ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secure Sharing Of Data for Dynamic Multi Owner in Cloud Storage

S.Surya[1], V.Karuppuchamy[2]

M.E, Department of CSE, Muthayammal Engineering College, Tamilnadu, India[1]

AP, Department of CSE, Muthayammal Engineering College, Tamilnadu, India[2]

ABSTRACT - Cloud computing is an emerging computing paradigm. It provides an economical and efficient solution for sharing group resource among cloud users. Due to frequent change of members in multi owner group, preserving user data and their identity privacy becomes a challenging issue in cloud. In this paper, we propose a secure multi-owner data sharing scheme, for dynamic groups in the cloud. By including group signature and stateless broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead, length of the signature and the running time of the signing algorithm are independent with the number of group members.

KEYWORDS—Cloud computing, identity privacy, multi owner, dynamic groups

I. INTRODUCTION

Cloud computing is recognized as an alternative to traditional information technology 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.

One of the most fundamental services offered by cloud providers is data storage. Let us consider a practical data application. A company allows its staffs in the same group or department to store and share files in the cloud. By utilizing the cloud, the staffs can be completely released from the troublesome local data storage and maintenance. However, it also poses a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not fully trusted by users while the data files stored in the cloud may be sensitive and confidential, such as business plans. 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 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. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Therefore, traceability, which enables the group manager (e.g., a company manager) to reveal the real identity of a user, is also highly desirable.

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, where only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in practical applications. More concretely, each user in the group is able to not only read data, but also modify his/ her part of

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

data in the entire data file shared by the company.

Last but not least, groups are normally dynamic in practice, e.g., new staff participation and current employee revocation in a company. The changes of membership make secure data sharing extremely difficult. On one hand, the anonymous system challenges new granted users to learn the content of data files stored before their participation, because 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 the secret keys of the remaining users is also desired to minimize the complexity of key management.

Several security schemes for data sharing on untrusted servers have been proposed. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption keys only to authorized users. Thus, unauthorized users as well as storage servers cannot learn the content of the data files because they have no knowledge of the decryption keys.

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. By setting a group with a single attribute, Lu et al proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique , which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. 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.

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

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. 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.
3. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

II. RELATED WORK

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 file group with a unique file-block key, the data owner can share the file groups 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.

In files stored on the untrusted server include two parts: file metadata and file data. The file metadata implies the access control information including a series of encrypted key blocks, each of which is Encrypted under the public key of authorized users. Thus, the size of the file metadata 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 NNL construction [10] is used for efficient key revocation. However, when a new user joins the group, the private key of each user in an NNL system needs to be recomputed, which may limit the application for dynamic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale.

Ateniese et al leveraged proxy re encryptions to secure distributed storage. Specifically, the data owner encrypts blocks of content with unique and symmetric content keys, which are further encrypted under a master public key. For access control, the server uses proxy cryptography to directly reencrypt the appropriate content key(s) from the master public key to a granted user's public 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.

Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the 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 group manager assigns an access structure and the corresponding secret key to authorized users, such that a user can only decrypt a ciphertext if and only if the data file attributes satisfy the access structure. To achieve user revocation, the manager delegate's tasks of data file reencryption and user secret key update to cloud servers. However, the single-owner manner may hinder the implementation of applications with the scenario, where any member in a group should be allowed to store and share data files with others.

Lu et al. 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. 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 untrusted cloud remains to be a challenging issue. In this paper, we propose a novel Mona protocol for secure data sharing in cloud computing. Compared with the existing works, any user in the group can store and share data files with others by the cloud.

1. The computational effort for signing and verification are independent with the number of members leave the group.
2. User revocation can be achieved without updating the private keys of the remaining users.
3. The length of group's public key independent of the number of group members.

III. PRELIMINARIES

3.1 Bilinear Maps

Let G_1 and G_2 be an additive cyclic group and a multiplicative cyclic group of the same prime order q, respectively. Let e : $G_1 \times G_1$! G_2 denote a bilinear map constructed with the following properties:

1. Bilinear:For all a, b € Z_q^* and R,Q €G_1, e(aR,pQ)=e(R,Q).

2. Nondegenerate: There exists a point R such that e(P,Q)^ab.

3. Computable: There is an efficient algorithm to compute e(R,Q) for any R,Q€G1.

3.2 Group Signature

The concept of group signatures was first introduced in by Chaum and van Heyst. In general, 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. In this paper, a variant of the short group signature scheme will be used to achieve

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

anonymous access control, as it supports efficient membership revocation.

3.3 Dynamic Broadcast Encryption

Broadcast encryption enables a broadcaster to transmit encrypted data to a set of users so that only a privileged subset of users can decrypt the data. Besides the above characteristics, dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information, i.e., user decryption keys need not be recomputed, the morphology and size of ciphertexts are unchanged and the group encryption key requires no modification. The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique in, which will be used as the basis for file sharing in dynamic groups.

