ISSN No: 2309-4893
International Journal of Advanced Engineering and Global Technology
Vol-2, Issue-8, August 2014

Multi-Owner Data Sharing Using Key Policy Attribute-Based Encryption Method in the cloud

Ms. Rupali Shelke and Mr. Rakesh Rajani

Abstract: There is a Major problem in public clouds about the sharing of documents on attribute based policies, sharing data in a dynamic groups . With the help of advantage of low maintenance, cloud computing gives the effective solution for sharing group resource among cloud users. As the sharing of documents with different keys like attribute based encryption (ABE), and/or proxy re-encryption (PRE) approach has some weaknesses so, it cannot handle efficiently adding/revoking users and attributes of identification. Unfortunately, there is still a challenging issue, to share a data in multi-owner manner and preserve data and their confidentiality. In this paper, we propose Multi-Owner Data Sharing scheme, using attribute based encryption method. By using maximum advantage groupsignature , signed receipts and dynamic broadcast encryption techniques, any can share the data on the cloud. As the result we achieve the secure data sharing in the cloud we expect to combine the group signature and dynamic broadcast encryption techniques.

***Index Terms*— Cloud computing, shared data, access control, dynamic groups.**

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its in-trinsic resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage in large volume with high security. Such cloud providers cannot be trusted to protect the confidentiality if the data. In fact, data privacy and protection issues have been major issues for many organizations utilizing these services. Data often encode sensitive information and should be protected as mandated by various organizational policies and legal protocols. Encryption is a commonly adopted approach to protect the privacy of the data. Encryption alone however is not efficient as organizations often have to enforce fine access control on the data. Such control is often depends on the parameters of users, referred to as identity attributes, such as the type of users in the industrial organization, projects on where users are working and so further.

An important requirement is to support fine-grained access control, based on policy spicier using identity attributes, over encrypted data. However, it also posses significant risk to the confidentiality of those stored. files. To preserve data confidentiality, a basic solution is to encrypt and decrypt data files, and then upload the encrypted data into the cloud. Unexpectedly, 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 Second, it is 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.

By Comparing with the single-owner case, where only the group manager can store and edit data in the cloud, the multiple-owner case is more flexible in practical applications any one can change and edit the data. As compared with the single-owner case, Third, member revocation and signed receipt e.g., new member participation and current member revocation in a group. The changes of membership make private data sharing extremely difficult, it is impossible for new granted users to contact with similar data owners, and obtain the corresponding decryption keys. On the second hand, an efficient membership re-vocation mechanism without updating of the secret keys of the remaining users minimize the complexity and increases the efficiency of key management , signed receipt is collected after every member revocation in the group it minimizes the multiple copies of encrypted file and also reduces cost.

II. ISSUES AND CHALLENGES

- Identity privacy is one of the most significant obstacles for the wide deployment of cloud computing. Without the information of identity privacy, users may be unknown to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. On the another hand, unconditional identification privacy may incur the misuse of privacy
- 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 case. Compared with the single-owner case, where only the group manager can store and edit data in the cloud, the multiple-owner manner is more easily accessible in practical applications.
- Groups are normally dynamic in practical approach, e.g., new staff entered and current employee revocation in a company. The changes of membership make privacy data sharing extremely difficult.

Our contributions. To solve the challenges presented above, we propose a secure multi-owner data sharing scheme for dynamic groups in the cloud. The contributions of this paper include the following:

- A secure multi-owner data sharing scheme implies that any user in the group can securely share data with others by the untrusted cloud.
- It able to support dynamic groups efficiently and effectively. Normally, new granted users can directly decrypt data files uploaded before their participation without contacting with data owners. User revocation can be easily accepted through a novel revocation list without modifying the secret keys of the rest of the users. The size and computation overhead of encryption are constant and not dependent on the number of revoked users.
- Provide secure and privacy-preserving access control to users, which fixed any member in a group to similar utilize the cloud resource. Now, the real identification of data owners can be opposed by the group manager when problem occur.
- Provide high security analysis, and perform extensive simulations to illustrate the efficiency of our scheme in terms of storage and computation overhead.

