Protected Policy Based Anti-Conflict Data Allocation Scheme for Dynamic Groups in the Cloud

Rahul barfa[1], Sunil nimawat[2]
Department of Science And Technology Engineering
[1,2] PG Scholar, IPS ACADEMY INDORE

Abstract- *Major problem in public clouds is how to share documents based on fine-grained attribute based access control policies, sharing data in a dynamic groups while preserving data and identity privacy from an un trusted cloud is still a challenging issue, due to the frequent change of the membership., encrypting documents with different keys using a public key cryptosystem such as attribute based encryption (ABE), and/or proxy re-encryption (PRE) approach has some weaknesses: it cannot efficiently handle adding/revoking users or identity attributes, and policy changes; it requires to keep multiple encrypted copies of the same documents; it incurs high computational costs [1]. In this paper, We are focusing on secure group communication in which if we want to assign message to specific user then only that user can read the message and reply to the message even he will be present in the group. We propose a secure multi-owner attribute authorities based data sharing scheme for dynamic groups in the cloud.*

That aim of my paper is secure data sharing in a dynamic group where the there is no fixed Attribute authorities where as multi – owner attribute authorities scheme is possible. key policy key policy attribute-based encryption (KP-ABE) method is used to select dynamic AA (Attribute authorities) . By leveraging group signature, signed receipts and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. As the result the computation cost is reduced and storage overhead and encryption computation cost of our scheme are independent with the number of revoked users so the encryption cost is also reduced [2]

Keywords- Key distribution, Cloud computing, Privacy-preserving, Access control. attribute based encryption (ABE), proxy re-encryption (PRE)

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology due to its in-trainsick resource-sharing and low-maintenance characteristics. One of the most fundamental services offered by cloud providers is data storage. We are focusing on secure group communication in which if we want to assign message to specific user then only that user can read the message and reply to the message even he will be present in the group. Such cloud providers cannot be trusted to protect the confidentiality if the data . In fact, data privacy and security issues have been major concerns for many organizations utilizing such services. Data often encode sensitive information and should be protected as mandated by various organizational policies and legal regulations.

Encryption is a commonly adopted approach to protect the confidentiality of the data. Encryption alone however is not sufficient as organizations often have to enforce fine-grained access control on the data. Such control is often based on the attributes of users, referred to as identity attributes, such as the roles of users in the organization, projects on which users are working and so forth. These systems, in general, are called attribute based systems. Therefore, an important requirement is to support fine-grained access control, based on policy spicier using identity attributes, over encrypted data [3].

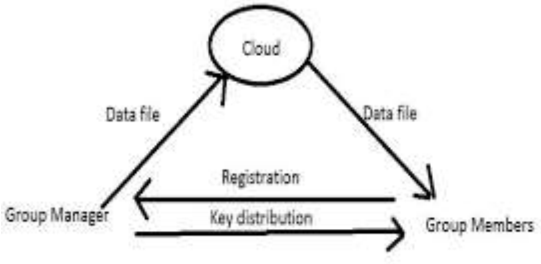

Fig:1- Overview of Group Communication

However, it also poses significant risk to the confidentiality of those stored files. 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 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. Compared with the single-owner manner [4], Third, member revocation and signed receipt e.g., new member participation and current member revocation in a group . The changes of membership make secure data sharing extremely difficult, it is impossible for new granted users to contact with anonymous data owners, and obtain the corresponding decryption keys. On the other hand, an efficient membership revocation mechanism without updating of the secret keys of the remaining users minimize the complexity 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 computation cost [5].

II. LITERATURE SURVEY

From proposed a cryptographic storage system that enables secure file sharing a n un trusted servers, named Plautus. By dividing file into file groups and encrypting each file group with a unique lock group key, the data owner can share the file groups with others through delivering the corresponding group key, where the lock group-key is used to encrypt the lock-group keys. However, it brings about a heavy key distribution overhead for large-scale file sharing. Additionally, the Lock group key needs to be updated and distributed again for a user revocation.

