Group User Revocation Policy in Cloud Computing

[1]Shubhangini Bhorde, [2]Prof. Kailash Tambe
Department of Computer Engineering, Zeal College of Engineering and Research, Pune.

Abstract: - *With the development of cloud computing, outsourcing information to cloud server attracts scores of attentions. To ensure the safety and attain flexibly fine-grained file access management, attribute primarily based secret writing (ABE) was planned and utilized in cloud storage system. However, user revocation is that the primary issue in ABE schemes. During this article, we offer a ciphertext-policy attribute primarily based secret writing (CP-ABE) theme with economical user revocation for cloud storage system. The problem of user revocation will be resolved with efficiency by introducing the conception of user cluster. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notably, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our scheme under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is relatively low and can be constant. Our scheme is suitable for resource constrained devices.*

Keywords: Cloud computing, attribute-based encryptions outsource decryption, user revocation, collusion attack.

I. INTRODUCTION

In this project, we provide a cipher text-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the concept of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access structure. To reduce the computation cost, we outsource high computation load to cloud service providers without leaking file content and secret keys.

With the increasing of sensitive data outsourced to cloud, cloud storage services are facing many challenges including data security and data access control. To solve those problems, attribute-based encryption (ABE) schemes [2-4] have been applied to cloud storage services. Sahai and Waters [1] first proposed ABE scheme named fuzzy identity-based encryption which is derived from identity-based encryption (IBE) [4]. As a new proposed cryptographic primitive, ABE scheme not only has the advantage of IBE scheme, but also provides the characteristic of "on e-to-m an y" encryption . Presently, ABE mainly includes two categories called ciphertext -policy ABE (CPABE) and key-policy ABE (KP-ABE) [4]. In CP-ABE, ciphertexts are associated with access policies and user's private keys are associated with attribute sets. A user can decrypt the ciphertext if his attributes satisfy the access policy embedded in the ciphertext. It is contrary in KPABE. CP-ABE is more suitable for the outsourcing data architecture than KP-ABE because the access policy is defined by the data owners. In this article, we present an efficient CP-ABE with user revocation ability.

II. RELATED WORK

Boldyreva et al [6] presented an IBE scheme with efficient revocation, which is also suitable for KP-ABE. Nevertheless, it is not clear whether their scheme is suitable for CP-ABE.

Although ABE has shown its merits, user revocation and attribute revocation are the primary concerns. The revocation problem is even more difficult peculiarly in CP-ABE schemes, because each attribute is shared by many users. This means that revocation for any attribute or any single user may affect the other users in the system. Recently, some work [6] has been proposed to solve this problem in efficient ways. Boldyreva et al. [6] presented an IBE scheme with efficient revocation, which is also suitable for KP-ABE. Nevertheless, it is not clear whether their scheme is suitable for CP-ABE. Yu et al. [7] provided an attribute based data sharing scheme with attribute revocation ability. This scheme was proved to be secure against chosen plaintext attacks (CPA) based on DBDH assumption. However, the length of ciphertext and user's private key are proportional to the number of attributes in the attribute universe. In the key generation, encryption and decryption stages, computation involves all attributes in the attribute universe. Yu [7] provided an attribute based data sharing scheme with attribute revocation ability. This scheme was proved to be secure against chosen plaintext attacks (CPA) based on DBDH assumption. However, the length of cipher text and user's private key are proportional to the number of attributes in the attribute universe. Yu [7] designed a KP-ABE scheme with fine-grained data access control. This scheme requires that the root node in the access tree is an AND gate and one child is a leaf node which is associated with the dummy attribute.

In the existing scheme, when a user leaves from a user group, the group manager only revokes his group secret key which implies that the user's private key associated with attributes is still valid. If someone in the group intentionally exposes the group secret key to the revoked user, he can perform decryption operations through his private key. To clarify this attack, a concrete instance is given. Assume that the data is encrypted under the policy "professor AND cryptography" and the group public key. Suppose that there are two users: user1and user2 whose private keys are associated with the attribute sets {male, professor, cryptography} and {male, student, cryptography} respectively. If both of them are in the group and hold the group secret key, then user1can decrypt the data but user2can't. When user1is revoked from the group, he can't decrypt alone because he does not have the updated

group secret key. However, the attributes of user1are not revoked and user2 has the updated group secret key. So, user1can collude with user2 to perform the decryption operation. Furthermore, security model and proof were not provided in their scheme.

III. PROPOSED SYSTEM

In this system, we have a tendency to target coming up with a CP-ABE theme with economical user revocation for cloud storage system. We have a tendency to aim to model collusion attack performed by revoked users cooperating with existing users. What is more, we have a tendency to construct associate economical user revocation CP-ABE theme through raising the present theme and prove our theme is comptroller secure below the selective model. to unravel existing security issue, we have a tendency to insert a certificate into every user's non-public key.. In this way, each user's group secret key is different from others and bound together with his private key associated with attributes. To reduce users' computation burdens, we introduce two cloud service providers named encryption-cloud service provider (E-CSP) and decryption-cloud service provider (D-CSP). The duty of E-CSP is to perform outsourced encryption operation and D-CSP is to perform outsourced decryption operation. In the encryption phase, the operation associated with the dummy attribute is performed locally while the operation associated with the sub-tree is outsourced to E-CSP. Security issues are main obstacles for wide application of cloud computing. To achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used. However, user revocation is the primary issue in ABE schemes. We need efficient user revocation for cloud storage system. At the same time heavy computation cost should not spoil the application performance. The system should with stand collusion attack performed by revoked users cooperating with existing users. The system should be suitable for resource constrained devices also.

