Privacy Preserving Data Sharing Scheme for Group Users in Simulated Cloud

Saranya C, Vinoth P

***Abstract*— Now a days, Cloud Computing has become the easiest and efficient way of data storage management. As it requires low maintenance, it is more preferable than normal local storage .One of the challenging issue is that sharing of data in the untrusted cloud with privacy of data and identity is complex. This is because the groups are often dynamic, that is there will be an often change in the membership. The solution for the above problem is that a privacy-preserving data sharing scheme was proposed for the dynamic group users in the cloud. It uses the short signature scheme and dynamic broadcast encryption techniques. This data sharing scheme can provide sharing services along without affecting the privacy of the data. Therefore, through this sharing scheme the dynamic group user can share data at low storage and communication overhead and also with low encryption computation cost.**

***Index Terms*— cloud, data privacy, identity-privacy, multi-owner data sharing, privacy-preserving.**

I. INTRODUCTION

Cloud computing grew out of our never-ending hunger for ever-faster and ever-cheaper computation [1]. As this technology enables a resource-sharing and low cost feature, it was widely accepted and recognized for usage. Many public cloud services like Amazon offers the cloud services at lower cost and high quality. Thus, the internet users gradually move from the local data management to the cloud data management. Here, the storage services offered by the cloud service provider is upcoming service has some challenges in case of the data sharing among the dynamic groups in the cloud. That is, if there exists a group or department, which want to store and share a data in the cloud. However, the integrity of stored data should be preserved because the data will be highly confidential and sensitive data .Usually encrypting data is one of best way to preserve the integrity but in case of data sharing among a group of users is extremely difficult in the key management, especially while dealing with dynamic groups. Therefore, there is a need for a completely privacy-preserving data sharing scheme for group users in the cloud.

Manuscript received May, 2014.

***Saranya C**, PG Scholar, Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, TamilNadu, India.*

***Vinoth P**, Assistant Professor, Department of Computer Science and Engineering, Mepco Schlenk Engineering College, Sivakasi, TamilNadu, India.*

The following are some of the issues while designing such a scheme; the first issue is that the identity privacy, the cloud users will be afraid of joining the cloud where the real identity of the user may be disclosed to the attackers easily. And also if the identity privacy is unconditional then it is difficult to find if any users or staffs in the group misbehaves on the sharing of data. Therefore, the scheme should support the traceability of the real identity.

The next problem is that every member in the group should enjoy the entire services offered by the cloud, which is not to have single-owner manner. In Single-Owner manner only the group manager can store and manipulate the data stored in the cloud. The other group members can only read the shared data but they cannot modify the data shared with them. So, the data sharing scheme should support multi-owner manner.

The final challenge is that often the groups are dynamic in nature, that is a new user may be added to a group or a existing user may be revoked from the group or organisation. It is not possible for the new users to read the data that are shared before his participation, as the key used before should be retrieved from the owner is extremely difficult.

Also, to reduce the key management complexity, the revocation mechanism should be able operate without the updating the secret keys of other users.

Many secure data sharing schemes for the untrusted servers was proposed previously, here the data stored in the cloud are encrypted and the decryption keys are distributed among those share that data file .Only the authorized group member will be provided the decryption key but however the complexity of new member registration and user revocation increases rapidly when the data owner and the revoked users increases.

The main goal of this privacy-preserving data sharing scheme are to

1. Allow any authorized users in the cloud to securely share data with others in the group.
2. Provide secure and privacy-preserving access control to users.
3. Support the dynamic groups efficiently in the cloud.
4. Reveal the real identities of the user when any dispute occurs.

The rest of the paper is organized as follows: Section 2 describes the research background and related work. Section 3 describes the data sharing system architecture and the techniques used. Section 4 describes the scheme description and the algorithms. Section 5, presents the performance of the experimental results. Finally, concluded the paper in Section 6.

ISSN: 2278 – 1323

II. RELATED WORK

In [3] Yu et al. proposed a key policy attribute-based encryption (KP-ABE) data access control scheme [9] The data owner uses a random key to encrypt a file and the random key is encrypted with a set of attributes. The group manager assigns an access structure and the corresponding secret key to authorized users, such that if the file attributes satisfy the access structure a user can only decrypt a cipher text. The drawback, it supports only the single-owner manner.