In un trusted server has two parts of files to be stored those : file metadata and file data. The file meta-data implies the access control information that includes a series of encrypted key blocks, each of which is encrypted under the symmetric key of authorized users. It is proportional to the number of authorized users. The user revocation in the scheme is an intractable issue especially for large-scale sharing, since the file metadata needs to be updated. In their extension version, the NNLconstruction is used for efficient key revocation. However, when a new user joins the group, the private key of each user in NNL system needs to be recomputed, which may limit the application for dynamic groups. Another concern is that, the computation overhead of encryption linearly increases with the sharing-scale [6].

To ensure security in distributed storage. Specifically the data owner encrypts blocks of content with unique and symmetric content keys. For access control, the server uses proxy cryptography to directly re-encrypt through dynamically encrypted keys the appropriate content key(s) from the AA,s dynamically derived symmetric key. Unfortunately, a collusion attack between the un trusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks[7].

In, Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. The data owner uses a random key to encrypt a file, where the random key is further encrypted with a set of attributes using KP-ABE. Then the AA's for the group assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a cipher text if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegates tasks of data file re-encryption and user secret key update to cloud servers. The single-owner manner may hinder the implementation of applications with the scenario, where any member in a group should bellowed to store and share data files with others[8].

It proposed a secure scheme, which is built upon group signatures and policy attribute-based encryption techniques. 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.

Meanwhile, the user signs encrypted data with her group signature key for privacy-preserving and traceability. However, user revocation is not supported in their scheme. From the above analysis, we can observe that how-to securely share data files in a multiple-owner manner for dynamic groups while preserving identity privacy from an un trusted 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 [9].

1) The user in the group can share and store data files with others by the cloud.

2) The complexity and size taken for encryption is 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 and signed receipts will be collected after any revocation that reduces duplication of encrypted copies.

III. PROBLEM STATEMENT

In previous work it recommend a data sharing scheme, which can achieve key distribution and data sharing for static group. The basic contributions of that scheme include:

1. It is able to carry static groups basically, when a new user joins in the group or a user is revoked from the group, the private keys of the other users is need.

2. It secure data sharing scheme which can be confined from collusion attack. The revoked users can not be capable to get the original data files once they are revoked even if they

combine with the cloud. Our scheme can accomplish secure user revocation with the help of polynomial function.

3. It provides security examination to prove the security of our scheme. In addition, we perform imitations to exhibit the competence of our scheme.

4. It provides a secure way for key distribution with secure communication channels. But in our method the users can firmly obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user [10].

IV. PROPOSED SOLUTION

Cloud is operated by Cloud Service Providers(CSPs) which provides abundant storage services. However, the cloud is not fully trusted 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.

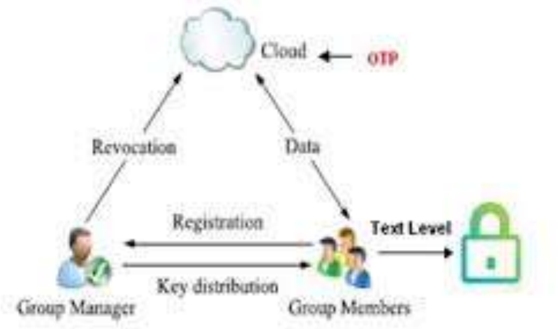

Fig-2:Execution Model

A Manager for group 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 AA manager is acted by the administrator of an organization. Therefore, we assume that the AA 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 my example, each group has members. Note that, the group membership is dynamically changed, due to the Member resignation and new member participation in an organization