IV. SYSTEM MODEL AND DESIGN GOALS

4.1 System Model

We consider a cloud computing architecture by combining with an example that a company uses a cloud to enable its staffs in the same group or department to share files. 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 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.

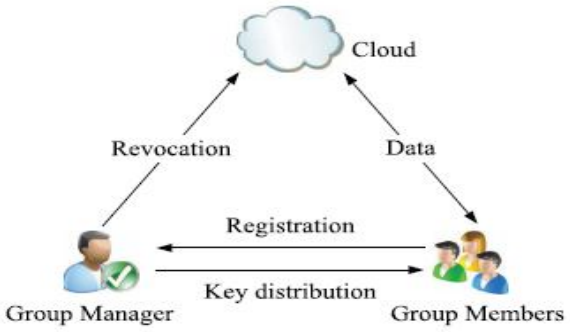

Fig. 1. System model.

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.

4.2 Design Goals

In this section, we describe the main design goals of the proposed scheme including access control, data confidentiality,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

anonymity and traceability, and efficiency as follows:

Access control: The requirement of access control is twofold. First, group members are able to use the cloud resource for data operations. Second, unauthorized users cannot access the cloud resource at any time, and revoked 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 of learning the content of the stored data. An important and challenging issue for data confidentiality is to maintain its availability for dynamic groups. Specifically, 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, traceability and efficiency: Anonymity guarantees that group members can access the cloud without revealing the real identity. Although anonymity represents an effective protection for user identity, it also poses a potential inside attack risk to the system. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to tackle the inside attack, the group manager should have the ability to reveal the real identities of data owners. 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. That is, the remaining users do not need to update their private keys or reencryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

V. THE PROPOSED SCHEME: MONA

5.1 Overview

To achieve secure data sharing for dynamic groups in the cloud, we expect to combine the group signature and dynamic broadcast encryption techniques. Specially, the group signature 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 ciphertext increase with the number of revoked users.

To tackle this challenging issue, we 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 ciphertext size. Specially, the computation overhead of users for encryption operations and the ciphertext size is constant and independent of the revocation users.

5.2 Scheme Description

This section describes the details of Mona including system initialization, user registration, user revocation, file generation, access controlling, and traceability

5.2.1 System Initialization

The group manager takes charge of system initialization as follows:

- Generating a bilinear map group system S=(q,G1,G2,e(‘,’)).
- Selecting two random numbers H.H0 € G1 along with two random numbers £1£2 €G1.
- Randomly choosing two elements P.G€G1and a number γ€z*.

5.2.2 User Registration

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

For the registration of user i with identity ID_i, the group manager randomly selects a number $x_i \in Z_q^*$ and computes A_i; P_i as the following equation:

$$A_i = \frac{1}{\gamma + x_i} R \in G_1$$

$$P_i = \frac{x_i}{\gamma + x_i} . G \in G_1$$

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

5.2.3 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. As illustrated in Table 1, the revocation list is characterized by a series of time stamps ($t_1 < t_2 <$; :::; t_r). Let ID_{group} denote the group identity. The tuple (A_i; x_i; t_i) represents that user i with the partial private key (A_i; x_i) is revoked at time t_i. R_1; R_2; :::; R_r and Z_r are calculated by the group manager with the private secret as follows:

$$R_1 = \frac{1}{\gamma + x_1} R \in G_1$$

$$R_2 = \frac{1}{(\gamma + x_1)(\gamma + x_2)} R \in G_1$$

$$R_r = \frac{1}{(\gamma + x_1)(\gamma + x_2) \ldots (\gamma + x_r)} R \in G_1$$

$$Z_r = \frac{1}{z(\gamma + x_1)(\gamma + x_2) \ldots (\gamma + x_r)} \in G_2$$

Motivated by the verifiable reply mechanism to guarantee that users obtain the latest version of the revocation list, we let the group manger update the revocation list each day even no user has being revoked in the day. In other words, the others can verify the freshness of the revocation list from the contained current date t_{RL}. In addition, the revocation list is bounded by a signature sig(RL) to declare its validity. The signature is generated by the group manager with the BLS signature algorithm, i.e., $sig(RL)=\gamma f_1(RL)$. Finally, the group manager migrates the revocation list into the cloud for public usage.

5.2.4 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 request to the cloud. Then, the cloud responds the revocation list RL to the member.

2 Verifying the validity of the received revocation list.

a. First, checking whether the marked date is fresh.Second, verifying the contained signature sig(RL) by the equation $e(W, f_1(RL) = e(P, sig(RL))$. If the revocation list is invalid, the data owner stops this scheme.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

3 Encrypting the data file M. This encryption process can be divided into two cases according to the revocation list.

a. Case 1. There is no revoked user in the revocation list:

i. Selecting a unique data file identity ID_{data};
ii. Choosing a random number k € Z_q^*,

iii. Computing the parameters C_1,C_2,K; C as the following equation:

a. $C_1 = k .Y € G_1$
b. $C_2 = k .P € G_1$
c. $K = Z^k € G_2$
d. $C = Enc_k(D)$

b. Case 2. There are r revoked users in the revocation list.

c. I Selecting a unique data file identity ID_{data};
d. II Choosing a random number k €Z_q^*;

e. III Computing the parameters C_1,C_2,K,C as the following equation:

4 Selecting a random number μ and computing f(μ). The hash value will be used for data file deletion operation. In addition, the data owner adds (ID_{data},μ) into his local storage.