III. RELATED WORKS

In [4], proposed a cryptographic storage system that enables secure file sharing on untrusted servers, named Plutus. First divid files into file groups and encrypting each file group with a unique secrete key, the data owner can share the file groups with others through delivering the secrete key. It brings the overhead for about a heavy key distribution for file sharing. Additionally, the key needs to be updated and distributed again for a user revocation. In [5], files stored on the any untrusted server include two parts: file metadata that is data about data and file data. The size of the file metadata is depends on the number of authorized users.

The file data gives the access control information including a series of encrypted key, each of which is encrypted under the public key of authorized users. The user revocation is an big issue especially for large-volume sharing, since the file needs to be updated data about data. Another issue is that, the computation overhead of encryption linearly increases with the sharing-scale. [6] To forced security in distributed storage with privacy. Specifically the data owner encrypts blocks of data with unique and symmetric content keys. When a new user joins the group, the private key of each user in the system needs to be calculated again, which may limit the application for dynamic groups. Another concern is that the issues of encryption linearly increases with the data sharing scale. The data owner encrypts content with unique and symmetric keys, which are further encrypted with a master public key. Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which does not able them to learn the decryption keys of all the encrypted blocks. In [3], Yu et al. presented a scalable and fine-grained data accessed control scheme in cloud computing based on the KPABE technique. The data owner select any random key to encrypt a file, where the random key is next encrypted with a set of attributes using KP-ABE. Then, the group manager gives permission for accessing structure and the corresponding secret key to authorized users, such that a user can able to decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager changes tasks of data file re encryption and user secret key edit to cloud servers.

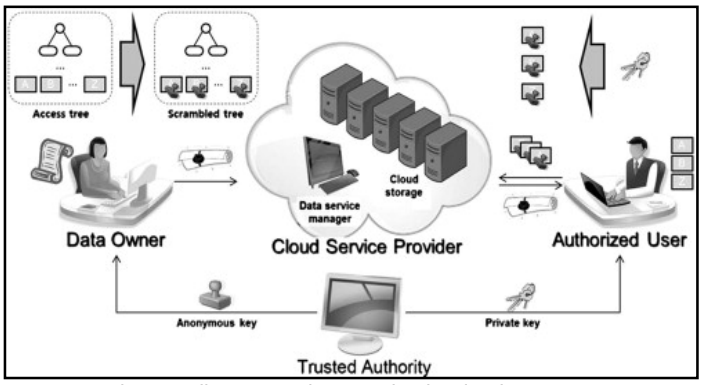

Fig 1. Attribute-Based Encryption in Cloud Storage

This paper addresses this challenging open issue by, on one hand, defining and enforcing access policies based on data attributes, and, on the other hand, allowing the data owner to delegate most of the computation tasks involved in fine-grained data access control to entrusted cloud servers without disclosing the underlying data contents. We achieve this goal by exploiting and uniquely combining techniques of attribute-based encryption (ABE), proxy re-encryption, and lazy re-encryption. Our proposed scheme also has salient properties of user access privilege confidentiality and user secret key accountability. Extensive analysis shows that our proposed scheme is highly efficient and provably secures under existing security models.

However, the single owner manner may hide the implementation of applications with the case, where any member in a group should be allowed to store and share data files with others. Lu et al. [7] proposed a secure provisional scheme, which is built upon group signatures and cipher text-policy attribute-based encryption techniques are used. Particularly, the system in their scheme is set with a single attribute. Each user obtains two keys after the registration process: 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. Meanwhile, the user signs encrypted data with her group signature key for privacy preserving and traceability. However, user revocation does not support in their data scheme. From the above result, we can observe thatHow to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an untrusted cloud remains to be a challenging issue. The proposed scheme uses a protocol for secure data sharing in cloud computing.Compared with the existing works the new protocol offers:

- The user in the group can share and store data files with others by the cloud.
- The complexity and size taken for encryption is independent with the number of revoked users in the system.
- User revocation can be achieved without updating the private keys of the remaining users and signed receipts will be collected after any revocation that reduces duplication of encrypted copies.

