International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 9 Issue 3 –SEPTEMBER 2014.

Secure Sharing Of Data for Dynamic Multi Groups in Cloud Environment

Jonna Siva Tejaswi[*1], and Y. Siva Prasad[#2]

[*]*Student, Dept of CSE, Guntur Engineering College, A.P., India*

[#] *Associate Professor, Dept of CSE, Guntur Engineering College, A.P., India*

[1]sivatejaswimca@gmail.com

[2]spy@reddiffmail.com

***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, integrity, scalability**

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.

1.1. 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

1.2. 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.

II. 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.

2.1 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 re-encryption operations. New granted users can learn all the content data files stored before his participation without contacting with the data owner.

III. THE PROPOSED SCHEME: MONA

3.1 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.

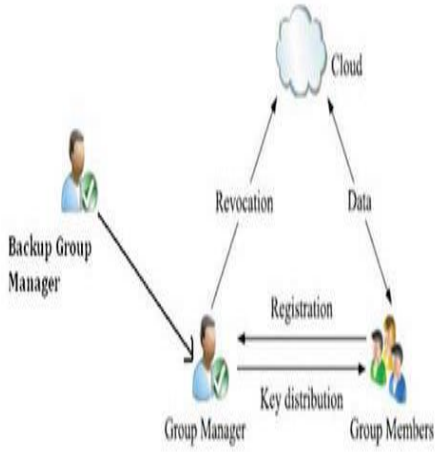

Fig 2: Proposed System Model

3.2 User Registration

User registered with their details such as identity (user name, password and email-id). Group manager select random number, base point , parameters and performs modulo with prime number, by using ECC (Elliptic Curve Cryptography) generate an private key. For registered users they will obtain private key, that private key is used for group signature and file decryption. The Group manager adds the user identity (ID) to the group user list that will be used in traceability phase.

3.3 User Revocation

User Revocation is performed by the group manager. Delta Revocation List is publicly available based on those, group members are allowed to encrypt the data and make that data confident against revoked users. Revoked users are maintained in the revoke user list and make publicly available in the cloud. Delta RL is bounded by signature to declare its validity. Upon receiving the resignation request from the group member, group member will be in evoked user list.

3.4 File Generation

Group members will store their data in real cloud. Aspose real cloud (SaaS) is provided by cloud service provider mainly for storage. The group members will request with group id and based on the Delta RL allow the data owner to upload the data in the cloud, if their signature is true. If it's a revoked user, cloud server will not allow generating the data and signature verification status false. When generating the data, hash id will be generated that will be used for deleting the data.

Data owner	File Name	Hash id	Hash code	date
Name	name	F(∂)	C1,c2,c	t_{data}

3.5 File Access

To access the data that are stored in the cloud, group member will give request as group id, data id. Cloud server will verify their signature, if the group member in the same group then allow to access file. Group member have rights to access data, but not having rights to delete or modify the data that are stored in the cloud. If any request from revoked user, cloud server won't allow accessing the data.

3.6 File Deletion

File that are stored in the cloud can be deleted by either group member (i.e., the member who uploaded the file into the server) or by group manager. It allows data owners to delete their own files that are stored in the cloud. If any delete request from the group member, cloud server will verify the signature and delete the data file that are stored in the cloud.

3.7 Traceability

Group manager will reveal their real identity in case of any dispute occurs. If any malpractice happened inside the organization it can be easily traceable. If any group members are modify or delete the data file of other groups, it can easily identify which member doing such activities.

3.8 Delta RLS

In existing RLS, revoked user details such as private key are updated manually for every day. Revoked users can access the cloud, hacking is possible. But in Delta RLS set a ttp value (threshold value), when it reaches the threshold value revoked users are updated automatically. Revoked users can't able to access the cloud hacking attack is reduced and communication overhead is also reduced.

IV. CONCLUSION

In conclusion, cloud computing is very attractive environment for business world in term of providing required services in a very cost effective way. However, assuring and enhancing security and privacy practices will attract more enterprises to world of the cloud computing In Thus to achieve the reliable and scalable in MONA, in this paper we are presenting the new framework for MONA. In this method we are further presenting how we are managing the risks like failure of group manager by increasing the number of backup group manager, hanging of group manager in case number of requests more by sharing the workload in multiple group managers. This method claims required efficiency, scalability and most importantly reliability. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well. Here we also show that how user gets extra time even after the time out this also one of the advantage of proposed schema.

REFERENCES

[1] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 41-55, 2004.

[2] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf.Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[3] D. Boneh, B. Lynn, and H. Shacham, "Short Signature from the Weil Pairing," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology, pp. 514-532, 2001.

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

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

[6] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu "Plutus: Scalable Secure File Sharing on Untrusted Storage," Pro USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[7] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[8] S.Kulkarni and Bezawada Bruhadeshwar, "Rekeying and Storage Cost for Multiple User Revocation," Department of Computer Science and Engineering, Michigan State University, East Lansing, MI48824USA.

[9] 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.

[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.