Lu et al. [7] proposed a scheme based on the cipher text policy attribute-based encryption technique [8].In [4] a secure file sharing technique called Plutus was proposed by Kallahalla et al., here files are divided into file groups and each such group is encrypted with a unique key. A lockbox key is used encrypt the file-block keys and these keys are shared with the file groups. The drawbacks are heavy key distribution overhead and often the file-block key is to be updated for each user revocation.

In [5], files include two parts: file metadata and file data are stored on the cloud server. The file metadata is the access control information that includes a series of encrypted keys, each of which is encrypted using the public key. The user revocation is an issue for large cloud sharing, since the file metadata is also to be updated.

Ateniese et al. [6] proposed proxy re-encryptions to secure storage. The data owner encrypts blocks with content keys, which are encrypted by a master public key. For access control, server directly re-encrypts the content keys from the master public key to a granted user's public keys. Here, the drawback is a collusion attack between the server and any revoked user, which lead to the reveal of decryption keys of all the encrypted blocks.

From this we can provide a secure scheme but the preserving identity privacy from an untrusted cloud remains to be a challenging issue. The privacy-preserving data sharing in cloud propose a method for secure data sharing in cloud computing. It offers features as follows:

- Achieve privacy-preserving data sharing with access control and data confidentiality.
- Reduced encryption complexity.
- Anonymity and Traceability.
- User revocation achieved without updating the private key of remaining users.

III. ARCHITECTURE AND TECHNIQUES

Data sharing architecture for outsourced data in clouds is shown in Fig. 1.Consider for example a company with many departments of staffs. Each department acts as a group and the staffs in each department are the members of the group. The manager of the company is the group manager who has the right to decide which data file to be shared and accessed to which group. This architecture of data sharing consists of three entities. The entities are the Group Manager, Group Members and the Cloud.

- Cloud

  Cloud provides data storage service and has enough storage space and computation resources. It is operated by the Cloud Service Provider (CSP).Cloud Server is honest but curious and try to learn about data and identities stored in the cloud.

- Group Manager

  Group Manager performs the system initialization, user registration, user revocation and traceability of real identity of dispute user.

- Group Members

  Group members are the authorized users who store data in the cloud and share to other users in the group.

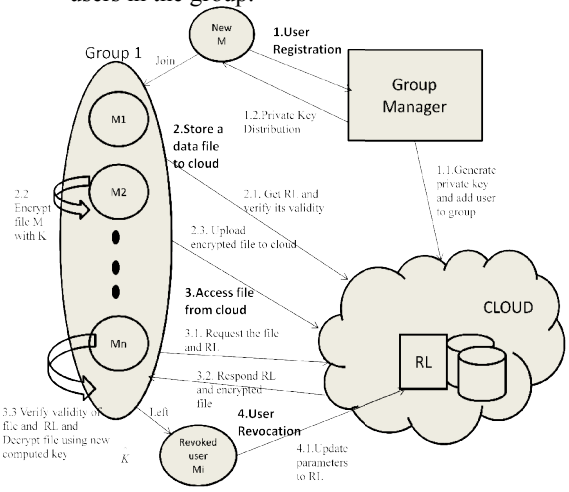

Fig. 1. Privacy-Preserving Data sharing architecture.

The entire goal of this scheme is to provide the access control, data confidentiality, anonymity and traceability in cloud.

Access Control: Authorized users can access the data stored in the cloud and the unauthorized and revoked users should not able to access the cloud.

Data Confidentiality: Data stored in the cloud must not be revealed to other including the cloud. Data is disclosed only to the granted users of the group.

Anonymity: The real identity of the group members is not revealed to other users of group in the cloud.

Traceability: Group manager should be able to trace and reveal the real identity of the user if any dispute occurs.

This scheme involves the following algorithms: *Group Signature Generation, Group Signature Verification, User Revocation Verification,* and *Parameters Computing* algorithms. The techniques used in this scheme are Bilinear Maps, Group Signature, and Dynamic Broadcast Encryption.

