INTERNATIONAL JOURNAL OF RESEARCH IN COMPUTER APPLICATIONS AND ROBOTICS
ISSN 2320-7345

PRESERVING SECURITY AND PRIVACY TO DATA OF MULTIPLE OWNER GROUP IN THE CLOUD

Dinesh Babu Junuthla[1], Mr.CT. Kiran Kanth[2]

[1] *PG Scholar, Department of Computer Science, AVN College of Engineering and Technology, JNTUH Hyderabad, Telangana, India*
[2] *Assistant Professor, Department of Computer Science, AVN College of Engineering and Technology, JNTUH Hyderabad, Telangana, India*
[1]***dinichary@gmail.com,*** [2]***kirankanth.ct@gmail.com***

Abstract:

Cloud computing is an emerging computing paradigm in which resources of the computing are provided as services over the Internet. The cloud computing services besides serving in an efficient manner it also consists of some challenging issues. Proving security to multi owner data while preserving data and identity privacy from unauthorized users cloud is still a big challenging issue. In dynamic groups the members may frequently join into it or they may leave at any time, hence there is a need to have a robust system to protect the data from the unauthorized access from the cloud. To provide privacy and security to the stored data in the cloud it has to be encrypted and the decryption keys to be shared to only some set of authorized users only. When ever the new user register into the group the group manages has to provide access permissions to read the existing data present in the cloud.. This paper provides the reliability as well as improving the scalability by increasing the number of group managers dynamically. The storage overhead and encryption and decryption keys computation cost of our scheme are independent with the number of revoked users.

In cloud these resources are shared among different geographical locations, in order to preserve security and privacy, the users are divided into some groups and the data decryption permissions are given to the only the set of users present in that particular group.. Multiple users share their data in the cloud network. In cloud computing the groups are dynamically changes. As the group members are changing frequently it became a challenge to secure data of multi owners from the revoked users. The users present in other groups are not allowed to access the data from other group members shared information.

Keywords: cloud computing, encryption, cryptography, group signature, dynamic groups, revocation.

Introduction

Cloud Computing

Cloud computing is the next stage in the Internet's evolution, providing the means through which everything from computing power to computing infrastructure, applications, business processes to personal collaboration can be delivered to you as a service wherever and whenever you need.

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand.

The cloud isn't a technology. It's more of an approach to building IT services - an approach that harnesses the power of servers, as well as virtualization technologies that combine servers into large computing pools and divide single servers into multiple virtual machines. And there are several different deployment models for implementing cloud technology.

The four primary types of cloud models are:

- Public
- Private
- Hybrid
- Community

Each has its advantages and disadvantages with significant implications for any organization researching or actively considering a cloud deployment.

Public Cloud
A public cloud is a cloud computing model in which services, such as applications and storage, are available for general use over the Internet. Public cloud services may be offered on a pay-per-usage mode or other purchasing models. An example of a public cloud is IBM's Blue Cloud.

Private Cloud
A private cloud is a virtualized data center that operates within a firewall. Private clouds are highly virtualized, joined together by mass quantities of IT infrastructure into resource pools, and privately owned and managed.

Hybrid Cloud
A hybrid cloud is a mix of public and private clouds.

Community cloud
A community cloud is an infrastructure shared by several organizations which supports a specific community.

Issues in Cloud Computing

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, Lu et al. proposed a secure provenance scheme based on the cipher text-policy attribute-based encryption technique, which allows any member in a group to share data with others. However, the issue of user revocation is not addressed in their scheme. Yu et al. presented a scalable and fine-grained data access control scheme in cloud computing based on the key policy attribute-based encryption (KP-ABE) technique. 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 proposed a scheme to secure data shared by multiple owners in the groups. The main contribution includes:

1. We propose a scheme to secure data shared by multiple owners in the cloud. This scheme provides reliability and confidence to store and share data in cloud.
2. The group manager has to provide access permissions to the newly registered users. Without the access permissions the new user is not allowed to access the data in the cloud.
3. When a user revoked from the group then there is no need of updating the remaining users security parameters.
4. The real identity of the users is revealed when only the dispute occurs in the cloud. Without any dispute the identity will not be disclosed to outside world.
5. The group manager updates the revocation list frequently and make available to the users, to know revocation status.

