A Novel Approach for Secure Data Sharing in Multi-Owner groups in Cloud

Jaldi Rakesh[1], Janapati Venkata Krishna[2]

[1]*pursuing M.Tech (CSE), Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India*

[2]*working as Associate Professor & HOD (CSE Department) in Holy Mary Institute of Technology and Science, Keesara, Affiliated to JNTU- Hyderabad, A.P, India*

Abstract: **The cloud computing becoming a major platform for storing the group resources of any group and distributed those group resources among group member. But cloud is not the trusted partner for storing a secure data on it.In this paper we proposing a model by which we can store group resources to cloud and can share those resources to group member. In a group it's not compulsory that the group member will fixed. A group member can join or can leave any time that group so we implemented proposed system for dynamic group with secure group signature and dynamic broad casting techniques. In this system we implemented group member revocation method also for adding or removing the group member.**

Keywords: Cloud computing, group resources, group signature, revocation.

1. INTRODUCTION

Cloud computing is identifying as an alternative way to traditional information technology due to essential resource-sharing and low- maintenance feature. 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 databases into cloud servers, users can enjoy efficient services and save significant investment on their local infrastructures.

One of the elementary services offered by the cloud providers is data storage. Let us consider real time application. A company allows its staff in the same group to store and share files in the cloud, the staffs can completely quit from the troublesome local data storage and maintenance. However, it's a significant risk to the confidentiality of those stored files. Especially the cloud servers managed by cloud providers are not fully trusted by the users, the storing data files may contains confidential and sensitive data. To prevent data privacy the fundamental solution is to encrypt the date files and upload the encrypted files into cloud. Unfortunately designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task because of following issues.

First, identity privacy is one of the most significant barrier for the deployment of cloud computing. Without guarantee of identity privacy, users may be not willing to join in the cloud be easily disclosed to cloud providers and hackers. On the other way, unconditional identity
Privacy may suffer the abuse of privacy. For example a misbehaved employee can cheat others in the company by sharing false files without being traceable. So, traceability which enables the group manager to reveal the real identity of a user is also highly advantages.

Second, it is highly recommended that each and every member of group should be enjoy the data storing and sharing services provided by the cloud, which is called as multi-owner manner. Compared with single owner manner here only group manager store and modify the data files in the cloud, the multiple-owner manner is very flexible in practical applications. More frequently, every user in the group is capable of not only read data, but also modifies his/her part of data in the entire data file shared by the company.

Last, groups are normally dynamic in nature, e.g., new employee participation and current employee deletion in a company. The changes of members make secure data sharing is highly difficult. On one hand, the unknown system challenges newly added users to learn the content of data files stored before their participation, because it is not possible for new added users to contact with unknown data owners, and obtain the associated decryption keys. On the other hand, an effective membership revocation mechanism without updating the secret keys of the remaining users is also desired to minimize the difficulty of key management.

Various security schemes to data sharing on untrusted servers have been proposed. In this point of view, a data owner stores the encrypted data files in untrusted storage and distributed the corresponding decryption keys only to authorized users. So, unauthorized cloud users as well as storage servers cannot learn the content of the data files.

However, the complexities of user adding and removing (revocation) in these schemes are linearly increasing with the number of data owners and the number of revoke users, respectively. By form a group with a single attribute. Proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique [8], which allows any employee in a group to share the data with others. However, the issue of member revocation is not addressed in

their scheme. Unfortunately, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to save and share data in the cloud.

Our benfications.To solve the problems represented in the above, we propose a secure multi-owner data sharing scheme for dynamic groups in the cloud. The main advantage of this paper includes.

