INTERNATIONAL JOURNAL OF COMPUTER SCIENCE ENGINEERING RESEARCH AND DEVELOPMENT (IJCSERD)

ISSN 2248 – 9363(Print)
ISSN 2248 – 9371(Online),
Volume 4, Number 2, April- June (2014), pp: 25-33

IJCSERD

ENCRYPTION BASED MULTI USER MANNER SECURED DATA SHARING AND STORING IN CLOUD

[1]Laxmi Nirawaneppa Gokavi, [2] Mrs. Divya A K

[1]Department of Computer Science and Engineering, VTU Belgaum, KVGCE Sullia, DK
[2]Assoc Professor Department of Computer Science and Engineering KVGCE Sullia, DK

ABSTRACT

With the character of low management, cloud computing provides an various and efficient solution for sharing group tasks among cloud users. Unfortunately, sharing data in a multi-owner manner while handling data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent gradiant of the membership. In this paper, a secure multi owner data sharing scheme for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments.

INDEX TERMS: Cloud Computing, Data Sharing, privacy–preserving, access control, dynamic groups.

I. INTRODUCTION

Cloud computing is recognized as one of the latest traditional information technology [1] 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 analysing 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 [2]. Unfortunately, designing an efficient and secure data sharing scheme for groups in the cloud is not an easy task due to the following challenging terms. 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 [3], 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 data in the entire data file shared by the company.

Cloud computing is a new concept of computing technique, by which computer resources are provided dynamically via Internet. It attracts considerable attention and interest from both academia and industry. However, it also has at least three challenges that must be handled before applied to our real life. First of all, data confidentiality should be guaranteed. When sensitive information is stored in cloud servers, which is out of users' control in most cases, risks would rise dramatically. The servers might illegally inspect users' data and access sensitive information. Unauthorized users may also be able to intercept someone's data (e.g. server compromise). Secondly, personal information (defined by a user's attributes) is at risk because one's identity is authenticated according to his information.

As people are becoming more concerned about their privacy these days, the privacy-preservability is very important. Preferably, any authority or server alone should not know any client's personal information. Last but not least, the cloud computing system should be resilient in the case of security breach in which some part of the system is compromised by attackers. Few years later, and Waters proposed a new type of IBE Fuzzy Identity-Based Encryption [4], which is also known as Attribute-Based Encryption (ABE).

In this work, an identity is viewed as a set of descriptive attributes. Different from the IBE, where the decrypted could decrypt the message if and only if his identity is exactly the same as what specified by the encrypted, this fuzzy IBE enables the decryption if there are 'identity overlaps' exceeding a pre-set threshold between the one specified by encrypted and the one belongs to decrypter. However, this kind of threshold-based [5] scheme was limited for designing more general system because the threshold based semantic cannot express a general condition. Before long, more general tree-based ABE schemes. 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 [6] proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique [7], which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique [7]. Unfortunately, the single owner manner hinders the adoption of their scheme into the case, where any user is granted to store and share data. To solve the challenges presented above, we propose Mona, a secure multi-owner data sharing scheme for dynamic groups in the cloud.

The main contributions of this paper include:

1. 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. This 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.
4. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

II. RELATED WORKS

By dividing files into file groups 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 [7], 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 [8] 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 groups. Another concern is that the computation overhead of encryption linearly increases with the sharing scale. 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 re encrypt the appropriate content key(s) from the master public key to a granted user's public key.

Unfortunately, a collusion attack between the untrusted server and any revoked malicious user can be launched, which enables them to learn the decryption keys of all the encrypted blocks. In presented a scalable and fine-grained data access control scheme in cloud computing based on the KPABE 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 cipher text if and only if the data file attributes is as follows:

1. Any user in the group can store and share data files with others by the cloud.
2. The encryption complexity and size of ciphertexts are 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.
4. A new user can directly decrypt the files stored in the cloud before his participation

III. PROPOSED SCHEME

To secure share data files in a multiple owner manner for dynamic groups while preserving identify privacy from an untrusted cloud remains to be a challenging issue. In the group can store and share data files with others by the cloud. The encrypted complexity and size of cipher texts are independent with the number of revoked users in the system. Used revocation can be achieved without updating the private keys of the remaining users. The group manager takes charge of system initialization. Before participation of the user the main processing of the system should be ready to initial to performing the upcoming action due to the each and every development 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 re encryption operations. New granted users can learn all the content data files.

Fig.1: The system model consists of three different entities: the cloud, a manager and a large number of group members as illustrated in Fig.1.

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 system model 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 [3], [7], 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 [7], [8], 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.

A. Functions of Proposed methods

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

1).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.

2).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 **3).Group Signature**

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 [9] will be used to achieve anonymous access control, as it supports efficient membership revocation. 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.

4.) Anonymity and traceability:

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.

5).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. 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.

6) Dynamic Broadcast Encryption

Broadcast encryption [8] 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.

IV. IMPLEMENTATION

A .System Initialization

This section describes the details of user actions along with all the information data that contains system initialization, user registration, user revocation, file generation, file deletion, file access and traceability. Selecting random number for each elements and generating

B. User registration

For the registration of user with identity ID the group manager randomly selects a number x and y computes. Then, the group manager adds in to the group user list, which will be used in the traceability phase. After the registration, user obtains a private key which will be used for group signature generation and file decryption.

