International Journal on Applications in Information and Communication Engineering
Volume 1: Issue 12: December 2015, pp 24-27. www.aetsjournal.com ISSN (Online) : 2394-6237

Secure Data Sharing Scheme For Dynamic Group In Public Cloud

M.uday, S.Jayakumar

Abstract— Cloud computing provides an economical and efficient solution for Dynamic sharing. Due to frequent changes in membership and sharing data in a multi-owner manner to an untrusted cloud is still a challenging issue. In this paper we define a secure data sharing scheme, for dynamic group in the public cloud. Using an AES encryption, cloud user can securely share data with others. Meanwhile, the excess of storage and encryption computation cost of the scheme are independent with the number of revoked users. We can also analyze the security of this group with exact proofs. One-Time Password is one of the most secure forms of authentication. First the user selects the text based password and OTP is sent to his/her corresponding e-mail account.

Keywords— Cloud computing, AES encryption, OTP

I. INTRODUCTION

Cloud computing is Internet ("cloud") based development and use of computer technology ("computing"). It is a computing that which dynamically scalable and virtualization resources provides a service over the internet. Data storage is the most fundamental services offered by cloud providers. Let us consider a company allows its staff in the same group or department to store and share files in the cloud which can be shared in any time. it has a significant risk for stored files like confidentiality problems. Specifically, the cloud servers were managed by cloud providers are not fully trusted by users because the data files stored in the cloud may be sensitive and confidential. To provide a privacy for data, a basic solution is that we have to encrypt data files, and then upload the encrypted data files into the cloud.

Identity privacy is one of the most significant obstacles for deployment of cloud computing. Without the guarantee of identity privacy, users can not join in cloud computing systems because their real identities will be easily disclosed to cloud providers and attackers. For example, one of the members in the group shared false files without being traceable. Then, traceability was enabled by the group manager (e.g., a company manager) to reveal the real identity of a user. It is recommended that any member in a group is able to store the data and sharing files and services provided by the cloud, it is called as the multiple-owner manner. As we compared with the single-owner manner, where there is only the group manager, he can only store and modify data in the cloud, but in practical applications the multiple-owner manner is more flexible. Every user in the group is able to read data and also modify his/her part of data in the entire data file shared by the company. Groups are normally dynamic in practice, e.g., new staff will join and current employee will leave the company. The changes in membership make secure data sharing was very difficult. The anonymous system challenges newly joined users to learn the content of data files stored before their participation, because it is impossible for newly joined users to contact with other data owners, and obtain the decryption keys. It is an efficient membership revocation mechanism without updating the secret keys of the others users is also desired to minimize the complexity of key management. In these approaches, data owners store the encrypted data files in untrusted storage and distribute the corresponding decryption files.

keys is used for authorizing users. Thus, unauthorized users will not access the content of shared data files because they did not have knowledge of the decryption keys. To solve the challenges which are presented above, we propose a secure multi-owner data sharing scheme for dynamic group in the cloud. The main contribution of this paper include, To provide security for dynamic group we integrates two levels of protection like Image based authentication and one time password to achieve high level of security.

The main Objective of providing a two levels of security is a unique and an esoteric study of implementation of an extremely secured system.

LEVEL 1: In level 1 we have a security provides a simple text based password.

Level 2: After the successful entry of the above level 1, the Level 2 Security System will generate the one-time numeric password that should be valid for that login session. The authentic user will get this one time password to his e-mail.

II. SYSTEM MODEL, SECURITY REQUIREMENTS AND DESIGN GOAL

A. Group Signature

The concept of group signatures was first introduced in by Chaum and van Heyst. In general, a group signature scheme allows any member in the group has to sign messages to keep their identity secret from verifiers. Only the group manager can able to reveal the identity of the signature's originator when a problem occurs, which is denoted as traceability. In this paper, we use a short group signature to achieve

M.uday, M.Tech-CSE Final Year,SRM University, Ramapuram, Chennai, India (Email: udaymedapaati@yahoo.in)
Mr.S.Jayakumar Assistant Professor - CSE, SRM University,Chennai, India (Email: Jayakumar.s@rmp.srmuniv.ac.in)

anonymous access control, as it supports efficient membership revocation.

