Asian Journal of Engineering and Applied Technology (AJEAT)
Vol.2.No.1 2014pp 25-29
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

RGDS: ACHIEVING REVOCATION FOR GROUP-BASED DATA SHARING IN CLOUD

Vinod S E, Dr.M.JayaPrasad
Dept of CSE, RGIT
Bangalore-32
Vinuvinod79@gmail.com, mj_prasad@yahoo.com

ABSTRACT

A new revocation technique will be proposed in this paper. The paper MONA provides the securely sharing the data among the groups, which maintains the data and identity privacy by making use of the concept of the group signature and dynamic broadcast encryption. In our scheme RGDS a separate revocation list will be constructed by the group manager which helps to identify the revoked user.

Key words: Revocation , Tracing, Data Sharing , Cloud Computing.

1. INTRODUCTION

Cloud computing is one of the emerging technology [2] in the recently years due to the advantages of greater flexibility and availability in obtaining computing resource at lower cost. Cloud Computing gained more popularity among individuals as well as organizational users. Cloud Computing system provides on-demand service to end user with “pay-as-you-go” basis. That is user pay only based on the type of access service and time of access. Some of the cloud service providers such as Amazon, Verizon, and IBM are able to provide various services to cloud users with the help of powerful datacenters.

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application, A organization allows its workers in the same group to store and share files in the cloud.By making use of cloud, the worker can be completely freed from the troublesome local data storage and maintenance. However ,it also poses a significant risk to the confidentiality of those stored files. The cloud service provider or third party may not fully trusted by the users. While the data files stored in the cloud may be sensitive and confidential. The basic solution is to encrypt the data and then upload the encrypted data into the cloud. Designing am efficient and secure sharing scheme for groups in cloud is a difficult task due to the following reason:

Initially, identity privacy has to be maintained, which is the most significant obstacles for the wide deployment of cloud is 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

Next challenging issue is that, data storing and data sharing, it is highly recommended that any members in a group should be able to fully enjoy the data storing and data sharing services provided by the cloud, which is called as multiple owner manner. Now each user in the group is able to not only read data but also modify the data.

Next issue is that, the changes of membership make secure data sharing extremely difficult. Another challenging thing is that newly granted users to learn the content with the anonymous data owners, and obtain the corresponding decryption keys.

Next challenging issue is that efficient membership revocation mechanism should be achieved without updating their secret keys of the remaining users and it is also desired to reduce the complexity of the key management.

The draw backs of the existing system can be overcome using this proposed system[1]. The main contribution of this paper is that:

- The proposed system uses MONA. Any user in the group can store and share data files with others by the cloud.
- This schema 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.

- It provides the secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resources.
- The real identities of data owners can be identified or revealed by the group manager when dispute occur.
- User revocation can be easily achieved through a novel revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users.
- We demonstrate the efficiency of our schema in terms of storage and computation head by security analysis.

2. RELATED WORKS

In [10] Lu et al proposed a secure provenance schema which uses the concept of cipher text-policy attribute based encryption and the group signature. In this proposed schema the user obtains two keys after the registration i.e group signature key and an attribute key. The attribute encryption is used to encrypt the data file, this encrypted data file can be decrypted using the attribute key. The main drawback of this, is that user revocation is not achieved in this schema.

In [3] Yu et al proposed a scalable and fine grained data access in cloud using Key Policy-Attribute based encryption method. The data owner encodes the data file using any random key, where the chosen random key is again encrypted along with a set of attributes using KP-ABE. Then, the group manager provides an access structure and decryption keys to the user. The cipher text can be decrypted by the user if and only if the attributes satisfy the access structure assigned. To achieve user revocation, data owner needs to update all attributes and keys. The main drawback is that does not allow multiple owner sharing and maximum utilization of cloud.

In [4], Kallahalla et al. developed a cryptographic storagesystem that facilitates secure file sharing on untrustedservers called Plutus. The file is divided into no of smallfiles each then encrypted with secret key. Users areprovided with corresponding key to decrypt required fileblocks. The main drawback is that, heavy key distributionoverhead experienced for large scale file sharing. Also, toperform user revocation entire file blocks need to be re-encrypted for redistribution

In [11] The proxy re-encryption model given by Atenieseet al. strengthens the distributed storage. The user encryptsthe file using symmetric keys which further encrypted by amaster public key. For access control, server uses proxycryptography to re-encrypt the content using master keysThe main drawback is that,a collusion attack betweenuntrusted server and revoked users may launch, whichenables them to know the decryption keys used for theencryption. From the above analysis the author observedthat the how to securely share data files in a multi-ownermanner for dynamic groups while preserving the identityprivacy from an untrusted cloud.

