A Secure data sharing approach for dynamic groups in cloud with multi owners

CH.Pravallika[1]
Department of CSE, TKRCET
Telangana,India

G.Arnab Sarkar[2]
Department of CSE, TKRCET
Telangana,India

Abstract: Cloud computing provides an easy solution for sharing group resource among cloud users. In a multi owner manner data preserving and privacy identity from untrusted cloud is still an exigent issue. In this Paper we are going to discuss about a secure data sharing for dynamic groups in the cloud. Analyze the security with proofs, and demonstrate the correct scheme in experiments.

Key points: Cloud computing, Data privacy, secure system, Multi owners, dynamic groups

I. INTRODUCTION

Cloud computing is a recently evolved computing terminology or metaphor based on utility and consumption of computing resources. It involves deploying groups of remote servers and software networks that allow centralized data storage and online access to computer resources. It can broadly classify into three categories:

IAAS- Information as a service

PAAS- Platform as a service

SAAS- Software as a service

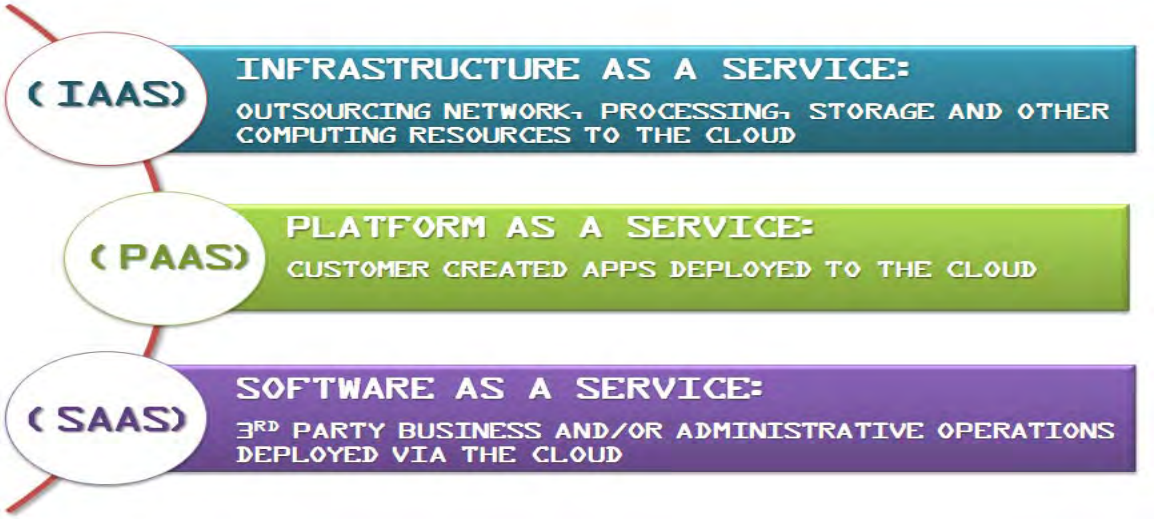

Fig. 1 Cloud Computing Service

Cloud Computing comprises three different service models, namely Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three service models or layer are completed by an end user layer that encapsulates the end user perspective on cloud services. The model is shown in figure below. If a cloud user accesses services on the infrastructure layer, for instance, she can run her own applications on the resources of a cloud infrastructure and remain responsible for the support, maintenance, and security of these applications herself. If she accesses a service on the application layer, these tasks are normally taken care of by the cloud service provider.

