International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud

Anusha Jaliparthi[*1] and CH. Ravindra Reddy[#2]

[*]*Student, Dept of CSE, Sree Vahini Institute of Science and Technology, Tiruvuru., A.P, India*

[#]*Associate Professor, Dept of CSE, Sree Vahini Institute of Science and Technology, Tiruvuru., A.P, India dist*

Abstract— Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as services over the Internet. As promising as it is, this paradigm also brings forth many new challenges for data security and access control when users confidential against untrusted servers, existing solutions usually apply cryptographic methods by disclosing data decryption keys only to authorized users. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. To preserve data privacy, a basic solution is to encrypt data files, and then upload the encrypted data into the cloud. To resolve this problem recently the best efficient method MONA presented for secured multi owner data sharing in however we identified some limitations in the same approach in terms of reliability and scalability. Hence in this paper we are further extending the basic MONA by adding the reliability as well as improving the scalability by increasing the number of group managers dynamically.

Key Words— Cloud Computing, dynamic groups, data sharing, reliability

I. INTRODUCTION

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. In cloud computing, the word cloud (also phrased as "the cloud") is used as a metaphor for "the Internet," so the phrase cloud computing means "a type of Internet-based computing," where different services — such as servers, storage and applications —are delivered to an organization's computers and devices through the Internet. 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. 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.

Cloud offers enormous opportunity for new innovation, and even disruption of entire industries. Cloud computing is the long dreamed vision of computing as a utility, where data owners can remotely store their data in the cloud to enjoy on demand high-quality applications and services from a shared pool of configurable computing resources. 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. For example, a misbehaved staff can deceive others in the company by sharing false files without being traceable. Maintaining the integrity of data plays a vital role in the establishment of trust between data subject and service provider. Although envisioned as a promising service platform for the Internet, the new data storage paradigm in "Cloud" brings about many challenging design issues which have profound influence on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that of data integrity verification at untrusted servers. What is more serious is that for saving money and storage space the service provider might neglect to keep or deliberately delete rarely accessed data files which belong to an ordinary client. CS2 provides security against the cloud provider, clients are still able not only to efficiently access their data through a search interface but also to add and delete files securely.

Advantages and Disadvantages of Cloud Computing:

Advantages:-

- Location Independent
- Less cost (Pay-as-per-you-Use).
- Easy to Maintain.
- Secure Storage and Management
- High level computing

Disadvantages:-

- Lack of control

- Security and privacy.
- Higher operational cost.
- Reliability

II. Our contributions

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

III. 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.

IV. Design Goals

In this section, we describe 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 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*.

For the registration of user i with identity IDi, the group manager randomly selects a number xi€Zq and computes Ai. 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.

5.3 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 (t1 < t2 <; :::; tr). Let IDgroup denote the group identity. The tuple (Ai; xi; ti) represents that user i with the partial private key (Ai; xi) is revoked at time ti. R1; R2; :::; Rr and Zr are calculated by the group manager with the private secret key.

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 tRL. 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)=γf1(RL). Finally, the group manager migrates the revocation list into the cloud for public usage.

5.4 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 IDgroup 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, f1(RL)= e(P, sig(RL)). If the revocation list is invalid, the data owner stops this scheme.

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 IDdata;

ii. Choosing a random number k € Zq

iii. Computing the parameters C1,C2,K; C as the following equation:

a. C1 = k .Y € G1
b. C2 = k .P € G1
c. K = Zk € G2
d. C = Enck(D)
b. Case 2. There are r revoked users in the revocation list.
c. I Selecting a unique data file identity IDdata;
d. II Choosing a random number k €Zq*;
e. III Computing the parameters C1,C2,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 (IDdata,μ) into his local storage.

5. Constructing the uploaded data file as shown in Table 2, where tdata denotes the current time.

5.5 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 (IDgroup, IDdata, t) by using Algorithm 1, where t denote the current time, and the IDdata can be obtained from the local shared file list maintained by the manager. Then, the user sends a data request containing (IDgroup, IDdata,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.

5.6 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 Ai. Given the parameter Ai, 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, Mona, for dynamic groups in an untrusted cloud. In Mona, a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona 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] 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.