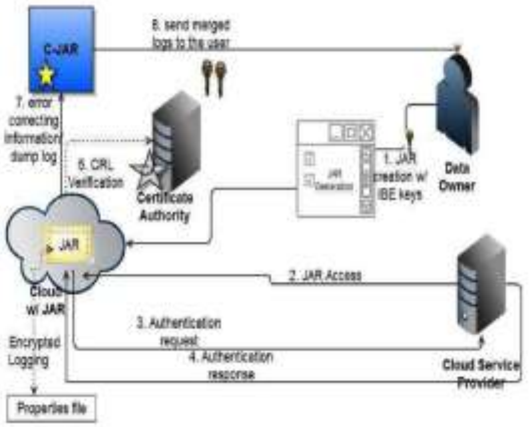
C-JAR
8. send merged logs to the user
7. error correcting information dump log
6. CRL Verification
Certificate Authority
JAR
1. JAR creation w/ IBE keys
Data Owner
JAR
Cloud w/ JAR
2. JAR Access
3. Authentication request
4. Authentication response
Encrypted Logging
Properties file
Cloud Service Provider

Fig-3: Proposed Model

Design goals

The main design goals of the proposed scheme including access control, data confidentiality, anonymity and traceability and efficiency as follows.

Access Control

The requirement of access controls two-fold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at anytime, and revoked users will be incapable of using the cloud once again they are revoked.

Data Confidentiality

Data confidentiality requires that unauthorized users including the cloud are incapable of learning the content of the stored data. 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 are 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 imposes 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 and share data files with others in the group by the cloud. User revocation cane achieved without involving 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 broadcast encryption technique allows data owners to securely share their data files with others including new joining users.

Unfortunately, each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increase with the number of revoked users. Thus the Large cipher text size may hinder the adoption of the broadcast encryption scheme to capacity-limited users. To tackle this challenging issue, let the group manager compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size. Specially, the computation overhead of users for encryption operations and the ciphertext size is constant and independent of their vocation users.

V. CONCLUSION

The In this paper, I design a secure data sharing scheme, for dynamic groups in an un trusted cloud. In this scheme a user is able to share data with others in the group without revealing identity privacy to the cloud. Secure policy supports efficient user revocation and new user joining [11]. Efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Extensive analyses show that the proposed scheme satisfies the desired security requirements and it guarantees efficiency as well [12].

VI. ACKNOWLEDGEMENT

The work is assessed and drafted with the assistance of guidance under the IPS which drives me to the immense results. Without them it would not be feasible for me to beat the issues and issues confronted. Along these lines, the author thanks the guide for their significant remarks, which reinforced the paper. They additionally get a effective results of the chance to express appreciation to GUIDE NAME who had guided me all through this research and being held dependably for discourse with respect to the methodology adjusted for this paper.

REFERENCES

[1] K.Marimuthu,D.Ganesh Gopal,K.Sashi Kanth,Srujay Setty and Kunal Tainwala “Scalable and Secure Data Sharing for Dynamic Groups in Cloud”,-2014 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)

[2] Tao Jiang, Xiaofeng Chen, and Jianfeng Ma “Public Integrity Auditing for Shared Dynamic Cloud Data with Group User Revocation”-2015 10.1109/TC.2015.2389955, IEEE Transactions on Computers

[3] Zhongma Zhu, Zemin Jiang and Rui Jiang, “The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in theCloud,” 2013 International Conference on Information Science and Cloud Computing Companion.

[4] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, “Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013.

[5] Anton Beloglazov and Rajkumar Buyya “Energy Efficient Allocation of Virtual Machines in Cloud Data Centres”-2013 10th IEEE/ACM International Conference on Cluster, Cloud and Grid Computing

[6] 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.

[7] 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.

[8] 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.

[9] C. Delerablee, P. Paillier, and D. Pointcheval, “Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ci-phertexts or Decryption Keys,” Proc. First Int’l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[10] Rui Jiang, Zhongma Zhu and Zemin Jiang, , “The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013), Guangzhou, Dec.7, 2013, pp. 185-189.

[11] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, “Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage,” IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[12] Xukai Zou, Yuan-shun Dai, and Elisa Bertino, “A practical and flexible key management mechanism for trusted collaborative computing,” INFOCOM 2008, pp. 1211-1219.