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

PROVIDING SECURITY TO MULTI OWNER GROUPS IN CLOUD

Ramesh Sriramula[1], Dr. G. Venkata Rami Reddy[2]

[1] PG Scholar, Department of Computer Science, School of Information Technology, JNTUH Hyderabad, Telangana-500085, India
[2] Associate Professor, Department of Computer Science, School of Information Technology, JNTUH Hyderabad, Telangana-500085, India
[1]sriramramesh85@gmail.com, [2]gvr_reddi@yahoo.co.in

Abstract:

Cloud Computing is an emerging computing trend in which resources are shared over the network. Cloud computing shares resources to all the geographical locations over the internet. Cloud Computing provides remote storage of resources from the data owners. As providing many benefits such as global access and cost effective it also suffers from some challenging issues such as security and access control. Existing mechanisms usually apply encryption methods in Cryptographic technologies and the decryption keys are shared to the authorized members.

In cloud these resources are shared among different locations, in order to preserve security, the users are categorized into some groups and the data is shared to only those group members with a group signature. 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.

Keywords: cloud computing, cryptography, group signature, dynamic groups, revoked users.

Introduction

Cloud Computing

Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications. Cloud Computing became as an alternative to the traditional storage of data in information technology due to its features and services such as software as a service, infrastructure as a service, platform as a service and etc.. By using these intrinsic features of cloud computing paradigm the cloud users are enjoying quality services and significant investment saving.

Cloud data storage is one of the important features of the cloud computing. Cloud storage is away from the data owners and changes from one location to another location. This may lead to some risks to the privacy of the data stored in cloud. The cloud data managed by the cloud service providers is not trusted by the cloud users. To achieve data confidentiality and privacy the data is encrypted with cryptographic technologies

and placed in the cloud. But it became a challenging task to preserve data from the dynamic groups in the cloud. To designing an appropriate data sharing scheme the following challenging issue should be taken into account.

Identity privacy is one of the challenging issue in the cloud computing. In cloud storage all users can share data and get access to the data provided by the other users as well. If the cloud service provider not provide an efficient way to trace the real identity, other users unwilling to join in the cloud computing system because their real identity may disclosed to other attackers.

Second challenging issue deals about that any group member in a cloud should be able to enjoy the sharing and access services by the group. In a group any number of members can share their data in the cloud storage, thus it leads to multi owner approach. Each group is maintained a member, called as group manager. Group manager has the privilege to modify data and distribute the permissions among all the users in the group. Each member in a group is able to read the data and can change his/her part of the data in the cloud.

Groups are normally dynamically changes e.g. new employees may join in the company and old employees may resign to their post hence securing the data of the cloud from the revoke users is a challenging task. The newly joined members should be given access permissions by the group manager and the revoked users list need to be maintained to ensure access control to the data stored in the cloud network.

Several schemes are proposed to secure the data from unauthorized users and preventing the cloud servers learn from the stored data, because they don't have much knowledge about the decryption keys. The complexities of user joining and removing in the schemes are increasing linearly number of data owners and number of revoked users in the cloud computing.

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 of multi-owners in the cloud. The users in the group can share their data without any fear of losing data confidentiality.
2. A newly joined user can access the data after gaining access permission from the group manager without waiting for the data owner to grant the access permissions.
3. User revocation is achieved without updating the secret keys of the remaining users.
4. The real identity of the users is not revealed to the outside world unless a dispute occurs.
5. Revocation list is updated frequently and given access to the group members to know about revocation list 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 to encrypt the data and private key to decrypt the data from the cloud storage. However the newly admitted users can directly access data.

From the above analysis, we observe that need of an approach to store the data securely 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.

Preliminaries

Group Signature

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

Dynamically changing Groups

The data owners can broadcast the encrypted data to the group members. Group members can decrypt the data using their own private 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 modified when the new user is registered.

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 members.

