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

E. Ajith Kumar[1], S. Balaji[2], S. Maheswari[3], V. Senthil Kumar[4]

[1, 2, 3] Student, department of Computer science and Engineering, KSRCE, TamilNadu, India.
Email:balajisivaraman99@gmail.com[2]

[4] Professor, Department of Computer Science and Engineering, KSRCE, TamilNadu, India.

Abstract - With the rapid development of cloud services, huge volume of data is shared via cloud 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 computing. Although cryptographic techniques have been utilized to provide data 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.

Keywords - Include at least 5 Keyword or phrases related to domain.

I INTRODUCTION

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 behaviour 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 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 conditional 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 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 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. Besides the requirement of conditional data dissemination, multiparty access control problem for data sharing in cloud computing such as cloud collaboration and cloud-based social networks comes along [18, 19], which means the special authorization requirements from multiple associated users can be accommodated together to control the shared data. Consider an example where a co-authoring document or a co-photo in cloud computing with three users, Alice, Bob, and Carol. If Alice who is the data owner uploads this co-authoring document or cophoto to the CSP and tags both Bob and Carol as the crowners. Alice can restrict this data to be disseminated to a certain group of users, while the co-owners Bob and Carol may have different privacy concerns about this data. It is a massive and serious privacy problem if applying the preference of only one party, which may cause such data to be shared with undesired receivers. However, merging privacy preferences of data owner and multiple co-owners is not an easy task, due to privacy conflict is inevitable in multiparty authorization enforcement [20, 21]. Privacy conflict happens when the crowners have opposite privacy policies, and it results in data being impossibly accessed with anyone [22]. To deal with this dilemma, multiparty access control mechanisms'. (e.g. voting scheme) are further provided. However, all of them are based on plaintext data. In this paper, we propose an identity-based secure data group sharing and conditional dissemination scheme with multi-owner in cloud computing. To mitigate the problems mentioned above, we introduce 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: (1) We achieve 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. (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 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. (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. This paper is structured as follows. We review related work in Section 2 and introduce the preliminaries in Section 3. We provide the system model and policy aggregation strategies in Section 4, and describe the proposed scheme in Section 5. We present the system analysis and experimental results in Section 6 and Section 7 respectively. Finally, we conclude this paper in Section.

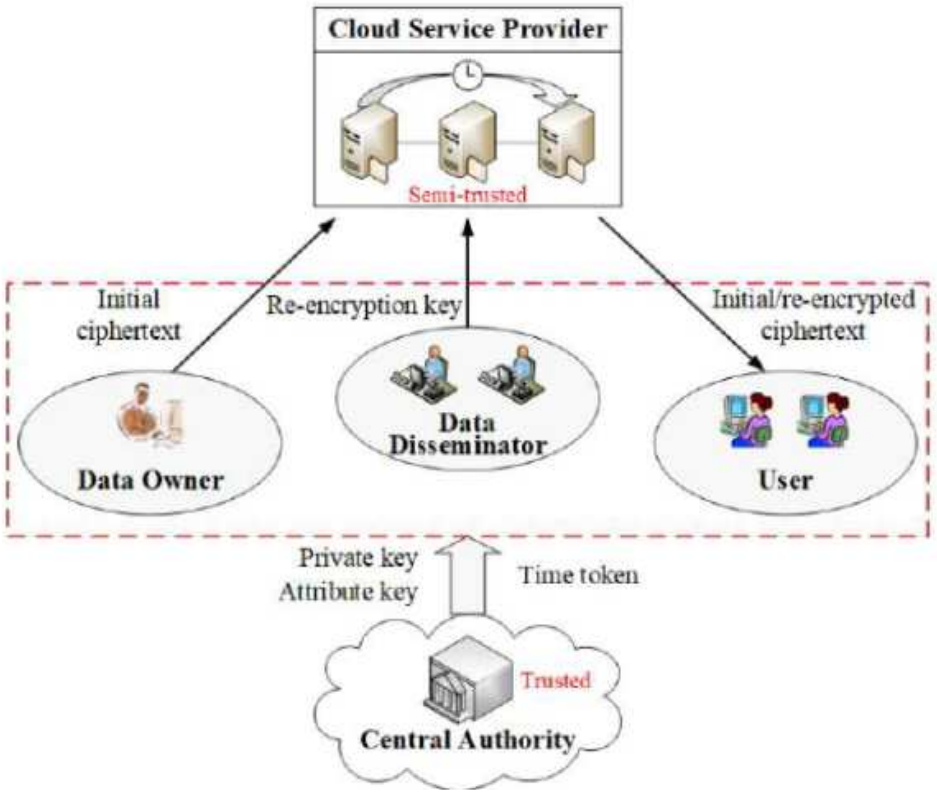
II RELATED WORKS

In this project, we propose a secure data group sharing and dissemination scheme with attribute and time conditions in public cloud. The main contributions of our scheme are as follows: (1) We employ IBBE technique to achieve secure data group sharing in public cloud, which allows data owner to outsource encrypted data to semi-trusted cloud and share it with a group of receivers at one time. It is more convenient that email and username could be used as public keys for users. (2) We design an access policy embedding releasing time and take the advantages of attribute-based CPRE, to achieve fine-grained and timed-release data group dissemination. The CSP can re-encrypt initial cipher texts for data disseminator after the designate time if his attributes associated with the re-encryption key satisfy the access policy in the cipher texts. (3) We analyze the security of our proposed scheme, and conduct a detailed theoretical and experimental analysis. The results show that our scheme makes tradeoffs between computational overhead and expressive dissemination conditions, and performs significantly better in data group sharing and dissemination in public cloud.