2.1 Revocation List

It is list of the revoked users, who tries to attack the dataThe revoked list should be updated frequently [8]. Therevocation list will be monitored by the group manager andeven updates in the cloud, so that revoked user cannotaccess or share the data in the cloud.

2.2 Group Signature

Chaum and Van Heyst introduced the concept called groupsignature[6].In this paperwe present a new type ofsignature for a group of person called a group signaturewhich has the following properties:

(i) Any members of the group can sign messages.
(ii) Keeps the identity secret from the verifiers.
(iii) Only the group manager can reveal the real identity, when the dispute occurs which is called as traceability.

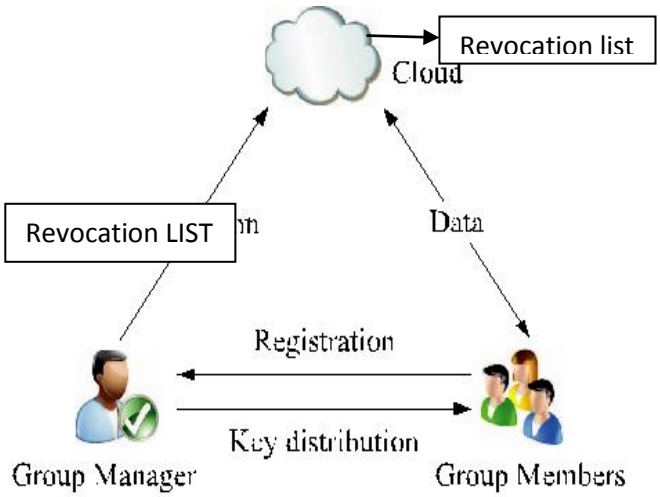
2.3 Dynamic Broadcast Encryption

Broadcast encryption allows a user to distribute messagesecurely to a set/group of users in an in secure environment [7] so that only a privileged subset of users can decrypt thedata. Apart from this Dynamic broadcast encryption alsoallows the group manager to dynamically include newmembers while preserving previously computed information, i.e., user decryption keys need not berecomputed, the morphology and size of cipher texts areunchanged and the group encryption key requires nomodification. The first formal definition and constructionof dynamic broadcast encryption are introduced based onthe bilinear pairing technique, which will be used as thebasis for file sharing in dynamic groups

3 SYSTEM MODEL AND DESIGN GOALS

3.1 System Model

The system model consists of three different entites as illustrated in the below figure. The Group manager, Group members and the cloud which would be represented as:



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 a members. Note that, the group membership is dynamically changed, due to the staff registration and new worker participation in the organization.

Manager of the group takes charge of user registration, system parameters generation, 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 an organization. Therefore we assume that the group manager is fully trusted by the other parties.

Cloud is operated by cloud service provider(CSPs) and provides priced abundant storage services However, the cloud is not fully trusted by the users are very likely to be outside the cloud user's trusted domain

3.2 Design Goals

Achieving Revocation: The revocation should be achieved by maintaining the revocation list. If the signature does not match then he will be considered a revoked users. The revoked user should not be allowed to share or access the data files from the cloud.

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

Traceability and Anonymity: 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

Access Control: The requirement of access control is 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.

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 can be 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 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 is unable to decrypt the data moved into the cloud after the revocation.

Compared with the existing system, it has the following advantages

- 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
- 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
- The new user can directly decrypt the files stored in the cloud before his participation.