Related Work

Kallahalla et al. proposed a cryptographic storage system that enables to secure file sharing on untrusted servers. In this approach the file is divided into file groups and encrypted each group with a file-block key. However, it brings about a heavy key distribution overhead for a large scale file sharing.

Ateniese et al. leveraged proxy re encryptions to secure distributed storage. The data owner encrypts blocks of data content with unique and symmetric content keys, which are further encrypted by master encrypted key. However it suffers from collusion attack.

Xuefeng Liu proposed a system, secure multi owner data sharing for dynamic groups in the cloud. It provides efficient security mechanism by providing group signature and individual signature. Group signature is to encrypt the data and individual signature key to decrypt the data from the cloud storage. However the newly admitted users can directly access data stored in the cloud without any access permissions from the data owner.

From the above analysis, we observe that need of an approach to provide privacy and in the cloud storage.

1. Any user of the group can share and store his/her own data with other members in the same group securely without fear of losing data confidentiality.
2. Encryption complexity and size of the cipher text are independent with the number of users in the group.
3. User revocation is achieved without updating the private keys of all the group members.
4. A newly registered user must have access permission from the group manages before accessing the data from the cloud.
5. Revoked users status is updated frequently, and made available to the users in the group
6. Other group members are strictly prohibited from accessing data.

Preliminary Requirements

Group Signature

Group Signature is based on the Strong Diffie-Hellman assumption. It allows users to sign without revealing the original identity to the group members. If any dispute activity occurs then the group manager can reveal the real identity of disputed group member. Group Signature achieves access control and efficient member revocation.

Dynamic Groups

The data owners can broadcast the encrypted data to all the group members. Group members can decrypt the data using their own decryption keys. New members can dynamically join into the groups and they can leave at any time from the group. The existing users decryption keys need not be updated when the new user is registered or revoked from the group.

Broadcasting Encrypted data

A broadcast scheme allocates keys to the group members so that they can encrypt the data using a common key and decrypt the data with their own private decryption keys. The final goal of broadcast encryption scheme is to securely transmit the data to all privileged subset of all the group members.

Architecture

Consider a cloud computing architecture by comparing with a company cloud to enable its employees to access data from their own cloud. Here each team is considered as a separate group. The head of the team is considered as group manager and team members are the group members. The team members are allowed to share their ideas in their own team (group) and the other members in the same group are allowed to access that information from the cloud. Here the cloud consists of three different entities

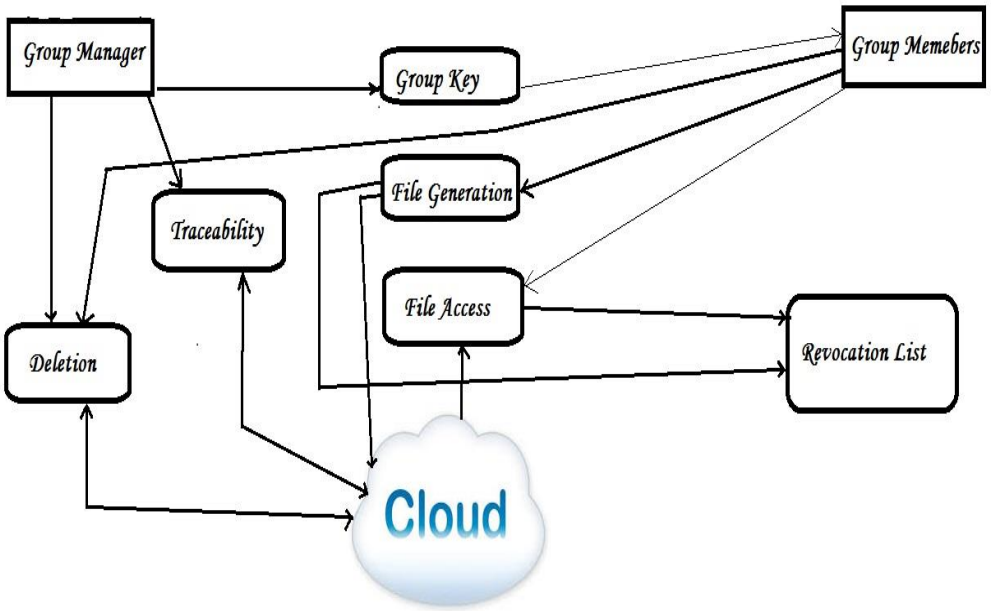
They are:

1. The cloud
2. The group manager and
3. Group members

Cloud: Cloud is operated by cloud service provider. The cloud service providers are outside the trusted domain so cloud is not fully trusted because and they may try to learn the content of the data shared in the cloud. The cloud service will not try to delete or modify the user data in the cloud.

