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, Issue 6, June 2014

Sharing Of Multi Owner Data in Dynamic Groups Securely In Cloud Environment

Deepa Noorandevarmath[1], Rameshkumar H .K [2], C M Parameshwarappa [3]

[1]PG Student, Dept of CS&E, STJIT, Ranebennur. Karnataka, India

[2]Assistant Professor, Dept of CS&E, STJIT, Ranebennur, Karnataka, India

[3]Professor, Dept of CS&E, STJIT, Ranebennur, Karnataka, India

ABSTRACT : cloud computing is the delivery of computing services over the Internet. Whether they realize it or not, many people use cloud computing services for their own personal needs. Here preserving the data privacy and identity privacy is somewhat difficult task in sharing a data in multi owner manner. In this paper we propose a secure multi owner data sharing schema by leveraging group signature and using dynamic broadcast encryption techniques any members can share and data with other users. And here numbers of revoked users are independent with the storage over head & encryption computation cost. In this paper the main goal is to provide the security for the data and demonstrate the efficiency of our schema in experiments.

KEYWORDS-*: cloud computing*, security analysis, identity privacy, data privacy, multi owner, dynamic groups.

I INTRODUCTION

Here before going to the main concept lets us see the meaning of cloud computing & main services offered by cloud. Cloud computing is the use of computing resources hardware and software that are delivered as a service over a network typically the Internet. Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

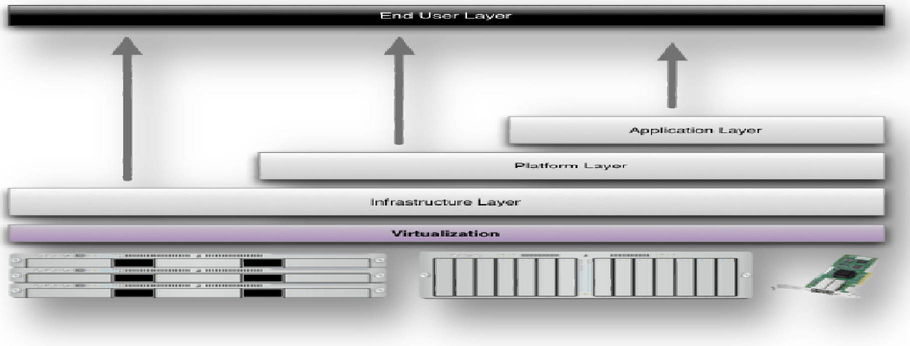

Fig 1: Structure of service models

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 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.

Objective of the paper

This paper presents a Secure Multi owner data sharing scheme, Named Mona, For dynamic groups in the cloud. By leveraging group Signature and dynamic broadcast Encryption techniques, any cloud user can anonymously share data with others.

Aim

The major aims of this method 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. 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.

II RELATED WORK

2.1 Bleumer and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi-trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security and we demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

Proxy re-encryption allows a proxy to transform a ciphertext computed under Alice's public key into one that can be opened by Bob's secret key. There are many useful applications of this primitive. For instance, Alice might wish to temporarily forward encrypted email to her colleague Bob, without giving him her secret key. In this case, Alice the delegator could designate a proxy to re-encrypt her incoming mail into a format that Bob the delegate can decrypt using his own secret key. Alice could simply provide her secret key to the proxy, but this requires an unrealistic level of trust in the proxy.

We present several efficient proxy re-encryption schemes that offer security improvements over earlier approaches. The primary advantage of our schemes is that they are unidirectional (i.e., Alice can delegate to Bob without Bob having to delegate to her) and do not require delegators to reveal all of their secret key to anyone – or even interact with the delegate – in order to allow a proxy to re-encrypt their ciphertexts. In our schemes, only a limited amount of trust is placed in the proxy. For example, it is not able to decrypt the ciphertexts it re-encrypts, and we prove our schemes secure even when the proxy publishes all the re- encryption information it knows. This enables a number of applications that would not be practical if the proxy needed to be fully trusted.

2.2 Improved proxy re-encryption schemes with applications to secure distributed storage In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called atomic proxy re-encryption, in which a semi trusted proxy converts a ciphertext for Alice into a ciphertext for Bob without seeing the underlying plaintext. We predict that fast and secure re-encryption will become increasingly popular as a method for managing encrypted file systems. Although efficiently computable, the wide-spread adoption of BBS re-encryption has been hindered by considerable security risks. Following recent work of Dodis and Ivan, we present new re-encryption schemes that realize a stronger notion of security and demonstrate the usefulness of proxy re-encryption as a method of adding access control to a secure file system. Performance measurements of our experimental file system demonstrate that proxy re-encryption can work effectively in practice.

2.3 Advantages of proposed paper

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. 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. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. 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 DESIGN

3.1 Cloud Module :

In this we create a local Cloud and provide priced abundant storage services. The users can upload their data in the cloud. We develop this module, where the cloud storage can be made secure. 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.

3.2 **Group Manager Module :**

Group manager takes charge of followings,

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

3.3 Group Member Module :

Group members are a set of registered users that will

1. store their private data into the cloud server and
2. Share them with others in the group.

Note that, the group membership is dynamically changed, due to the staff resignation and new employee participation in the company. The group member has the ownership of changing the files in the group. Whoever in the group can view the files which are uploaded in their group and also modify it . The group meme

3.4 File Security Module :

1. Encrypting the data file.
2. 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).

3.5 **Group Signature Module :**

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.

3.6 User Revocation Module :

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.

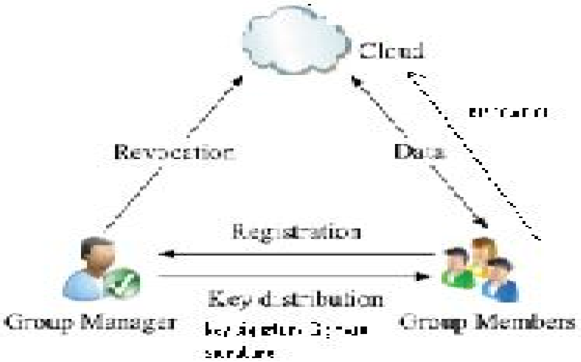

Fig 2: System design

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, Issue 6, June 2014

IV CONCLUSION

In this paper, we design a secure data sharing scheme & 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. And here numbers of revoked users are independent with the storage over head & encryption computation cost. In this paper the main goal is to provide the security for the data and demonstrate the efficiency of our schema in experiments.

REFERENCES

(1) 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.

(2) 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.

(3) 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.

(4) 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.

(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.