3.1 Bilinear Maps

Let G1 and G2 be the additive cyclic group and a multiplicative cyclic group of same prime order *q*. Bilinear map is given by

$$e : G_1 \times G_2 \rightarrow G_T$$

The Bilinear map constructed should satisfy the following properties

1. Bilinear: $\forall a, b \in Z_q^* \quad P, Q \in G_1$

$$e(aP, bQ) = e(P, Q)^{ab}$$

2. Non-degenerate :If there exists a point P such that $e(P,P) \neq 1$

3. Computable : There is an efficient algorithm to compute $e(P,Q)$ for any $P,Q \in G_1$

3.2 Group Signature

Chaum and van Heyst [10] introduced the concept of group signature; it allows any members can sign the messages. So, the identity of the signature originator is not known to others. If any dispute occurs then the group manager runs the traceability phase and can reveal the identity of the malicious user.

3.3 Dynamic Broadcast Encryption

In broadcast encryption , the data is send to all users but only granted users can decrypt the data. In, dynamic broadcast encryption the group manager can dynamically add new users by also preserving the earlier decryption keys and the size of the cipher text remains constant. The bilinear pairing technique is used to implement this dynamic broadcast encryption for data sharing in dynamic groups.

IV ALGORITHMS FOR DATA SHARING SYSTEM

The algorithm for the data sharing process are as follows

1. *Group Signature Generation Algorithm*

Algorithm Group Signature Generation
//**Input:** private key (A ,x)
system parameter (P,U,V,H,W)
data M
//**Output:** Valid group signature on M.
begin
Select random numbers $\alpha, \beta, r_\alpha, r_\beta, r_x, r_{\delta_1}, r_{\delta_2} \in Z_q^*$
Set $\delta_1 = x\alpha$ and $\delta_2 = x\beta$
Compute the values of $T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5$

$T_1 = \alpha.U$
$T_2 = \beta.V$
$T_3 = A_i + (\alpha + \beta).H$
$R_1 = r_\alpha.U$
$R_2 = r_\beta.V$
$R_3 = e(T_3, P)^{r_x} e(H.W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}}$
$R_4 = r_x.T_1 - r_{\delta_1}.U$
$R_5 = r_x.T_2 - r_{\delta_2}.V$

Set $c = f(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5)$

Construct the following numbers

$$s_\alpha = r_\alpha + c\alpha$$
$$s_\beta = r_\beta + c\beta$$
$$s_x = r_x + cx$$
$$s_{\delta_1} = r_{\delta_1} + c\delta_1$$
$$s_{\delta_2} = r_{\delta_2} + c\delta_2$$

return $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
end

2. *Group Signature Verification Algorithm*

Algorithm Group Signature Verification
//**Input:** system parameter (P,U,V,H,W)
data M
signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$
// **Output:** True or False
begin
Compute the following values

$\tilde{R}_1 = s_\alpha.U - cT_1$
$\tilde{R}_2 = s_\beta.V - cT_2$
$\tilde{R}_3 = (e(T_3,W)/e(P,P))^c e(T_3,P)^{s_x} e(H,W)^{-s_\alpha - s_\beta} e(H,P)^{-s_{\delta_1} - s_{\delta_2}}$
$\tilde{R}_4 = s_x.T_1 - s_{\delta_1}.U$
$\tilde{R}_5 = s_x.T_2 - s_{\delta_2}.V$

if $c = f(M, T_1, T_2, T_3, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5)$
return true
else
return false
end

3. *Revocation Verification Algorithm*

Algorithm Revocation Verification
// **Input:** system parameter (H_0,H_1,H_2),
group signature σ
set of revocation keys $A_1,\ldots,A_r$
// **Output:** Valid or Invalid
begin
set temp =$e(T_1,H_1)e(T_2,H_2)$
for i=1 to n
if $e(T_3 - A_i, H_0) = temp$
return Valid
end if
end for **return** Invalid
end

4. *Parameters Algorithm*

Algorithm Parameters Computing
//**Input:** The revoked user parameters
$(P_1, x_1), \ldots, (P_r, x_r)$
private key (A,x)
//**Output:** $A_{r,r}$ or NULL
begin
set temp = A
for λ = 1 to r
if x = x_λ **return** NULL
else **set** $temp = \frac{1}{x - x_\lambda}(P_\lambda - temp)$
return temp

end

V CONSTRUCTION OF THE DATA SHARING SCHEME

This scheme provides a privacy preserving method to ensure the confidentiality of data stored in the cloud is securely shared among the dynamic groups.