1. We propose a secure dynamic multi-owner data sharing scheme. It implicit that any user in the group can securely share the data with others by the untrusted cloud.
2. Our proposed scheme is having capable of supporting dynamic groups effectively. The newly granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily reached through a novel revocation without updating the secrete keys of remaining users. The size and computation is overhead of encryption is constant and independent with number of revoked users.
3. We provide secure and privacy preserving access control to users, which says that any member in the group can independently utilize the cloud resource. Moreover, the identities of data owners can be revealed by the group manager when disagreement occur
4. We provide careful security analysis, and perform considerable simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

2. RELATED WORK

Kallahalla et al introduced a cryptographic storage system that enables secured file sharing on untrusted servers, named Plutus. By dividing data files into file groups and encrypting each file group each file group with a unique file-block key, owners of the data can share the file groups with others through delivering the corresponding lockbox key, where the lockbox key is used for encrypt the file-block keys.it gets about heavy key distribution overhead for large file sharing. Additionally, the file blocks key needs to be updated and distributed the key after user revocation.

Files stored on the untrusted server contain two parts: file data and file metadata. The file metadata specifies the access control information includes a series of encrypted key blocks, each of which encrypted under the public key of authorized users. Thus the size of the file metadata is equals to number of users. The user revocation in this scheme is an intractable issue especially for large sharing, since the file metadata needs to be updatable. In their extension version, the NNL construction is used for efficient key revocation. However, when a new user joining in to the group, the private key of each user in an NNL system needs to be recomputed, it may limit the application for dynamic groups. Another involvement is that the computation overhead of encryption linearly increases with the sharing file.

Ateniesea introduced proxy re encryptions to secure distributed storage. Specifically, the data owners encrypt blocks of data with unique and symmetric content keys, which are encrypted further by using master public key. For access control, the server's uses proxy cryptography to directly re encrypts the appropriate content keys from the master public key to the granted user public key. Unfortunately, a clash attack between the untrusted server and any revoked harmful user can be launched, which enables to learn the decryption keys of all the encrypted blocks.

C. Wang presented a scalable and fine-grained data access control scheme in cloud computing based on the KP-ABE technique. Here the data owner uses a random key to encrypt the data file, where the random key encrypted further with set of attributes using KP-ABE. Then, the group manager gives an access structure and the associate secret key to authorized users, such that a user has only decrypt a cipher text if the data file attributes satisfy the access structure. To reach user revocation, the manager transfers tasks of data file re encryption and user secret key update to cloud servers. However, the single owner manner may delay the implementation of applications with the synopsis, where any member in a group should be allowed to store and share the data files with others.

X. Lin proposed a secure origin scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques. Especially, the system in their scheme is set with a single attribute. Every user get two keys after the registration: one is group signature key and an attribute key. Thus, any user have the capability to encrypt a data file using attribute-based encryption and others in the group can decrypt the encrypted data using their own attribute keys. Meanwhile, the user gives encrypted data with his/her group signature key for privacy preserving and traceability. However, user revocation will not support in their scheme.

From the above analysis, we can discover that how to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be challenging issue.

In this paper, we introduce a concept called secure data sharing in the cloud computing.it has some unique qualities Those are.

1. Any user in the group can store and share the data files with others in the cloud.
2. User revocation can be achieved by without changing the private key of remaining users.
3. A new user can directly store the encrypted data before participating.

3. SYSTEM MODEL AND DESIGN GOALS

3.1 **System Model**

We consider cloud computing architecture is a company uses cloud computing it enables their staff to store and share data files in the same group or department. The system model contains of three different entities: the cloud, a group manager

(i.e., the company manager), and a large number of group members (i.e., the staffs).

Cloud is operated by cloud service providers and provides storage services on price based. But, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. We assume that the cloud server is honest but not secure. That is, the cloud server will not intentionally delete or modify user data due to the protection of data auditing schemes but they will try to learn the content of the stored data and the identities of cloud users.

The group manager having the permission of adding the new user to group and revoke the user. The group manager is acted by the administrator of the company. Therefore, we can assume that the group manager is fully trusted by the other parties.

Group members are a group of registered users they will store their private data into the cloud server and share them with others in the group. In our example, data owners play the role of group members. Note the group membership is dynamically changed, due to the employee resignation and new employee participation and deletion in the company.

3.2 Design Goals

Here, we describe the main design goals of the proposed scheme including access controls, data confidentiality, anonymity and traceability and efficiency as follows:

Access control: The need of access control is twofold.

