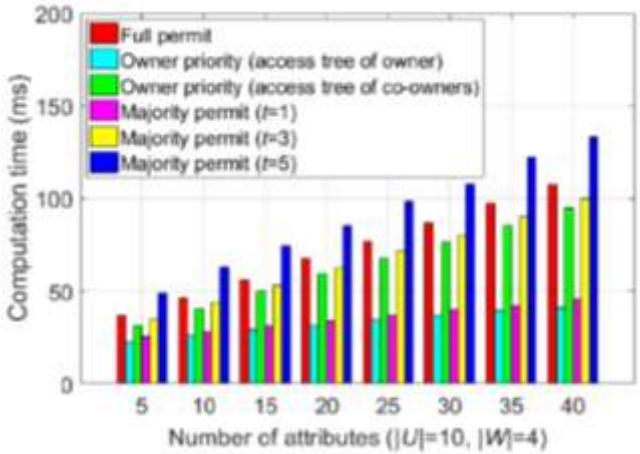

Fig. 3: Computation cost versus attributesin re-encryption phase.

Fig. 4 describes the computation time on accessor side when decrypting ciphertext versus the number of accessors. The computation time of decrypting a reencrypted ciphertext is much higher than the time of decrypting an initial ciphertext.

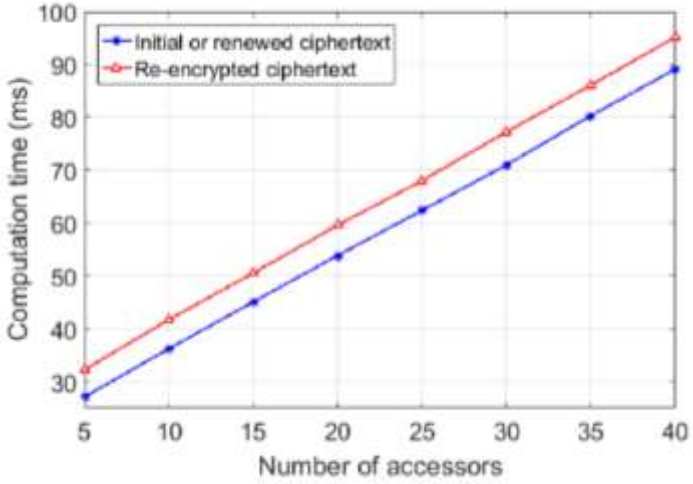

Fig. 4: Computation cost versus accessorsin decryption phase.

V. CONCLUSION

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 accessors at one time in a convenient way based on IBBE technique. Meanwhile, the data owner can specify fine-grained access policy to the ciphertext based on attribute-based CPRE, thus the ciphertext can only be re-encrypted by data disseminator whose attributes satisfy the access policy in the ciphertext.

We further present a multiparty access control mechanism over the ciphertext, which allows the data co-owners to append their access policies to the ciphertext. Besides, we provide three policy aggregation strategies including full permit, owner priority and majority permit to solve the problem of privacy conflicts. The security analysis and the performance evaluation show that the proposed scheme is secure and efficient.

REFERENCES

1. K. Xu, Y. Guo, L. Guo, Y. Fang, and X. Li, "My privacy my decision: control of photo sharing on online social networks," IEEE Trans. on Dependable and Secure Computing, vol. 14, no. 2, pp. 199-210, 2017.
2. K. Thomas, C. Grier, and D. M. Nicol, "UnFriendly: multi-party privacy risks in social networks," Proc. International Symposium on Privacy Enhancing Technologies Symp. (PETS '2010), pp. 236-252, 2010.
3. A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc. 24th Ann. International Conf. on Theory and Applications of Cryptographic Techniques (EUROCRYPT '05), pp. 457-473, 2005.
4. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. on Computer and Communications Security (CCS '06), pp.8998, 2006.
5. S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attributebased data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.
6. L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving socialassisted mobile content dissemination scheme in DTNs," Proc. 32nd IEEE International Conf. on Computer Communications (INFOCOM '2013), pp. 2301-2309, 2013.
7. W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attributebased access control with constant-size ciphertext in cloud computing," IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp. 617-627, 2017.
8. M. Green and G. Ateniese, "Identity-based proxy re-encryption," Proc. 5th International Conf. on Applied Cryptography and Network Security (ACNS '07), pp. 288-306, 2007.
9. Y. Zhou, H. Deng, Q. Wu, B. Qin, J. Liu, and Y. Ding, "Identity-based proxy re-encryption version 2: Making mobile access easy in cloud," Future Generation Computer Systems, vol. 62, pp. 128-139, 2016.
10. Y. Yang, H. Lu, J. Weng, Y. Zhang, and K. Sakurai, "Fine-grained conditional proxy re-encryption and application," Proc. International Conf. on Provable Security (ProvSec '2014), pp. 206-222, 2014.
11. K. Wang, J. Yu, X. Liu and S. Guo, "A pre-authentication approach to proxy re-encryption in big data context," IEEE Transactions on Big Data, 2018, https://ieeexplore.ieee.org/document/7921569.
12. H. Hu, G. J. Ahn, and J. Jorgensen, "Detecting and resolving privacy conflicts for collaborative data sharing in online social networks," Proc. 27th Ann. Computer Security Applications Conf. (ACSAC '11), pp. 103-112, 2011.
13. J. M. Such and N. Criado, "Resolving multi-party privacy conflicts in social media," IEEE Trans. on Knowledge and Data Engine, vol. 28, no. 7, pp. 1851-1863, 2016.

14. H. Hu, G. Ahn, and J. Jorgensen, "Multiparty access control for online social networks: Model and mechanisms," IEEE Trans. on Knowledge and Data Engine, vol. 25, no. 7, pp. 1614-1627, 2013.

Author's Profile:

K. Venkateswarlu has received his MCA degree from Saraswathi Valu College of Engineering, Vellore affiliated to *Anna University in 2010* and M.Tech degree in *Computer Science* from PBR Vits, Kavali affiliated to *JNTU, Ananthapur* in 2014 respectively. He is dedicated to teaching field from the last 6years. He has guided 25 P.G students. At present he is working as an*AssistantProfessor* in Narayana Engineering College, *Gudur*, AndhraPradesh, India.

V. Manasa has Received her B.Sc Degree in*Computer Science* fromESS Degree College Venkatagiri, affiliated to *VikramaSimhapuri University,Nellore* in 2017 and pursuing PG Degree in *Master of Computer Applications*(M.C.A)from NarayanaEngineering College,Gudur affiliated to JNTU Anantapur, Andhra Pradesh, India.