4.1 Overview

The cloud multi-owner data sharing framework has the following processes: Construction of

1. Group User's Management
2. File Management
3. Traceability

4.2 Group user's Management

It consists of 3 phases

4.2.1 System Initialization

Group manager initializes the system.

i. A bilinear map group system $S = (q, G_1, G_2, e(.,.))$ is generated.

ii. Select 2 random elements $H, H_0 \in G_1$ along with 2 random numbers $\xi_1, \xi_2 \in Z^*_q$ and compute U and V and also H_1 and H_2

$$U = \xi_1^{-1} H$$
$$V = \xi_2^{-1} H \in G_1$$
$$H_1 = \xi_1 H_0$$
$$H_2 = \xi_2 H_0 \in G_2$$

iii. Choose 2 random elements $P, G \in G_1$ and a number $\gamma \in Z_q^*$ and compute W,Y and Z.

$$W = \gamma . P, Y = \gamma . G, Z = e(G, P)$$

iv. Publish the system parameters

$(S, P, H, H_0, H_1, H_2, U, V, W, Y, Z, f, f_1, Enc())$

$f : \{0,1\}^* \rightarrow Z_q^*$

$f_1 : \{0,1\}^* \rightarrow G_1$ hash functions

$Enc_k()$ secure symmetric encryption with secret key k.

4.2.2 User Registration

Group manager adds the user into the group user list.

i. Select a number $x_i \in Z_q^*$ and computes

$$A_i = \frac{1}{\gamma + x_i} . P \in G_1$$

$$B_i = \frac{x_i}{\gamma + x_i} . G \in G_1$$

ii. Group manager adds (A_i, x_i, Id_i) in the group user list.

iii. After registration, each user i is given a private key (x_i, A_i, B_i).

4.2.3 User Revocation

It is performed by group manager using publicly available Revocation list (RL), using this others can encrypt their data and ensure confidentiality against revoked users.

TABLE1RevocationList

Id_{group}	A_1	x_1	t_1	P_1			
	A_2	x_2	t_2	P_2			
		.	.	.	.		
	A_r	x_r	t_r	P_r	Z_r	t_{RL}	sig(RL)

Table1 shows the revocation list and it has the time stamps (t1<t2<t3....tr), ID_{group} is the group identity. $P_1, P_2, ... P_r$ and Z_r are calculated,

$$P_1 = \frac{1}{\gamma + x_1} . P \in G_1$$

$$P_2 = \frac{1}{(\gamma + x_1)(\gamma + x_2)} . P \in G_1$$

$$P_r = \frac{1}{(\gamma + x_1)(\gamma + x_2)...(\gamma + x_r)} . P \in G_1$$

$$Z_r = Z \frac{1}{(\gamma + x_1)(\gamma + x_2)...(\gamma + x_r)} \in G_2$$

- t_{RL} = Current date
- sig(RL) = signature generated by group manager

Here, the ECDSA signature algorithm is used.

4.3 File Management

It consists of 3 phases

4.3.1 File Generation

A group member performs operations to store and share data file in the cloud.

i. Get the Revocation List RL from the Cloud.

ii. Verify the validity of the RL

iii. Encrypt the file M. Two cases: 1.No revoked users in the RL.
$C_1 = k.Y$
$C_2 = k.P$
$K = Z^k$
$C = Enc_K(M)$, $Y, P \in G_1$ $Z \in G_2$
2. There are r revocation users in RL.
$C_1 = k.Y$
$C_2 = k.P$
$K = Z_r^k$
$C = Enc_K(M)$, $Y, P \in G_1$ $Z_r \in G_2$

iv. Compute $f(\tau)$,Hash value. Member adds (Id_{data}, τ) into his local storage.

v. Construct the uploaded Data file in the format in Table 2.

vi. Upload data into the cloud server . Cloud first invokes the algorithm 2 that verifies the group signature and then the algorithm 3 that verifies the revocation

4.3.2 File Deletion

File stored in the cloud can be either deleted by group manager or data owner.

File Deletion by Group Manager

i. Computes a signature $\gamma f_1(ID_{data})$ and send it along with ID_{data} to the cloud

ii. Cloud will delete the file if $e(\gamma f_1(ID_{data}), P) = e(W, f_1(ID_{data}))$ holds.