Architecture

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

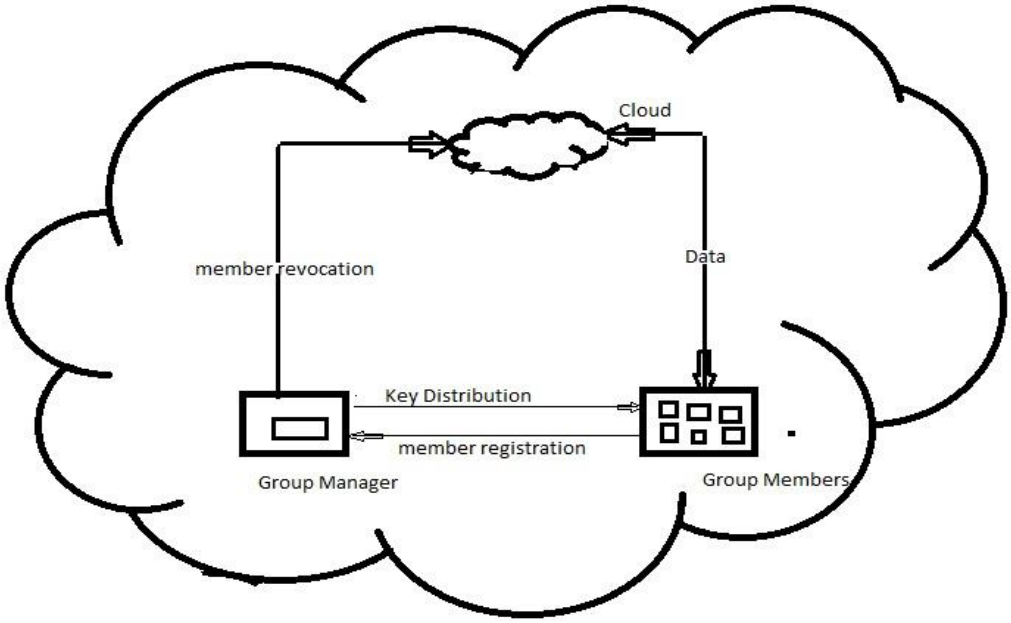
They are:

1. The cloud (college cloud)
2. The group manager (head of the department) and
3. Group members (students in the college)

Cloud: cloud is operated by cloud service provider. Cloud is not fully trusted because the cloud service providers are outside the trusted domain 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.\

Group Manager: 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 encrypt their private information, store the data in the cloud and share the data among the group members. These users dynamically changes. Existing user may leave the group and new user can join the group at any time.



System Architecture

Design Goals

The goals of this scheme are data confidentiality, access control, efficiency, anonymity and traceability.

Data Confidentiality: It states that unauthorized users are not allowed to access data present in the cloud. The newly registered users are allowed to access the information after gaining access permissions from the group manager and the revoked members are not allowed to access the information.

Access Control: the group members are allowed to use all operations provided by the cloud. The registered users are allowed to access the information present in the cloud with their respective decryption keys and the revoked users are not allowed to access the information.

Efficiency: All the members of the groups in the cloud are able to store and share their information. User revocation can be done without involving the other users in the group. There is no need of again calculating the private key to decrypt the data for the existing users.

Anonymity and identifying dispute user: Anonymity states that the group member's identity is not revealed to others. Dispute user is identified at the time of dispute in the cloud. The group manager has the privilege to reveal the real identity of the dispute member.

User Registration:

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

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

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

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

Member 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:A123d5

K_1	**X_1**	**T_1**
K_2	**X_2**	**T_2**
K_3	**X_3**	**T_3**
.	.	.
K_n	**x_n**	**T_n**

Updated time: 12.00 **Signature: abc**

File Generation:

The group member performs the following operations to store and share the data files in the cloud.

1. The group member needs to get the revocation list. In order to get the list the member need to send his/her ID to the cloud then the cloud verify the ID and send the revocation list.
2. The member needs to verify the revocation list and encrypt the data file. The encryption process is carried in two ways. They are
    1. There is no revoked users in list
        i. Select a unique data identity ID_{data}
        ii. Choose a random integer numbers n
        iii. Perform encryption as follows

$C_1=n.L$

$C_2=n.P$

$N=Z^n$

$C=Encrypt_N(File)$.