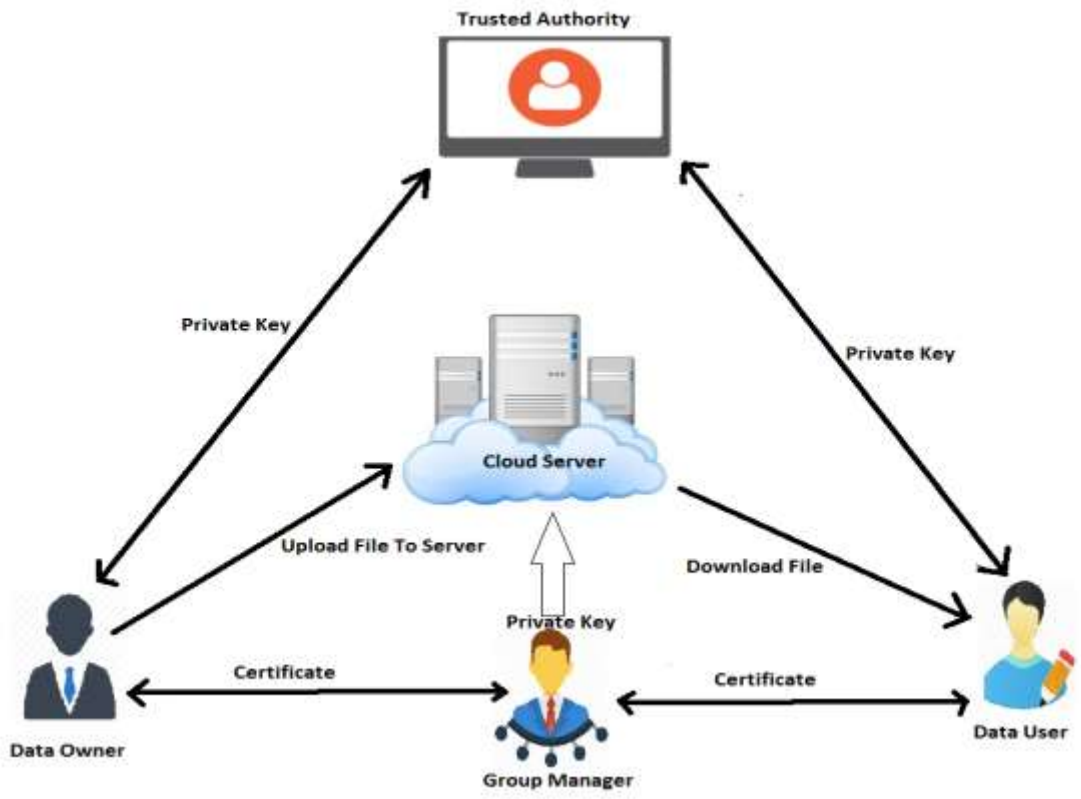

Figure 1: Architecture Diagram

Advantages of Proposed System:

- Reduce the heavy computation burden on users.
- We outsource most of computation load to E-CSP and D-CSP and leave very small computation cost to local devices.
- Our scheme is efficient for resource constrained devices such as mobile phones.
- Our scheme can be used in cloud storage system that requires the abilities of user revocation and fine-grained access control.

IV. CONCLUSION

We provided a formal definition and security model-ABE with user revocation. We also constructed a concrete CP-ABE which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to reduce the user's computation burdens. Through applying the technique of outsource, computation cost for local devices is much lower and relatively fixed. The results of

our experiment show that our scheme is efficient for resource constrained devices.

REFERENCES

[1]Jiguo Li, Wei Yao, Yichen Zhang, Huiling Qian and Jinguang Han ,"Flexible and Fine-Grained Attribute-Based Data Storage in Cloud Computing" IEEE Transactions on Services Computing (Volume: 10, Issue: 5, Sept.-Oct. 1 2017)

[2] A. Sahai and B. Waters, "Fu zzy Identity-Based Encryption,"EUROCRYPT '05, LNCS, vol. 3494, pp. 457-473, 2005.

[3] J.Bethencourt, A. Sahai and B.Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symposium on Security and Privacy,IEEE Transactions on Services Computing (Volume:PP , Issue: 99),22 January 2016pp. 321-334, May 2007, doi: 10.1109/ SP.2007.11.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc.13th ACM Conference on Computer and Communications Security (CCS'06), pp. 89-98, 2006, doi:10.1145/ 1180405.1180418.

[5] D. Boneh and M.K. Franklin, "Id en tity-Based Encryption fromthe Weil Pairing," SIAM Journal of Computing, vol. 32, no. 3,pp. 586-615, 2003.

[6] A. Boldyreva, V. Goyal, and V. Kumar , "Identity-Based Encryption with Efficient Revocation," Proc. 15th ACM conference on Computer and communications security (CCS ' 08), pp. 417-426, 2008.

[7] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. 5th ACM Symposium on Information, Computer and Communications Security (ASIACCS ' 10), pp.261-270, 2010.

[8] M. Yang, F. Liu, J. Han, and Z. Wang, "An Efficient Attribute based Encryption Scheme with Revocation for Outsourced Data Sharing Control," Proc. 2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control, pp.516-520, 2011.