B. *Dynamic Broadcast Encryption*

Broadcast encryption is a broadcaster to transmit encrypted data to authorized users so that only that users can decrypt the data. Dynamic broadcast encryption will allows the group manager to dynamically join the new members while storing previously computed information, means user decryption keys need not be recomputed, The first formal definition and construction of dynamic broadcast encryption are introduced based on the bilinear pairing technique used as the basis for file sharing in dynamic groups.

III. DESIGN GOALS

In this section, we have design goals of the proposed scheme are access control, data confidentiality, anonymity and traceability and efficiency.

A. Access control:

The requirement of access control is to fold. In this group members will use the cloud resource for data operations and unauthorized users cannot access the cloud resource in that group and revoked users will be incapable of using the cloud again once for data operations and unauthorized users cannot access the cloud resource in that group and revoked users will be incapable of using the cloud again once they are revoked.

B. Data confidentiality:

Data confidentiality requires that unauthorized cannot get the content of the stored data. An important and challenging issue for data confidentiality is to maintain availability for dynamic groups. Specifically, new user who are joined newly should decrypt the data stored in the cloud before their participation, and revoked users can not decrypt the data which was moved into the cloud after the revocation.

C. Anonymity and traceability:

Anonymity means that group members can access the data in cloud without revealing their real identity. anonymity has an effective protection for user identity. For example, an inside attacker may store and share a mendacious information to derive substantial benefit. Thus, to solve the inside attack, the group manager should have the ability to reveal their real identities of data owners.

D. Efficiency:

The efficiency means any group member can store and share data files with others users in the group by the cloud. User revocation was achieved without involving the remaining users. they do not need to update their private keys. New granted users can get all the content data files stored before their participation without contacting with the data owner.

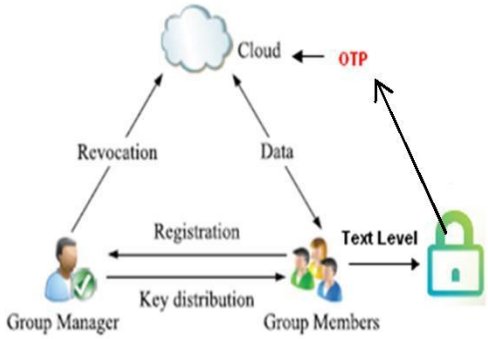
IV. PROPOSED SCHEME

A. Overview

To provide secure data sharing for dynamic groups in the cloud, we have to combine the group signature and dynamic broadcast encryption techniques. In group signature scheme users has to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to share their data files securely with others including newly joined users. Each user has to determine revocation parameters to protect their confidentiality from the revoked users in the dynamic broadcast encryption scheme. Thus, the heavy overhead and large ciphertext size makes it difficult for assumption of the broadcast encryption scheme to capacity-limited users. To solve this issue, the group manager has to determine the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the ciphertext size. The computation overhead of users for encryption operations and the ciphertext size are constant and independent of the revocation users.

Secure environments protect their resources against unauthorized access by enforcing access control mechanisms. So when increasing security the text based passwords are not enough to counter such problems. Using the instant messaging service available in internet, user will get the One Time Password (OTP) after image authentication. This OTP can be used by user to access their personal accounts. In this paper one time password is to achieve high level of security in authenticating the user over the internet.

ARCHITECTURE DIAGRAM



B. Admin or Group Owner

1. Group Creation

Groups are created by the admin. A company allows its staffs in the same group or department to store and share files in the cloud. Any member in a group should be able to store data and share flies services provided by the cloud, which is defined as the multiple-owner manner.

2. User Registration

For the registration of user i has a identity like IDi, the group manager will randomly selects a number and characters for generating random key. Then, the group manager update the group user list, which will be used in the traceability phase. After the registration completes, user i obtains a private key, which was used for group signature generation and file decryption.

3. Group Access Control

When a data dispute occurs, the tracing operation is performed by the group manager to identify the real identity of the data owner with the help of group signature scheme, can be regarded as a variant of the short group signature, which contains anonymous authentication, and tracking capability.

The requirement of access control, group members should use the cloud resource for data operations and unauthorized users cannot access the cloud resource in that group and revoked users cannot use the cloud again once they are revoked.