    2. There are r number of revoked users in the list
        i. Select a unique data identity ID_{data}
        ii. Choose a random integer number n
        iii. Perform encryption as follows

$C_1=n.L$

$C_2=n.P$

$N=Z_r^n$

$C=Encrypt_N(File)$.

$Z_r$is calculated as

$$M=\frac{1}{(\alpha+xi)(\alpha+x2)\ldots\ldots(\alpha+xr)}$$

$$Z_r=Z^M$$

3. Selecting a random number μ and computing a hash value, this hash value is used for deleting the file from the cloud. The data owner adds (ID_{data},μ) to cloud storage.

4. Create a table of uploaded information files

Uploading data table format

Group ID	Data ID	time	ciphertext	hash	signature
$ID_{grouop1}$	ID_{data1}	T1	C1	F(μ1)	S1
ID_{group2}	ID_{data2}	T2	C2	F(μ2)	S2
ID_{group3}	ID_{data3}	T3	C3	F(μ3)	S3

File deletion

The files stored in the cloud by the group members can be deleted by two ways. The data owner can delete his/her own file using ID_{data} and hash value generated by him at the time of file uploading. The group manager can also delete the data file using ID_{data} and his signature to the cloud.

Algorithms

1. **Generating Signature**

Input: private key (A, x) and parameters (P,Q,R,S,T) and data D
Output: group signature on data D
begin
Choose random integer numbers a,b,c,d,e,f,g
Compute d1=xa and d2=xb
Calculate the following values

$X_1=a.Q$
$X_2=b.R$
$X_3=A_i+(a+b).S$
$Y_1=c.Q$
$Y_2=d.R$
$Y_3=r_x.X1-r_{d1}.Q$
$Y_4= r_x.X2-r_{d1}.R$

$c=f(D,X_1,X_2, X_3, Y_1, Y_2, Y_3, Y_4)$

Calculate the following numbers

$K_a=r_a+ca$

$K_b=r_b+cb$

$K_x=r_x+cx$

$K_{d1}=r_{d1}+cd1$

$K_{d2}=r_{d2}+cd2$

Return $\alpha=(X_1, X_2, X_3, c, K_a, K_b, K_x, K_{d1}, K_{d2})$

End

2. **Verifying Signature**

Input: parameters (P, Q, R, S, T), data D and Signature $\alpha=(X_1, X_2, X_3, c, K_a, K_b, K_x, K_{d1}, K_{d2})$

Output: true or false

Begin

Calculate the following values

$M_1=K_a.Q-c.X_1$

$M_2=K_b.R-c.X_2$

$M_3=K_x.X_1-K_{d1}.Q$

$M_4=K_x.X_2-K_{d2}.R$

If $c=f(D, X_1, X_2, X_3, M_1, M_2, M_3, M_4)$

Return **true**

Return **false**

End

3. **Verifying revocation**

Input: parameters (H_0, H_1, H_2) a group signature and set of revocation keys

Output: true or false

Begin

set $z=e(X_1,H_1)\ e(X_2,H_2)$

for i= 1 to n

if $e(X_3-A_i,H_0)=z$

return**true**

end if

end for

return false

end

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 information file and revocation list from the cloud. The member sends a data request containing (ID_{group}, ID_{data},timestamp, signature). The cloud verifies the signature and provides revocation list to the member.
2. Verifies the validity of the revocation list.
3. Verify the validity of the information file and decrypt the data using his/her private key

Traceability:

The group member's identity is kept secret from other members in the cloud. But if any data dispute occurs it is the responsibility of the group manager to reveal the real identity of the user. Group manager takes the signature and lookup the table to identify the real dispute owner.

Conclusion

In this scheme the data is stored and shared in the cloud without revealing the identity of the original data owner. The group manager can reveal the real identity of the dispute member. This scheme provides efficient member revocation and new member joining. Whenever a new user wants to store the data, he/she can get the revoked users list and encrypt the data depending on the list. A newly joined user can access information without taking the permission of the data owner, but need to have permission with the group manager.

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.