International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Security and Privacy Sustained Cloud Data Authentication using IDM

Tanniru Hemalatha[1], Punugoti Pavan Kumar[2]

[1, 2]Computer Science Engineering, Rise Group of Institutions, Ongole, India

Abstract: ***Cloud data sharing is an untrustworthy service where any malicious user can access the data from cloud storage and make use of it so an encryption technique is used to convert data into a unreadable format but an hacker uses an different technique to decrypt the data. So a Steganography is introducing in cloud storage centre where the group member encrypt the data and send it to the cloud server, the server receive it and hide it in to an image. Data of the different owners in the group shares data with each other securely and preserving their identity from an untrusted cloud server is one of the challenging issues currently, due to the frequent change of the membership. In this paper, we propose a secure multiowner data sharing scheme for dynamic groups in the cloud. By aid of group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. In addition to the dynamic broadcast encryption techniques we are using image Steganography to store the data in the form of image in the cloud storage.***

Keywords: Cloud computing, privacy-preserving, dynamic groups, data sharing, access control, image conversion.

1. Introduction

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Doing so may give rise to certain privacy implications.

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licences, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations.

Another potential benefit is that personal information may be better protected in the cloud. Specifically, cloud computing may improve efforts to build privacy protection into technology from the start and the use of better security mechanisms. Cloud computing will enable more flexible IT acquisition and improvements, which may permit adjustments to procedures based on the sensitivity of the data. Widespread use of the cloud may also encourage open standards for cloud computing that will establish baseline data security features common across different services and providers.

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.

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.

2. Multi-Owner Manner

Multiple-owner manner is highly recommended that any member in a group should be able to store and sharing of data services provided by the cloud. 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.

Dynamic groups is one of the challenging issue where the existing group members or newly added group member are revoked due to the fault activity done on the untrusted could. Secure data sharing extremely difficult over dynamic group.

If any new group member get registered by the group manager he may able to retrieve data files stored in cloud i.e., generating new file and store it in the cloud, because it is impossible for new group member to contact with anonymous data owners, and obtain the corresponding decryption keys. Revocation mechanism helps without updating the secret keys of the remaining group member. The revoked users are not able to access the files in the cloud.

3. Secure Sharing

Secure sharing over dynamic group with multi-owners in cloud with dual encryption technique. Several security schemes for data sharing on untrusted servers have been proposed [3], [4], [5]. The main contributions of this paper include:

1) A secure multi-owner data sharing scheme implies that any user in the group can securely share data with others by the untrusted cloud.
2) Newly registered group member can directly decrypt data files uploaded before their participation without contacting with data owners.
3) Group member revocation can be easily achieved through a revocation list which is maintained by the Group manager without updating the secret keys of the remaining group member.
4) A secure and privacy access control to a group member, which assures that any member in a group to anonymously utilize the cloud resource. Further the real identities of data owners can be revealed by the group manager when malicious activity occurs.
5) Data stored as image by using steganography which ensure that dual-encryption to provide a high data confidentiality in an untrusted cloud.

4. The Proposed Scheme

Sharing data securely over dynamic group in the cloud, we combine the group signature and dynamic broadcast encryption technique. The group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers. In this paper, a variant of short group signature is used to support member revocation. Another one is dynamic broadcast encryption technique which helps to transmit encrypted data to a set of users so that only privileged subset of users can decrypt the data.

4.1. 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:

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 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.

3) Anonymity and Traceability
Anonymity guarantees that group members can access the cloud without revealingthe 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.

4) 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.

4.2. System Model

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

1) Cloud: cloud provides storage services where in which we can store the data. But cloud is not fully trusted because many malicious activities are going through the internet which may modify or delete the data that are stored in it. So data protection scheme helps to protect the data in it.
2) Group manager: Group manager perform User registration, Key distribution, User revocation and also trace the guilty users reveal their identity. He acts as an administrator so we assume that fully trusted from others.
3) Group members: Group members are the registered user by the group manager and get the secret key from the group manager. Using the secret key group member can store their data in untrusted and share with other.

5. Scheme Description

This section describes the details of user registration, user revocation, file generation, file deletion, file access and traceability.

5.1. User Registration

Group manager receives the user identity from the new user and generate secret key [1] and distribute to the user. One part of the key is stored with the user details in cloud which is used for traceability phase. Secret key is also used for signature generation and decryption process.