4. File Deletion

Group manager or data owner can delete the file which was stored in the cloud (i.e., the member who uploaded the file into the server). To delete a file ID data, the group manager has a signature ID data and he sends the signature along with ID data to the cloud.

5. Revoke User

User revocation is performed by the group manager by using public available revocation list RL, based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. The admin can only have permission to revoke user and remove revocation.

C. User Or Group Member

Group members means set of registered users they will store their private data into the cloud server and share data with others in the group.

1. File Upload

To store and share a data file in the cloud, a group member has to checks the revocation list and verify the group signature. First, we have to check whether the marked date is fresh. Second, verify the contained signature. Uploading the data into the cloud server and adding the ID data into the local shared data list maintained by the manager. Once we receive the data, the cloud has to check its validity. It returns true, the group signature is valid; otherwise, the cloud stops the data. In addition, if several users have been revoked by the group manager, the cloud also performs revocation verification, the data file will be stored in the cloud after successful group signature and revocation verifications.

2. File Download

Signature and Key Verification are two methods, a group signature scheme allows any member in the group to sign messages while keeping the identity secret from verifiers. The designated group manager can reveal the identity of the signature originator when a problem occurs, which is denoted as traceability.

3. OTP (One Time Password)

OTPs avoid a number of shortcomings that are associated with traditional passwords. The most important shortcoming that is addressed by OTPs is that, in contrast to static passwords, they are not vulnerable to replay attacks.This means that an intruder who manages to record an OTP will not be able to use it because the OTP he managed to login is already used and is no longer valid.

OTP can be used to authenticate a user in a system through the authentication server. Also, if some more steps are taken like the server calculates subsequent OTP value and sends/displays it to the user who checks it against subsequent OTP value calculated by his token and user can also authenticate the validation server.

Generation of OTP Value

The algorithm can be described in 3 steps:

Step 1: Generate the HMAC-SHA value Let HMK = HMAC-SHA(Key, T) // HMK is a 20-byte string Step 2: Generate a hex code of the HMK. HexHMK=ToHex (HMK)

Step 3: Extract the 8-digit OTP value from the string

OTP = Truncate (HexHMK) the Truncate function in Step 3 does the dynamic truncation and reduces the OTP to 8-digit.

4. AES Encryption

The input 16 byte Plain text can be converted into 4×4 square matrix. The AES Encryption consists of four different stages they are

Substitute Bytes: Uses an S-box to perform a byte-by-byte substitution of the block **Shift Rows:** A Simple Permutation

Mix Columns: A substitution that makes use of arithmetic overGF(2^8)

Add Round Key: A Simple Bitwise XOR of the current block with the portion of the expanded key

5. AES Decryption

The Decryption algorithm makes use of the key in the reverse order. However, the decryption algorithm is not identical to the encryption algorithm

V. CONCLUSION

In this paper, I proposed a secure data sharing scheme, for dynamic groups in an untrusted cloud. User can share data with other users in the group without revealing his 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 no need to update the keys of remaining users, and new users can directly decrypt files stored in the cloud before they going to participate. A new type authentication system, which is highly secure, has been proposed in this paper.

We use OTP it is the one of the most secure forms of authentication. First the user selects the text based password and OTP is sent to his/her corresponding e-mail account**.**

References

[1] X.Liu,B.Wang,Y.Zhang, and J.Yan,"Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,"IEEE Computer Society,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] G.Ateniese, R. Burns, R.urtmola, J.Herring, L. Kissner, Z. Peterson, and D.Song, "Deduplication in cloud storage using side channels in cloud services," Oct 2008.

[4] D. Boneh, X. Boyen, and E. Goh, "Hierarchical Identity Based Encryption with Constant Size Ciphertext," Proc. Ann. Int‟ l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 440-456, 2005.

[5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: A high-availability and integrity layer for cloud storage," in Proc. Of CCS‟ 09, 2009, pp. 187-198.

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

[7] 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.

[8] 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 Technologies, pp. 29-42, 2003.

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

[10] B. Sheng and Q. Li, "Verifiable Privacy-Preserving Range Queryin Two-Tiered Sensor Networks," Proc. IEEE INFOCOM, pp. 46-50, 2008.

[11] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.