IJCSN International Journal of Computer Science and Network, Volume 6, Issue 2, April 2017
ISSN (Online) : 2277-5420
www.IJCSN.org
Impact Factor: 1.5

A Scalable Secure File Sharing System for Dynamic Groups in Cloud Computing

[1] S.R.Suganya; [2] Dr.B.Jaison

[1] P.G.Student, [2] Associate Professor
[1, 2]Department of Computer Science and Engineering
R. M. K. Engineering College, Kavaraipettai, Chennai, Tamilnadu, India

Abstract - Cloud computing is an emerging technology over the last few years due to its characteristics like scalability, performance and security. Users can achieve the effective benefits for file sharing among group members in cloud with low cost and maintenance. Unfortunately, because of the frequent change of the membership, file sharing while providing privacy-preserving is a challenging issue. In this paper, we propose a secure file sharing approach for dynamic users Firstly, we propose a system for key distribution in secure manner without using any secure communication channels, and the users can get their private keys from group manager in secure way. Secondly, it can achieve fine-grained access control that is any user in the group can access the resource in the cloud. Thirdly, revoked user cannot get the original data file even if they intrigue with untrusted cloud. Lastly, the scheme can achieve fine efficiency, which means previous users need not to update their private keys.

Keywords - *Access control, Cloud computing, Efficiency, File sharing, Key distribution.*

1. Introduction

Cloud computing is a type of computing resources that are delivered as a service over a network. Cloud computing entrusts remote services with a user's data, software and computation. The resources are made available on the internet as managed third-party services. One of the most elementary services offered by cloud providers is data storage. The cloud computing is a ubiquitous based computing because the data is available at any time.

The cloud service provider (CSP) is affording various services to the users. To preserve data file privacy, the common method is to encrypt the files before the client upload the file in to the cloud. But it is complex to design a secure and effective file sharing scheme for dynamic groups in the cloud. This paper is based on a secure file sharing scheme which can achieve a secure key distribution and file sharing for dynamic groups in the cloud.

1.1 Service Models

Cloud has three different service models. The three service layers are completed by an end user layer that encloses the end user view on cloud services. SaaS: It can be express by the process called Application Service Provider (ASP) which provides different software applications over the internet. Paas: Paas is the delivery of a computing platform as a service without software downloads or installation for developers, managers or end-users. It gives a high level of integration in order to execute and test cloud applications.

IaaS: It shares the hardware resources for implementing services using virtualization technology. The main aim is to build resources such as servers, network and storage accessible by applications.

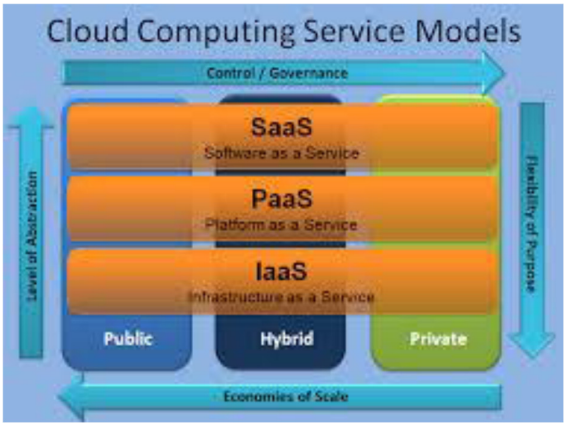

Fig. 1 Cloud Service Models

2. Related Work

Kallahala et al. presented a cryptographic storage framework that enables secure file sharing on untrustworthy servers based on the approach that separate the files into file groups and encrypting each file group with a file block key. In this scheme at the time of user revocation the file block key need to be update and distributed to the user therefore the updated keys has to be distributed.

Yu et al. exploited and combined technique of key policy attribute based encryption, proxy re-encryption to achieve fine grained data access control without disclosing data content.

Lu et al. presented a secure verified scheme by leveraging group signatures and cipher text policy attribute based encryption techniques. Each user gets two key after the registration. One key is used for decrypt the data which is encrypted by the attribute based encryption and the other key is used for privacy preserving. But revocation is not supported in this approach.

Liu et al. presented a scheme named Mona which is based on a secure multi-owner data sharing. This scheme is used to achieve fine-grained access control and revoked users cannot access the data from cloud once they are revoked. However, this scheme will easily suffer from the collusion attack. In order to get the secret file, revoked user can use his private key to decrypt the encrypted file after his revocation by intrigue with the cloud.

To access the file, the revoked user sends the request to the cloud and then the cloud sends the corresponding encrypted file and revocation list to the attacker without verification. The decryption key can be calculated using attack algorithm. This leads to reveal the details of other legal members in the group.

Zhou et al. presented a secure access control scheme on encrypted data in cloud storage by invoking role-based encryption technique. This scheme can achieve an efficient user revocation and access control policies with encryption to secure large file storage in the cloud.