Group Manager: Group manager is responsible for monitoring the entire group in the cloud**.** Group manager is responsible for user registration, user revocation, signature distribution, and revealing the real identities of the dispute data owners.

Group Members: Group members are the individual users. They can store and share their own data in the cloud. This stored data is encrypted in order to protect from the unauthorized usage. These users may dynamically change the groups. Existing user may leave the group and new user can join the group at any time.



System Architecture

Registration of a user:

Suppose the user *i* want to register with ID_i, the group manager will randomly select three integer numbers such as P, Q, x_i ,α,Z. Using these values the following values are generated

$$A_i = \frac{1}{\alpha + xi}.P$$

$$B_i = \frac{xi}{\alpha + xi}.Q$$

The group manager adds (A_i ,x_i,ID_i) into the group member list, it is used in the traceability phase. (x_i,A_i ,B_i) is used for group signature generation and private key to decrypt the information present in the cloud.

Revocation:

Member revocation is performed by group manager to provide confidentiality to the data from other members of the cloud. The group manager updates the revocation list time to time and make available to the group members. The revoked users list is indicated by set of time stamps indicates the time of revocation. The table is appended by time of updating and signature of the group manager.

Revoked user details

Group Id:ABCD1234

A_1	X_1	T_1
A_2	X_2	T_2
A_3	X_3	T_3
.	.	.
A_n	x_n	T_n

File Generation:

The group member performs the following operations to store and share the data files in the cloud. A file is generated and it is uploaded into the cloud. Whenever the user uploading the file, the system has to generate one key. This key is used when deleting a file from the cloud.

File deletion

In order to delete the files from the cloud there are two ways. The group member can delete the file his own with using the key generated at the time of uploading the file into the cloud. The second way is the group manager can also delete the file from the cloud directly.

File Access:

In order to access the information provided in the cloud the user need to follow these steps.

1. The member needs to get the revocation list from the cloud. Revocation list contains revoked users of the group and updated time along with the authorized signature of the group manger.

2. The cloud verifies the signature and provides revocation list to the member.
3. Verifies the validity of the revocation list.
4. Verify the validity of the information file and decrypt the data using his/her private key

Traceability:

The identity of the group members is kept confidential from the other users or outside the world. When ever a dispute occurs in the cloud then the responsibility of the group manger to trace the dispute users in the cloud. The group manager then reveals the real identity of the dispute user.

Conclusion

In this scheme will not reveal the identity of the group member until any dispute occurs. The group manager can reveal the real identity of the dispute member. This scheme provides information for efficient member revocation without any security threat to the data owners and new member joining. The newly registered users need to get access permissions from the group manager to know the data present in the cloud. The member present in one group is not allowed access the data from other groups. Here is no need of computing the new parameter to the existing members when a member is revoked from the group.

REFERENCES

1. Xuefeng Liu, 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. A. Fiat and M.Naor , "*Broadcast Encryption*" Proc.Int,l Cryptology Conf.advances in cryptology (CRYPTO), pp.480-49,1993.
3. SenyKamara, Kristin Lauter "*Cryptographic Cloud Storage*" Microsoft research cryptography group.
4. D.Boneh, X.Boyen, and H.Shacham, "*Short Group Signature*" Proc.Int'l Cryptography and Advances in Cryptology (CRYPTO) pp.41-55,2004
5. M.Kallahalla, E.Riedel, R.Swaminathan, Q.Wang, and K.Fu, "*Plutus: Scalable Secure File Sharing on untrusted Storage"*, Proc. USENIX Conf.Fileand Storage Technologies, pp.29-42,2003.
6. S.Yu, C.Wang, K.RenandW.Lou, "*Achieving Secure , Scalable, and fine Grained Data Access Control in Cloud Computing* " Proc. IEEE INFOCOM, pp.534-542, 2010.
7. D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol. 13, no. 3, pp. 361-396, 2000.
8. 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.