ISSN No: 2309-4893
International Journal of Advanced Engineering and Global Technology
Vol-2, Issue-8, August 2014

IV. PROPOSED SCHEME

A. System Model

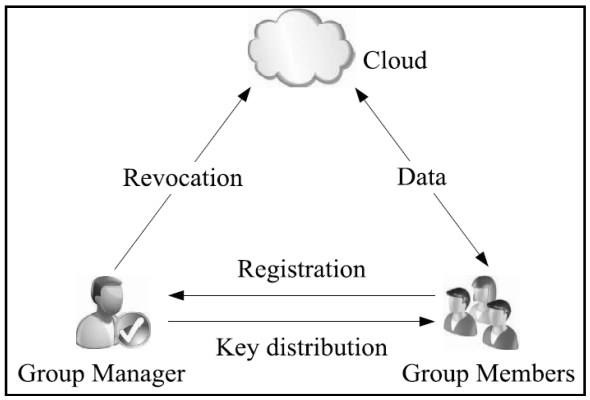

Fig. 2. System model

The system model consists 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) as Illustrated in Fig. 1. Cloud is provides high priced storage services. However, the cloud is not wholly trusted by users since the CSPs are very likely to be outside of the cloud users' trusted domain. Similar to [3], [7], we assume that the cloud server is honest but curious. That is, the cloud server will not automatically delete or modify user data due to the protection of data auditing schemes [8], [9], but will try to learn the content of the stored data and the identities of cloud users.

B. Design goals

In this section, we describe the main design goals of the proposed scheme including access control, data confidentiality, similarity and traceability, and efficiency as follows:

Access control: The requirement of access control is twofold. First, group members are use cloud resource for data operations. Second, without authorization users cannot access the cloud resource at any time, and revoked users will not capable of using the cloud again once they are revoked.

Data confidentiality: confidentiality -- and data integrity and availability as well -- are protections against malicious software (malware) spyware, spam and phishing attacks.. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. New users should decrypt the data stored in the cloud before their participation, and revoked users is unable to decrypt the data moved into the cloud after the revocation.

Anonymity and Traceability: Anonymity guarantees that group members can access the cloud without revealing the real identity it enables effective protection for user identity

It poses a potential inside attack risk to the system. To tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners.

Efficiency: The efficiency is defined as follows. Any group member can store, modify and share data files with others in the group by the cloud . User revocation can be achieved without interfering the remaining users and signed receipts will be collected after secure content sharing. the remaining users do not need to update

Data sharing : To achieve privacy preserved data sharing for dynamic groups in the cloud , the scheme combines the group signature, signed receipt and dynamic broadcast encryption techniques. Specially, the group signature and signed receipt scheme enables users to anonymously use the cloud resources, and the dynamic broadcasting encryption technique allows data owners to securely share and modify their data files with others including new joining users.

C. System Architecture

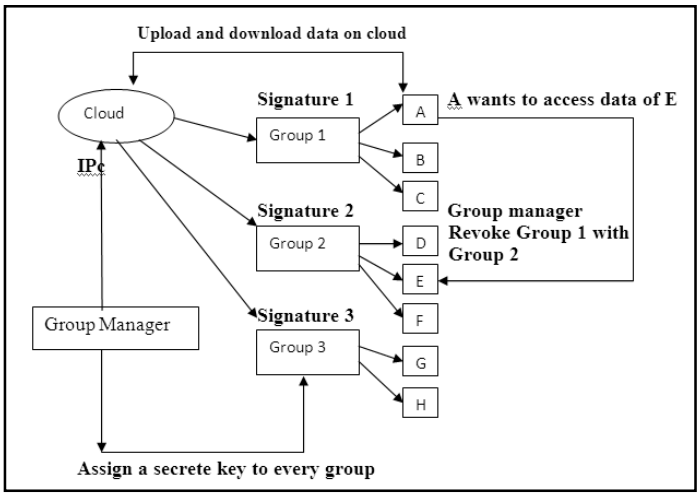

Fig 3. System Architecture

Cloud is operated by CSPs and provides priced abundant storage services. 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. That is, the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but will try to learn the content of the stored data and the identities of cloud users. Group manager takes charge of system parameters generation, user registration, user revocation, and revealing the real identity of a dispute data owner. In the given example, the group manager is acted by the administrator of the company. Therefore, we assume that the group manager is fully trusted by the other parties. Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. In our example, the staffs play the role of group members. Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