4. PROPOSED WORK

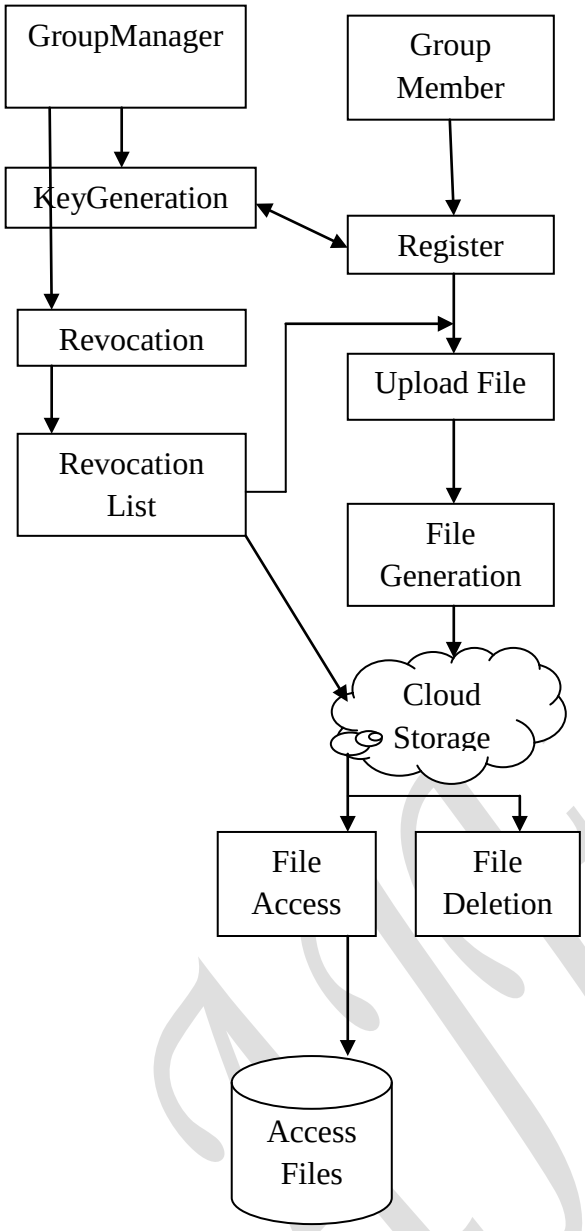
This section describes the details of system initialization, user registration, user revocation, file generation, file deletion, file access

4.1 System Initialization

The group manager takes charge of system initialization as follows: Generating a bilinear map group system S=(q,G1,G2,e(.,.));

4.2 User Registration

The user or the group members get registered to the group manager. The group manager will be held responsible .User has to provide the group ID for the registration, once the user got registered, user obtains private key, which will be used for group signature and file decryption.



4.3 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.

4.4 File Generation

To store and share a data file in the cloud, a group member performs the following operations

1. Getting the revocation list from the cloud. In this step, the member sends the group identity ID group as a request to the cloud. Then, the cloud responds the revocation list RL to the member

2. Verifying the validity of the received revocation list. First, checking whether the marked date is fresh. Second, verifying the contained signature. If the revocation list is invalid, the data owner stops this scheme

4.5 File Deletion

File stored in the cloud can be deleted by either the group manager or the data owner (i.e., the member who uploaded the file into the server). To delete a file the group manager computes a signature and sends the signature along with to the cloud. The cloud will delete the file if the equation holds.

4.6 File Access

To learn the content of a shared file, a member does the following actions:

1. Getting the data file and the revocation list from the cloud server. In this operation, the user first adopts its private key to compute a signature. Then, the user sends a data request containing to the cloud server Upon receiving the request, the cloud server checks the validity of the signature and performs a revocation verification according to the revocation list. After successful verification, the cloud server responds the corresponding data file and the revocation list to the user.

2. Checking the validity of the revocation list.

3. Verifying the validity of the file and decrypting it.

4.7 Traceability

When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner.

5.CONCLUSION

In this paper we design a secure data sharing scheme and achieves the revocation using the revocation list for dynamic groups in an untrusted cloud .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 a new user joining More specially, user revocation can be achieved through a public revocation list without updating the private keys of the remaining users , and the new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

REFERENCES

[1] X. Liu, Y. Zhang, B. Wang and J. Yan, “Mona: Secure Multi-Owner Data Sharing for Dynamic Group in the Cloud,” IEEE Tran. On Parallel and Distributed System,vol. 24, no. 6 June 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph R.H Katz,A. Konwinski, G. Lee,

A.D Patterson, A. Rabkin, I Stoica, and M. Zaharia " A View of Cloud Computing," comm.ACM vol. 53, no. 4, pp. 50-58, April 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] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136 149, Jan. 2010

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

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

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

[9] B. Wang, B. Li, and H. Li, "Knox: Privacy Preserving Auditing for Shared Data with Large Groups in the Cloud Proc. 10th Int Conf. Applied Cryptography and Network

[10] B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," proc. Int'l ConfPratice and Theory in Public Key Cryptography Conf. Public Key Cryptography pdf.2008

[11] G. Ateniese, K. Fu, M. Green, and S. Hohenberher Improved Proxy Re-Encryption Schemes with Applications to Secure distributed Storage," Proc. Network and Distributed System Security Symp. (NDSS), pp. 29-43,2003