First, group members are having the capable of use the cloud resources for data operations. Second, untrusted users cannot access the cloud resources at any time, and removed users will be incapable of using the cloud again once they are revoked.

Data confidentiality: Data confidentiality requires that unauthorized users including the cloud are incapable, learning the content of the stored data. An important and challenging task for data confidentiality is to maintain its availability for dynamic groups. Specifically, new users must decrypt the data stored in the cloud before their participation, and revoked users are don't have capable of decrypt the data moved into the cloud after the revocation.

Anonymity and traceability: Anonymity guarantees that group members (employee) can access the cloud without revealing real identity. Although anonymity shows an effective security for user identity, it also poses a potential inside attacker risk to the system. For example, an inside attacker may be store and share a mendacious information to derive substantial benefit. Thus, to crane the inside attack, the group manager should have the ability to reveal the real identity of data owners.

Efficiency: The efficiency is described as follows: Any group member can save and share data files with others in the group in the cloud. User revocation can be done without involving the remaining users. That is, the remaining users no need to update their private keys or re encryption operations. New added users can learn all the content data files stored before his participation without contacting with the data owner.

4. PROPOSED SYSTEM:

Here we introducing a concept called group signature, to achieve secure data sharing in multi dynamic groups. Here group member able to store the data file and share that files with corresponding group members and having the capability of deleting the data files. A group member doesn't have permission to access the data files of other groups.

But here the drawback is the group member may revoked.so at that time we make them to don't access the data files. So all this permissions like adding new user to group and revoking the users is given to group managers. Here first user has to register but he doesn't have credential to login immediately, before the group member login to first time the group manager has to add that user to associated group, while adding the group the group get the group signature by using all this details the group member has to register, but here the thing is in previous the group signature store in cloud directly. But even though the cloud has that much advantages it has some drawbacks, there is no security for data, so if store the original key in cloud it can be attacked.

To resolve all these problems the group signature has to convert in to cipher text and stored in the cloud, here the group signature and data to be stored in cloud should be convert in to cipher text.

In our project the admin has the permission to create a new group. Whenever a new group is created at the time a group signature will provided, when a group member adding to group that signature has mail to that new user by using that key the user can login and perform all the operations.

And the admin can remove the group, whenever he remove the group automatically it removes all the group members.

4.1 User Revocation: The user revocation operation performed only by the group manager. The revoked user doesn't have any permission to perform operations, whenever the group manager revoked a user he will change the key and that key mail to all group members available in that particular group and that key also converted into cipher text and stored in the cloud the original key goes to group members.

4.2 User Operations: The user has to perform operations like accessing the files, deleting the files and storing the files of the group but he doesn't have permission to accessing the files of another group. While he was storing the files in the cloud the file converted in to cipher text by using a cryptgraphic technique. In this project we use plain cypher technique while performing encryption. The group manager can see all the files available in the group and he can modify or delete the any file available in the group either that file belongs to group member or group manager. Here the group member doesn't have permission to delete the file of another group member but he can delete his files.

5. CONCLUSION:

In olden technique it stores the original group signature directly in the cloud, Even though cloud provides so many services it has a drawback that is security issue, so whatever

data stored in the cloud should be converted into cipher text using any technique. In our proposed system we will not store the original key directly in the cloud, before storing that we convert that in to cipher text then store in to cloud.

REFERENCES:

[1] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[2] 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.

[3] 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.

[4] 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.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[6] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and DistributedSystems Security Symp. (NDSS), pp. 131-145, 2003.

[7] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

[8] 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.

[9] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[10] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[11] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[12] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[13] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[14] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[15] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 480-491, 1993.

[16] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud," Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[17] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-265, 1991.

AUTHOR PROFILE

Jaldi Rakesh, pursuing M.Tech (CSE) from Holy Mary Institute of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.

Janapati Venkata Krishna, Associate Professor & H O D (CSE Department), Holy Mary Institute Of Technology and Science, Keesara, Ranga Reddy Dist., Affiliated to JNTU-HYDERABAD.