D. Mathematical Model

- User Registration

For the registration of user i with identity IDi, the group manager randomly selects a number $x_i \in Z^*_q$ and computes Ai; Bi as the following equation:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1. \end{cases}$$

Then, the group manager adds (A_i, x_i, ID_i) into the group user list, which will be used in the traceability phase.After the registration, user i obtains a private key (x_i, A_i, B_i), which will be used for group signature generation and file decryption.

- User Revocation

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. The revocation list is characterized by a series of time stamps (t1 < t2 <,tr). Let ID group denote the group identity. The tuple (A_i, x_i, t_i)represents that user i with the partial private key (Ai; xi) is revoked at time ti. P1; P2; :::; Pr and Zr are calculated by the group manager with the private secret as follows:

$$\begin{cases} P_1 = \dfrac{1}{\gamma + x_1} \cdot P \in G_1 \\ P_2 = \dfrac{1}{(\gamma + x_1)(\gamma + x_2)} \cdot P \in G_1 \\ \vdots \\ P_r = \dfrac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)} \cdot P \in G_1 \\ Z_r = Z^{\dfrac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)}} \in G_2. \end{cases}$$

V. RESULTS AND DISCUSSION

The proposed scheme of storage into cloud server is demonstrated using the private cloud setup with open stack. The SQL server 2005 and visual studio 2008 is used for building the ASPX pages that are used in demonstration of the proposed work. Microsoft Visual Studio 2008 helps individual developers accelerate solution development. Give breakthrough user experiences for all the users. It effectively building solutions for the Web, Windows, the Microsoft Office system, and latest Android Mobiles.

Visual Studio is a complete set of development tools for building ASP.NET Web applications, XML Web Services, desktop applications, and mobile applications. Visual Basic, Visual C#, and Visual C++ all use the same integrated development environment, which enables tool sharing and eases the creation of changed laguage solutions. In addition, these changed languages use the functionality of the .NET Framework, which provides access to key technologies that simplify the development of ASP Web applications and XML Web Services.

Regardless of which platform is being targeted, Visual Studio 2008 delivers the productivity, performance, and stability required to help developers remain focused on the real business challenges, along with a broad ecosystem that helps ensure they can always find the partners, information, and other community members to help them deliver great software. Also included is SQL Server 2005 Compact new Edition, SQL Server 2005 Express Edition and MSDN Express documentation.

The following are the visual studio 8 run-time member functions that are involved in the proposed system.

Math Functions – math functions are used to implement RSA algorithms which is used to encrypt the data fields (attributes) in the data base.

Conversion Functions – conversion functions are to implement KP- ABE , which ensures dynamic policy changes.

• Type Conversion Functions
• String Functions
• Math Functions
• CType Function

VI. CONCLUSION

Although it will design a secure data sharing and modifying scheme, For dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, It supports efficient user revocation and new user joining in the group. More specially, efficient user revocation can be achieved through a public revocation list without updating and editing the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extreme analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency of the system.

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] 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
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, “Sirius: Securing Remote Untrusted Storage,” Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.
[6] G. Ateniese, K. Fu, M. Green, and S. Hohenberger,“Improvedproxy re-encryption schemes with applications to secure distributed storage,” in Proc. of NDSS, 2005, pp. 29-43.
[7] 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.
[8] B. Wang, B. Li, and H. Li, “Knox: Privacy-Preserving Auditing forShared Data with Large Groups in the Cloud,” Proc. 10th Int’l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012
[9] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,” Proc. IEEE INFOCOM, pp. 525-533, 2010.