1. Algorithm for user Registration

```
If (new user)   // Owner
        then register and complete SLA; // SLA should be signed between CSP and service owner
    else
        login and upload service with service policy; // registered user

 if (new user) // end user
   then register with valid details;
   get new password through mail; //sent by the CKG(cloud key generator)
else
   login;    // already registered users
```

2. Algorithm for Key generation

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 in addition; the revocation list is bounded by a signature to declare its validity. The signature is generated by the group manager with the signature generation algorithm finally, the group manager migrates the revocation list into the cloud for public usage.

```
// this layer is dealing with user key generation and maintaining user log
If (user wants to access service)
{
   Apply to the CKG
     {
          If CKG grant user's request
           {
              A secret key will be send to the user; // that key user will use at the time of accessing
             That key and user's IP will be sending to owner's mail-id;
              That key and the User's IP will be stored to the log file; // to maintain access history
           }
else
{
   Wait for the CKG response;
}
```

C. Key Distribution

User revocation is performed by the group manager via a public available revocation list 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 ID denote the group identity. The tuple represents that user with the partial private key calculated by the group manager with the private secret as follows. If any user left out from the group means group manager need to send a revocation list to the cloud and every time no need to update the list. It will be directly updated dynamically to the cloud.

3. Complexity Assumptions

Definition 1 (q-strong Diffie-Hellman (q-SDH) Assumption [12]). *Given* $(P_1, P_2, \gamma P_2, \gamma^2 P_2, \ldots, \gamma^q P_2)$, *it is infeasible to compute* $\frac{1}{\gamma+x} P_1$, *where* $x \in Z_q^*$.

Definition 2 (Decision linear (DL) Assumption [12]). *Given* $P_1, P_2, P_3, aP_1, bP_2, cP_3$, *it is infeasible to decide whether* $a + b = c \bmod q$.

Definition 3 (Weak Bilinear Diffie-Hellman Exponent (WBDHE) Assumption [13]). *For unknown* $a \in Z_q^*$, *given* $Y, aY, a^2Y, .., a^lY, P \in G_1$, *it is infeasible to compute* $e(Y, P)^{\frac{1}{a}}$.

Definition 4 ((t,n)-general Diffie-Hellman Exponent (GDHE) Assumption [14]). *Let* $f(X) = \Pi_{i=1}^{r}(X + x_i)$ *and* $g(X) = \Pi_{i=1}^{n-r}(X + x_i^{'})$ *be the two random univariate polynomials. For unknown* $k, \gamma \in Z_q^*$, *given*

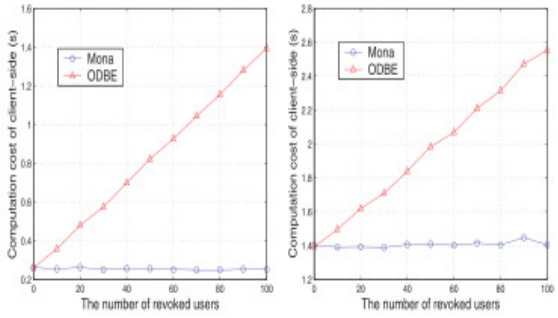
$G_0, \gamma G_0, ..., \gamma^{t-1} G_0, \gamma f(\gamma) G_0, P_0, ..., \gamma^{t-1} P_0, kg(\gamma) H_0 \in G_1$ and $e(G_0, H_0)^{f^2(\gamma) g(\gamma)} \in G_2$,

it is infeasible to compute $e(G_0, H_0)^{kf(\gamma)g(\gamma)} \in G_2$.

- Selecting two random elements $H, H_0 \in G_1$ along with two random numbers $\xi_1, \xi_2 \in Z_q^*$, and computing $U = \xi_1^{-1} H$ and $V = \xi_2^{-1} H \in G_1$ such that $\xi_1 \cdot U = \xi_2 \cdot V = H$. In addition, the group manager computes $H_1 = \xi_1 H_0$ and $H_2 = \xi_2 H_0 \in G_1$.
- Randomly choosing two elements $P, G \in G_1$ and a number $\gamma \in Z_q^*$, and computing $W = \gamma \cdot P$, $Y = \gamma \cdot G$ and $Z = e(G, P)$, respectively.
- Publishing the system parameters including $(S, P, H, H_0, H_1, H_2, U, V, W, Y, Z, f, f_1, Enc())$, where f is a one-way hash function: $\{0,1\}^* \rightarrow Z_q^*$; f_1 is hash function: $\{0,1\}^* \rightarrow G_1$; and $Enc_k()$ is a secure symmetric encryption algorithm with secret key k.

In the end, the parameter $(\gamma, \xi_1, \xi_2, G)$ will be kept secret as the master key of the group manager.

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



(a) Generating a 10 MB file (b) Generating a 100 MB file

V. PERFORMANCE DISCUSSION

Cloud computing is synonym for distributed computing over a network, and means the ability to run a program or application on many connected computers at the same time. This paper also more commonly refers to network-based services, which appear to be provided by real server hardware, and are in fact served up by virtual hardware, simulated by software running on one or more real machines. Such virtual servers do not physically exist and can therefore be moved around and scaled up on the fly without affecting the end user arguably, rather like a cloud. Access control 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 revoked.

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 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 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] 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. 136149, 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, "Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[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. 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.

[9] 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.

[10] 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.