5.2. User Revocation

Group manager manages the user revocation [1], [3] through revocation list maintained in cloud which is publicly available to all group members. If any group member performs a malicious activities then group manager detect those activity and user update the revocation list by adding the user detail to it. In addition group manager add signature for validation. Before generating a file group member first retrieve the revocation list from the cloud validate it and based on the number of revoked user group member can encrypt the file. For file access also retrieve revocation list

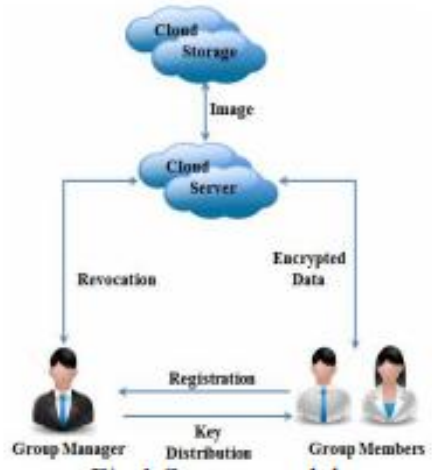

Fig.1 System model.

5.3. File Generation

Group member generate the file and encrypt it by the following operations:

1) Getting the revocation list from the cloud.
2) Verifying the validity of the received revocation list.
3) Encrypting the data file. This encryption process can be divided according to the revocation list.
4) Selecting a random number and computing the hash value will be used for data file deletion operation. In addition, the data owner adds this value with data identity into his local storage.
5) Uploading the data cloud server and adding the detail of file into the local shared data list maintained by the manager. On receiving the data, the cloud first invokes Signature Verification Algorithm [1] 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 Revocation Verification Algorithm [1].
6) Finally, after successful group signature and revocation verification the data file get converted into an image using steganography [2]. The converted image will be stored in the cloud.

5.4. File Deletion

Files in the cloud can be deleted by either the group manager or the data owner. To delete a file, Group manager computes a signature and sends the signature along with identity of data to the cloud. The cloud will delete the file if the signature is valid.

In addition to this data owner is also allowed to delete the file. Upon receiving the deletion request, the cloud calls the Signature Verification and Revocation verification algorithms to verify the group signature. After successful group signature verification, the cloud will delete the data file if requested hash value equals to the hash value contained in the file.

5.5. File Access

To access the file in cloud among the group members following action to be perform:

1) Group member request the cloud for data file and revocation list. In this operation the group member first compute the signature using his private key on the message which includes identity of the file, this can obtained by locally available file list maintained by the group manager in the cloud. Then, the group member sends the request to the cloud server.
2) Upon receiving the request the cloud server verify the validity of signature in the request by in invoking the Signature Verification Algorithm [1].
3) After successful verification, the cloud server get the image of identity which is equal to the Identity of data and convert into data file format and respond back to the group member along with revocation list.
4) Group member then verify the validity of the received revocation list. First, check whether the marked date is fresh. Second, verifying the contained signature. If the revocation list is invalid; the data owner stops this scheme. 3) Now group member must verify the validity of the file and decrypting it this operation is divided according to the time stamp and the revocation list.

5.6. Traceability

When a malicious activity occurs, the group manager identifies the real identity of the data owner. Given a signature the group manager use his private key to compute some portion of secret key of the user, the group manager can look up the user list to find the corresponding identity.

6. Conclusion

In this paper, data owner share their data among the group in untrusted cloud server with a dual encryption. In This paper, a group member is able to share the data with others in the group without revealing their identity. Group manager maintaining the revocation list in which the dispute occur by the members are added in to this list. Using this list the Group member can encrypt and decrypt the data file which they want to share with others. In addition to this steganography concept is added to convert the encrypted data into a image to perform high confidentiality of data sharing in cloud. So this concept provide an high security, confidentiality and efficiency

References

[1] Xuefeng Liu and Yuqing Zhang,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud",IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL.24, NO.6, JUNE 2013.
[2] Vijay Kumar Sharma, Vishal Shrivastava, "A Steganography Algorithm For Hiding Image In Image By Improved LSB Substitution By Minimize Detection" Journal of Theoretical and Applied Information Technology 15th February 2012. Vol. 36 No.1
[3] M. Kallahalla, E. Riedel, R. Swami Nathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on

Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003

[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] 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.