Minimizing Communication Overhead Computation Cost for Dynamic Users in The Cloud

B. Rajender, Manda. Sridhar

Christu Jyoti Institute of Technology & Science,Colombonagar, Yeshwanthapur, Jangaon, Andhra Pradesh, India

Abstract: Storing data on remote cloud storage makes the maintenance affordable by data owners. The reliability and trustworthiness of these remote storage locations is the main concern for data owners and cloud service providers. When Multiple data owners are involved, the aspects of membership and data sharing need to be addressed. In this paper, we propose a secure multi owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others.

1. Introduction

CLOUD computing is recognized as an alternative to traditional information technology [1] due to its intrinsic resource-sharing and low-maintenance characteristics. In cloud computing, the cloud service providers (CSPs), such as Amazon, are able to deliver various services to cloud users with the help of powerful datacenters. By migrating the local data management systems into cloud servers, users can enjoy high-quality services and save significant investments on their local infrastructures. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud [2]. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging issues. First, identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the guarantee of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the other hand, unconditional identity privacy may incur the abuse of privacy. Second, it is highly recommended that any member in a group should be able to fully enjoy the data storing and sharing services provided by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner [3], where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications.

2. Related Work

In [4], the authors specified a secure data sharing model, Mona, for dynamic groups in a remote storage. In Mona, a data owner can share data with others in the group without announcing their identity. Moreover, Mona supports effective user repudiation and new user registration. More specially, efficient user repudiation can be attained by a public revocation list without ideating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their presence.

In [5], Kallahalla et al. proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. By dividing files into filegroups and encrypting each filegroup with a unique file-block key, the data owner can share the filegroups with others through delivering the corresponding lockbox key, where the lockbox key is used to encrypt the file-block keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the file-block key needs to be updated and distributed again for a user revocation. Lu et al. [6] proposed a secure provenance scheme, which is built upon group signatures and ciphertext-policy attribute-based encryption techniques. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the

registration: a group signature key and an attribute key. Thus, any user is able to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their attribute keys.

3. Problem Statement

3.1: Existing System

To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task.

Existing System (Conti.)

In the existing System data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users.

However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users, respectively.

Disadvantages

1. Only the group manager can store and modify data in the cloud.
2. The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

3.2: Proposed System

1. We propose a secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the untrusted cloud.
2. Our proposed scheme is able to support dynamic groups efficiently. Specifically, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners.
3. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource.
4. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

Advantages

1. Any user in the group can store and share data files with others by the cloud.
2. The encryption complexity and size of ciphertexts are independent with the number of revoked users in the system.
3. User revocation can be achieved without updating the private keys of the remaining users.

4. System Architecture

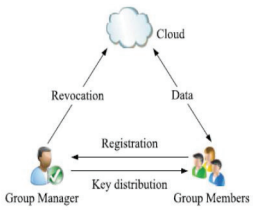


Fig. 1. System model.

5. Modules

1. Cloud Module

In this module, we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to we assume that the cloud server is honest but curious.

2. Group Manager Module

Group manager takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner

3. Group Member Module

1. Group members are a set of registered users that will
2. Store their private data into the cloud server and
3. Share them with others in the group.

4. File Security Module

1. Encrypting the data file.
2. File stored in the cloud can be deleted by either the group manager or the data owner.

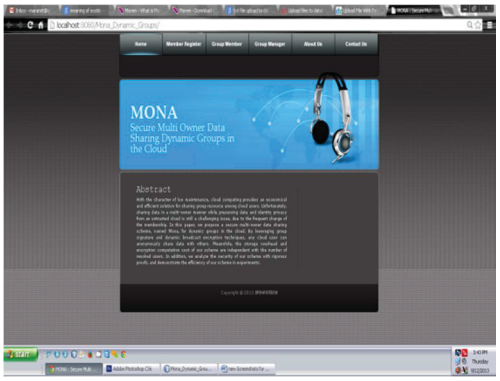
5. Group Signature Module

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. Besides, the designated group manager can reveal the identity of the signature's originator when a dispute occurs, which is denoted as traceability.

6. User Revocation Module

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users.

6. Experimental Results



7. Future Enhancement

8. Conclusion:

In this paper, we developed a secure Multi owner Data sharing Group key protocol for an untrusted cloud. In this model, a new user can store data on the cloud storage without communicating with all the data owners. The group key manager grants the key on request to the new data owners directly. The new user revocation and registration is made simple by allowing the user to communicate with the group key manager through the revocation policy. The storage overhead and the encryption computation cost are varied.

9. References

1. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.
2. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
3. S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.
4. Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, Ieee transactions on parallel and distributed systems, vol. 24, no. 6, june 2013.
5. M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.
6. R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.