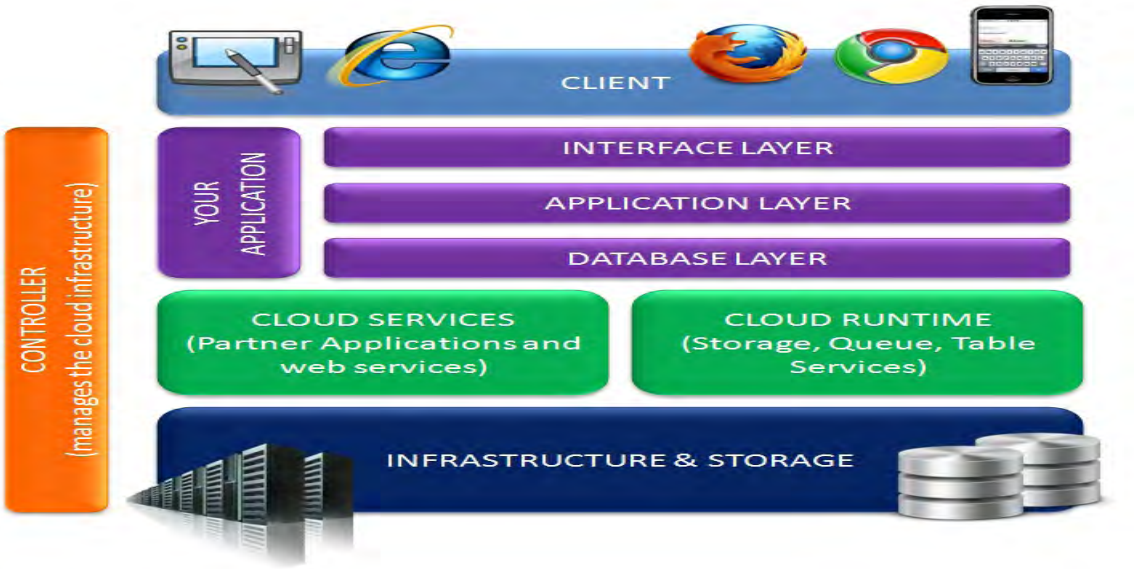

Fig. 2 Cloud Services and Layers

The major aims of this method 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. This scheme is able to support dynamic groups. Efficiently, 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. We present a secure and privacy-preserving access control to users, which guarantee any member in a group to anonymously utilize the cloud resource. The real identities of data owners can be revealed by the group manager when disputes occur. We provide rigorous security analysis, and perform extensive simulations to demonstrate the efficiency of our scheme in terms of storage and computation overhead. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users.

II. EXISTING SYSTEM

To Preserve the Confidentiality and integrity of the data one of the best approach is to encrypt the files by using secure encryption algorithm whenever we are deploying the data on to a cloud which is a open source to use on pay basis. Due to the vast availability of Clouds and their service many people are interested in sharing the data on cloud but at the same time designing an efficient and secure data sharing model for the groups in the cloud is not an easy task. In the present system data owner first encrypts the files and stores them in the cloud storage and shares the secret only to the users who are authorized. So that only authorized users only can decrypt and view the data shared by owners in the group. Complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the number of revoked users.

A. Disadvantages of existing system

In the existing Systems, Providing the security for identity of users who want to join and use the service of the cloud is a difficult task, the identity of the users may be disclosed to providers and attacker. On the other hand, unconditional identity privacy may incur the abuse of privacy. For example, a misbehaved person 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.

III. PROPOSED APPROACH

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. In this approach a authorized user can directly access the files and decrypt them without contacting the owners of the data.

Advantages of proposed system:

- ✓ Without any complexity users in the cloud can share the data between them.
- ✓ 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.

Fig. 3 System Architecture

Here we are using broadcast encryption which enables a broadcaster to transmit encrypted data to a set of users so that only a an authorized subset of users can decrypt the data. Dynamic broadcast encryption also allows the group manager to dynamically include new members while preserving previously computed information, where the user decryption keys need not be recomputed and size of ciphertexts are unchanged. There is no change in the group encryption key.Various secure key exchanging schemes will be used for securely exchanging the secret keys with in the cloud.

Features: 1. Any user in the group can store and share data files with others in the cloud.

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

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

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

Scheme Description

1. System Initialization: The group manager takes charge of system initialization.
   - Randomly choosing two elements and a number and respectively.
   - Publishing the system parameters and symmetric encryption algorithm with secret key k.
2. User Registration: For the registration of user I with identity I D, the group manager randomly selects a number x and computes A, B.
3. User Revocation: 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.
4. File Generation: To store and share a data file in the cloud, a group member performs it.
   - The member sends the group identity I D as a request to the cloud.
   - Verifying the validity of the received revocation list. Checking whether the marked date is fresh.
   - Encrypting the data file M.
5. File Deletion: File stored in the cloud can be deleted by either the group manager or the data owner. To delete a file ID, the group manager computes a signature and sends the signature along with ID to the cloud. The cloud will delete the file if the equation holds.
6. File Access: The user first adopts its private key (A,x) to compute a signature on the message by using algorithm 1. Then the user sends a data request containing (IDgroup, IDdata) to the cloud server. The cloud server employs algorithm 2 to check the validity os the signature.
   By using the following modules we have implemented the scheme as we discussed above

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. 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

1. System parameters generation,
2. User registration,
3. User revocation, and
4. Revealing the real identity of a dispute data owner.

3.Group Member Module

1. Store their private data into the cloud server
2. Share them with others in the group

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.

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

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.

IV. CONCLUSION

In this paper, we have designed a data sharing scheme for dynamic groups in an untrusted cloud which is more secure for sharing the data between the members of cloud groups. In this, a user is able to share data with others in the group without revealing his identity to the cloud. Efficient user revocation can be achieved through a public revocation list where there is no need of updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation or before communicating with the data owners.

REFERENCES

[1] 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, &ldquo,A View of Cloud Computing,&rdquo, Comm. ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

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

[3] S. Yu, C. Wang, K. Ren and W. Lou, &ldquo,Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing,&rdquo, Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang and K. Fu, &ldquo,Plutus: Scalable Secure File Sharing on Untrusted Storage,&rdquo, Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu and D. Boneh, &ldquo,Sirius: Securing Remote Untrusted Storage,&rdquo, Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] G. Ateniese, K. Fu, M. Green and S. Hohenberger, &ldquo,Improved Proxy Re-Encryption Schemes with Applications to Secure Distributed Storage,&rdquo, Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 29-43, 2005.

[7] R. Lu, X. Lin, X. Liang and X. Shen, &ldquo,Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing,&rdquo, Proc. ACM Symp. Information, Computer and Comm. Security, pp. 282-292, 2010.

[8] B. Waters, &ldquo,Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization,&rdquo, 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, &ldquo,Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,&rdquo, Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

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

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

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