5 Constructing the uploaded data file as shown in Table 2, where t_{data} denotes the current time on the

Table 1:Message Format For Uploading Data

Group ID	Data ID	Cipher Text	Hash	Time	Signature
ID_{group}	ID_{data}	C1,C2,C	f(μ)	T_{data}	σ

6 Uploading the data shown in Table 1 into the cloud server and adding the ID_{data} into the local shared data list maintained by the manager. On receiving the data, the cloud first invokes Algorithm 2 to check its validity. If the algorithm returns true, the group signature is valid; otherwise, the cloud abandons the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification by using Algorithm. Finally, the data file will be stored in the cloud after successful group signature and revocation verifications.

5.2.5 Access Controlling

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 ID_{data}, the group manager computes a signature $\mu f_1(ID_{data})$ and sends the signature along with ID_{data} to the cloud. The cloud will delete the file if the equation $e(\mu f_1(ID_{data}),P)= e(W,f1 (ID_{data})$ holds.

Algorithm (1).Signature Generation
Input: Private key(A,x),system parameter(P,U,V,H,W) and data D.
Output: Generate a valid group signature on D.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Begin
Select random numbers $\alpha,\beta,r_{\alpha},r_{\beta},r_x,r_{\delta 1},r_{\delta 2} \in Z_q^*$
Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
Compute the following values
$T_1 = \alpha.U$
$T_2 = \beta.V$
$T_3 = A_i + (\alpha + \beta).H$
$N_1 = r_{\alpha}.U$
$N_2 = r_{\beta}.V$
$N_3 = r_x.T_1 - r_{\delta 1}.U$
$N_4 = r_x.T_2 - r_{\delta 2}.V$
Set $l = f(D, T_1, T_2, T_3, N_1, N_2, N_3, N_4, N_5)$
Compute the following numbers
$s_{\alpha} = r_{\alpha} + l\alpha$
$s_{\beta} = r_{\beta} + l\beta$
$s_x = r_x + lx$
$s_{\delta 1} = r_{\delta 1} + l\delta 1$
$s_{\delta 2} = r_{\delta 2} + l\delta 2$
Return $\sigma = (T_1, T_2, T_3, l, s_{\alpha}, s_{\beta}, s_x, s_{\delta 1}, s_{\delta 2})$
end

Algorithm 2.Signature Verification
Input: System parameters(R,U,V,W),D and a signature $\sigma = (T_1, T_2, T_3, l, s_{\alpha}, s_{\beta}, s_x, s_{\delta 1}, s_{\delta 2})$
Output: True or False
Begin
Compute the following values
$R_1' = s_{\alpha}.U - l.T_1$
$R_2' = s_{\beta}.U - l.T_2$
$R_3' = \left(\frac{e(T3,W)}{e(P,P)}\right)^l e(T_3,R)^{S_x} e(H,W)^{-S_{\alpha}-S_{\beta}}$
$R_4' = s_X.T_1 - U.s_{\delta 1}$
$R_5' = s_X.T_2 - V.s_{\delta 2}$
If $l = f(D, T_1, T_2, T_3, R_1', R_2', R_3', R_4', R_5')$
Return True
Else
Return False
End

File Access

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

Getting the data file and the revocation list from the cloud server. In this operation, the user first adopts its private key (A, x) to compute a signature $\_u$ on the message (ID_{group}, ID_{data}, t) by using Algorithm 1, where t denote the current time, and the ID_{data} can be obtained from the local shared file list maintained by the manager. Then, the user sends a data request

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

containing (ID_{group}, ID_{data},t) to the cloud server. Upon receiving the request, the cloud server employs Algorithm 2 to check the validity of the signature. After a successful verification, the cloud server responds the corresponding data file and the revocation list to the user.

Checking the validity of the revocation list. This operation is similar to the step 2 of file generation phase.Verifying the validity of the file and decrypting it. The format of the downloaded file coincides with that given in Table 1.

5.2.6 Traceability

When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner. Given a signature σ the group manager employs his private key to compute A_i. Given the parameter A_i, the group manager can look up the user list to find the corresponding identity.

VI. CONCLUSION

In this paper, we design a secure data sharing scheme, 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 new user joining. More specially, 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.Moreover, the storage overhead, length of the signature and the running time of the signing algorithm are independent with the number of group members.

REFERENCES

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, Jingbo Yan "Mona:Secure Multi-owner Data Sharing for Dynamic Groups in the Cloud,"vol 24,No 6,June 2013.
[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] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.
[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] 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.
[6] 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.
[7] 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), 2006.
[8] 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.
[9] 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.
[10] 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.
[11] 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.