ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Anonymously Sharing of Data by Using Group Signature and Encryption Techniques in Dynamic Cloud Computing

V Sarojini Naidu
M.Tech Student,
Department Of Computer Science Engineering,
NRI Institute Of Technology,Guntur.

Mrs.P.Sujatha
Assistant Professor,
Department Of Computer Science Engineering,
NRI Institute Of Technology,Guntur.

Abstract:

Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. Due to frequent change of members in multi owner group, preserving user data and their identity privacy becomes a challenging issue in cloud. In this paper, we propose a secure multi-owner data sharing scheme, for dynamic groups in the cloud.

The major aims of this method is to secure multi-owner data sharing scheme. It implies that any user in the group can securely share data with others by the un trusted 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.

Keywords:
Privacy Preserving, Cloud Computing, data sharing, access control, dynamic groups.

Introduction:

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security.

It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Security issues associated with the cloud:

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud).

The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures. When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information.

As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can by viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation. The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured.

Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

Some security and privacy issues that need to be considered are as follows:

1) Authentication: Only authorized user can access data in the cloud.

2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure.

3) Availability: The cloud data should be easily available and accessible without any burden. The user should access the cloud data as if he is accessing local data.

4) No storage Overhead and easy maintenance: User doesn't have to worry about the storage requirement & maintenance of the data on a cloud.

5) No data Leakage: The user data stored on a cloud can accessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.

6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation

EXISTING SYSTEM:

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.

In the existing System 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.

DISADVANTAGES OF EXISTING SYSTEM:

- In the existing Systems, 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.

- Only the group manager can store and modify data in the cloud.

- The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.

PROPOSED SYSTEM:

1. 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.

2. 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

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.

3. We provide secure and privacy-preserving access control to users, which guarantees any member in a group to anonymously utilize the cloud resource. Moreover, the real identities of data owners can be revealed by the group manager when disputes occur.

4. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead.

ADVANTAGES OF PROPOSED SYSTEM:

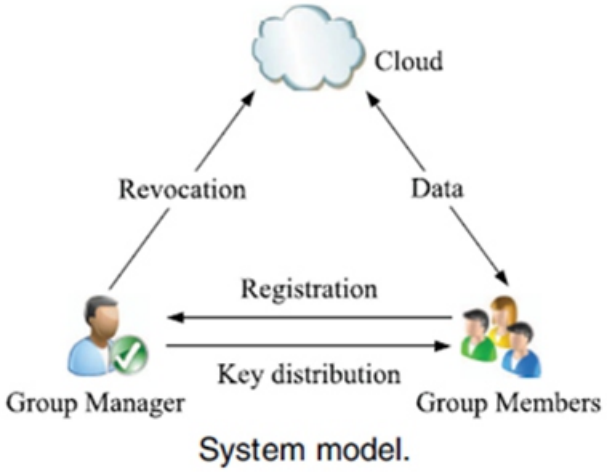
Any user in the group can store and share data files with others by the cloud.

- The encryption complexity and size of ciphertexts are independent with the number of revoked users in the system.

- User revocation can be achieved without updating the private keys of the remaining users.

- A new user can directly decrypt the files stored in the cloud before his participation.

SYSTEM ARCHITECTURE:



System model.

ALGORITHMS USED:

Signature Generation:

Input: Private key (A, x), system parameter (P, U, V, H, W) and data M.
Output: Generate a 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 $\delta_2 = x\beta$
Computes the following values

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

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

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

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

Signature Verification

Output: True or False.
begin
Compute the following values

$$\begin{cases} \tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R}_2 = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R}_3 = (\dfrac{e(T_3, W)}{e(P, P)})^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta} \\ \qquad\qquad e(H, P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases}$$

if $c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5})$
Return True
else
Return False
end

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Revocation Verification:

Input: System parameter (H_0, H_1, H_2), a group signature σ, and a set of revocation keys $A_1, ..., A_r$
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
Retum Invalid
end

MODULES:

1.Cloud Module.
2.Group Manager Module .
3.Group Member Module .
4.File Security Module .
5.Group Signature Module .
6. User Revocation Module .

MODULES DESCRIPTION:

1.Cloud Module :

In this module, 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.

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.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

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).

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.

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Monthly Peer Reviewed Open Access International e-Journal

Conclusion:

In this paper, we design a secure data sharing scheme, for dynamic groups in an untrusted cloud.A user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally,it 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. Moreover, the storage overhead, length of the signature and the running time of the signing algorithm are independent with the number of group members.

REFERENCES:

[1] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing forDynamic Groups in the Cloud", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, JUNE 2013.

[2] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[3] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.

[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] B. Wang, B. Li, and H. Li, "Knox: Privacy-Preserving Auditing for Shared Data with Large Groups in the Cloud,"Proc. 10th Int'l Conf. Applied Cryptography and Network Security, pp. 507-525, 2012.

[6] A. Fiat and M. Naor, "Broadcast Encryption," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO),pp. 480-491, 1993.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute- Based Encryption for Fine-Grained Access Control ofEncrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[8] D. Pointcheval and J. Stern, "Security Arguments for Digital Signatures and Blind Signatures," J. Cryptology, vol.13, no. 3, pp. 361-396, 2000.

[9] 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.

[10] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[11] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[12] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.