III PROPOSED SYSTEM

We propose an identity- based data group sharing and dissemination scheme in public cloud, in which data owner could broadcast encrypted data to a group of receivers at one time by specifying these receivers' identities in a convenient and secure way. In order to achieve secure and flexible data group dissemination, we adopt attribute-based and timed-release conditional proxy re-encryption to guarantee that only data disseminators whose attributes satisfy the access policy of encrypted data can disseminate it to other groups after the releasing time by delegating a re-encryption key to cloud server. The re-encryption conditions are associated with attributes and releasing time, which allows data owner to enforce fine-grained and timed-release access control over disseminated cipher texts. The theoretical analysis and experimental results show our proposed scheme makes a trade off between computational overhead and expressive dissemination conditions.

System Architecture



IV SYSTEM METHODOLOGY

Benefits brought by the proposed scheme are evident especially in public cloud storage systems. Our scheme is suitable for the scenarios where data can be shared and disseminated with time conditions in a group of users. Let's consider an application scenario. Suppose that company A uses the cloud storage service, in which the proposed scheme is being utilized. Some employees in company A usually share some important time-sensitive data with different intended workmates, and these workmates can access the data stored in the cloud with sufficient authorization, but gain their disclosure privilege at different time points. Specially speaking, since the business plan of this company may contain some business secrets, executive officer shares this plan with directors to discuss and improve the business plan at an early time, while others cannot access this plan. Then, only executive director can gain disclosure privilege to disseminate the business plan in the cloud to managers of some relevant departments at a later time point, when they take responsibility for the plan execution. At last, all the directors can disseminate the business plan in the cloud to make other employees in the company to have the access privilege after specific secrecy period.

V RESULT

We propose a personality based information bunch sharing and spread plan out in the open cloud, where information proprietor could communicate encoded information to a gathering of collectors one after another by indicating these beneficiaries' characters in an advantageous and secure manner. So as to accomplish secure and adaptable information bunch spread, we receive property based and planned discharge restrictive intermediary re-encryption to ensure that lone information disseminators whose characteristics fulfill the entrance arrangement of scrambled information can scatter it to different gatherings after the discharging time by assigning a re-encryption key to cloud server.

VI CONCLUSION

The IoT promises to deliver a step change in individuals‟ quality of life and enterprises‟ productivity. Through a widely distributed, locally intelligent network of smart devices, the IoT has the potential to enable extensions and enhancements to fundamental services in transportation, logistics, security, utilities, education, healthcare and other areas, while providing a new ecosystem for application development. A concerted effort is required to move the industry beyond the early stages of market development towards maturity, driven by common understanding of the distinct nature of the

opportunity. This market has distinct characteristics in the areas of service distribution, business and charging models, capabilities required to deliver IoT services, and the differing demands these services will place on mobile networks. With The Cloud Computing, we can access our data anytime anywhere. In this paper, we are implementing a tool which will be of no high cost but It we will give better security, Its called Revocable storage identity based encryption, which will do both the things simultaneously which are identity revocation and cipher text update, which will prevent user from accessing the shared data which is previously shared, as well as subsequently shared data's-IBE is better than others in the security in terms of efficiency and functionality, and RSIBE is more reliable. We also added the Fragment storage for this system. We can also save the Each Fragment on different Servers but that will be included in Future Scope.

REFERENCES

[1] L. Xu, C. Jiang, N. He, Z. Han, and A. Benslimane, "Trust-based col- laborative privacy management in online social networks," IEEE Transactions on Information Forensics and Security, vol. 14, no. 1, pp. 48- 60, 2019.
[2] C. Gentry and B. Waters, "Adaptive security in broadcast encryption systems (with short ciphertexts)," Proc. 28th Ann. International Conf. on Advances in Cryptology: the Theory and Applications of Cryptographic (EUROCRYPT '09), pp. 171-188, 2009.
[3] Q. Huang, W. Yue, Y. He, and Y. Yang, "Secure identity-based data sharing and profile matching for mobile healthcare social networks in cloud computing," IEEE Access, vol. 6, pp. 36584–36594, 2018.
[4] S. Patranabis, Y. Shrivastava, and D. Mukhopadhyay, "Provably secure key-aggregate cryptosystems with broadcast aggregate keys for online data sharing on the cloud," IEEE Transactions on Computers, vol. 66, no. 5, pp. 891–904, 2017.
[5] 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.
[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based en- cryption for fine-grained access control of encrypted data," Proc. 13th ACM Conf. on Computer and Communications Security (CCS '06), pp.89- 98, 2006.
[7] S. Wang, K. Liang, J. K. Liu, J. Chen, J. Yu, and W. Xie, "Attribute- based data sharing scheme revisited in cloud computing," IEEE Transactions on Information Forensics and Security, vol. 11, no. 8, pp. 1661–1673, 2016.
[8] L. Guo, C. Zhang, H. Yue, and Y. Fang, "A privacy-preserving social- assisted mobile content dissemination scheme in DTNs," Proc. 32nd IEEE International Conf. on Computer Communications (INFOCOM '2013), pp. 2301-2309, 2013.
[9] W. Teng, G. Yang, Y. Xiang, T. Zhang, and D. Wang, "Attribute- based access control with constant-size ciphertext in cloud compu- ting," IEEE Transactions on Cloud Computing, vol. 5, no. 4, pp. 617-627, 2017.