File Deletion by Data Owner

i. Obtain tuple (ID_{data}, τ) from his local storage.

ii. Invoke Algorithm 1 to compute a group signature on (ID_{data}, τ) .

iii. Send (ID_{data},τ) and signature as a deletion request to the cloud.
iv. Cloud calls the algorithm 2 and 3 to verify the group signature. If success then file is deleted.

4.3.3 File Access

The content of the shared file is accessed by group members by the following operations,

i. The user uses the private key (A,x) and compute signature σ_u on message (ID_{group}, ID_{data},t) using Algorithm1.User send the data request containing (ID_{group}, ID_{data},t,σ_u) to the cloud server.
ii. Cloud Server uses algorithm 2 and 3 to check the validity of the signature and revocation verification.
iii. Check the validity of revocation list.
iv. Verify the validity of the file and decrypt it .This operation differs for the 3 cases according to the timestamp t_{data} and revocation list.

Case 1: (t_{data} < t_1) No revoked user before the data file uploaded.

1. Invoke algorithm 2 to check the group signature . If it returns false then user stops this protocol.
2. Use his partial private key(A,B) to compute
$\hat{K} = e(C_1, A)e(C_2, B)$
3. Decrypt the cipher text C with the computed key $\hat{K}$

Case 2: (t_i<t_{data}<t_{i+1}) i revoked user revoked before the data file uploaded.

1. Verify the group signature σ by using Algorithm 2.
2. Algorithm 3 is called using inputs A_1, A2,…, Ai . If it returns invalid, the user terminates the operation.
3. Compute the value of

$$A_{i,r} = \frac{1}{(\gamma + x)\prod_{\lambda=1}^{i}(\gamma + x_\lambda)} P$$

4. Calculate the decryption key

$$\hat{K} = e(C_1, A_{i,r})e(C_2, B)$$

5. Decrypt the cipher text C with the computed key $\hat{K}$

Case 3: (t_r < t_{data}) r revoked user revoked before the data file uploaded.

1. Verify the group signature σ by using Algorithm 2.
2. Algorithm 3 is called using inputs A_1,A_2,…,A_i . If it returns invalid ,the user terminates the operation.
3. Compute the value of

$$A_{r,r} = \frac{1}{(\gamma + x)\prod_{\lambda=1}^{r}(\gamma + x_\lambda)} P$$

4. Calculate the decryption key

$$\hat{K} = e(C_1, A_{r,r})e(C_2, B)$$

5. Decrypt the cipher text C with the computed key $\hat{K}$

4.4 Traceability

If any data dispute occurs then the tracing operation is performed by the group manager to identify the real identity of the data owner.

1. Given a signature $\sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$ the group manager uses his private key (ξ_1, ξ_2) and compute
$A_i = T_3 - (\xi_1 . T_1 + \xi_2 . T_2)$
2. Given the parameter A_i, the group manager can look up the user list to find the corresponding identity.

Table 2.Data Format for uploading

Group ID	Data ID	Cipher text	hash	Time	Signature
ID_{group}	ID_{data}	C_1,C_2,C_3	f(τ)	t_{data}	σ

The above scheme is implemented using the Java Pairing Based Cryptography (JPBC) library and the simulated cloud, group manager and the user's module are implemented using java.

VI CONCLUSION

In this paper, a privacy-preserving data sharing mechanism was proposed for dynamic users in the group. This scheme satisfies the secure access control and data confidentiality with minimum key complexity.

ACKNOWLEDGMENT

The authors wish to express their heartfelt thanks and gratitude to the Department of Computer Science and Engineering of Mepco Schlenk Engineering College, Sivakasi for providing good support and encouragement for this work. The authors also thank their principal and management for providing the necessary facilities to carry out this work.

REFERENCES

[1] George Pallis "Cloud Computing, The New Frontier of Internet Computing", University of Cyprus.
[2] Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan, "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.*
[3] 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.
[4] 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 Tech, pp. 29-42,2003.
[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and distributedSystems Security Symp. (NDSS), pp. 131-145, 2003.
[6] 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.
[7] 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.
[8] 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.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security,, 2006.

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

Authors Bibliography

Saranya C received her B.E degree in Computer Science and Engineering from PSR Rengasamy College of Engineering for Women Sivakasi, TamilNadu, India in 2012. She is currently pursuing M.E in Computer Science and Engineering in Mepco Schlenk Engineering College, Sivakasi, India. Her research interests are in cryptography and in cloud computing.