Zou et al. presented a scheme which is practical and flexible key management mechanism for trusted collaborative computing. This method is modelled to achieve access control mechanism for dynamic groups.

Nabeel et al. presented a privacy preserving policy based content sharing scheme in cloud. But this scheme is not secure because of the weak protection.

3. Proposed Model

The main contribution of our model includes:

We distribute a key in a secure way without using any secure communication channels. The group users can securely acquire their private keys from the group admin without any Certificate Authorities because of the verification for the public key of the user.

This model can achieve fine-grained access control with the help of user list.

The group user can revoke from the group securely with the influence of polynomial function.

The proposed scheme can achieve fine efficiency which means a new user who joins in the group or revoked from the group, the other user's private key need not to recalculate and updated.

3.1 System Model

The system model consists of the cloud, group manager and the group members.

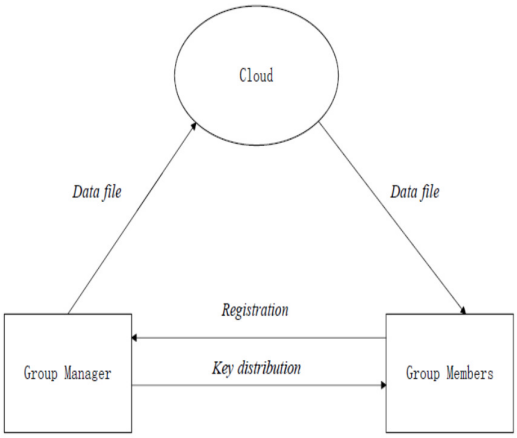

Fig.2 System Model

1) Cloud:

In this, we create a local cloud and provide price abundant storage services. The users can upload their data in the cloud. This module is developed, where the cloud storage can be made safe. However, the cloud is not fully trusted by users since the CSPs are very likely to be outside of the cloud users trusted domain. Similarly we assume that the cloud server is legal but intrusive. Therefore the cloud server will not maliciously delete or modify user data due to the protection of data auditing schemes, but endeavour to know the content of the stored data and the identities of cloud users.

2) Group Manager:

The role of group manager is to generate a system parameter, User registration, User revocation and revealing the identity of a dispute data owner. The group manager is fully trusted by the other parties. The group manager has the logs of each and every process in the cloud.

3) Group Member:

The role of group member is to store their private data into the cloud server and Share them with others in the group.

The account of a group is dynamically changed, due to the staff revocation and new employee participation in

the company. The group member has the ownership of changing the files in the group. Any user in the group can view the files which are uploaded in their group and also modify it. Group members are able to use the cloud resource for file storage and sharing. Unauthorized users cannot get the cloud resource at any time, and resigned users will be incapable of using the cloud resource again once they are revoked.

3.2 Design Goals

This study describes the principle goals of the proposed design including key distribution, access control, data confidentiality and efficiency are as follows:

Key distribution: The requirement of key distribution is user can get their private keys in secure manner from the group manager without any Certificate Authorities. In other methods, this can be achieved by the communication channel which is secure.
Access control: Registered group users are able to access the file at any time in the cloud.

Confidentiality: Data secrecy requires that users who are not in the group are incapable of accessing the content of the stored file. To maintain the confidentiality of sharing file for dynamic groups is an important issue. Mainly the users who are revoked from the group are unable to decrypt the file.

Efficiency: Any user in the group can store and transfer the files with other group members in the cloud. User revocation can be achieved without affecting others which implies other users need not to update their private keys.

All these design goals should be achieved efficiently in the sense the system is scalable.

3.3 System Description

The system description includes system initialization, registration for user, file upload, user revocation and file download.

System Initialization: This operation can be performed by group manager. In this symmetric encryption algorithm is used. The group manager will keep the parameter as the master secret key.

Symmetric Encryption Algorithm (Triple DES- 3DES)

This algorithm was created to provide a level of security far beyond that of standard DES. 3DES uses three 64-bit keys for an overall key length of 192-bits.It can be employed using two or three keys and a combination of encryption or decryption for additional security. It employs 48 rounds in its encryption computation, generating ciphers that are 256 times stronger than DES ciphers.

Triple DES Encryption is as follows:

In the 1st operation, 3DES encrypts the message with K1, then decrypts it with K2, and then encrypts it again with K1. The notation is [E {D [E (M, K1)], K2}, K1]. In the 2nd operation, 3DES encrypts the message with K1, then it encrypts it again with K2, and then it encrypts it a third time with K2 again or [E {E [E (M, K1)], K2}, K1]. In the third operation, 3DES encrypts the message three times with three different keys; [E {E [E (M, K1)], K2}, K3]. This is the most secure level of encryption.

Registration for Existing User: This operation is performed by user, group manager and the cloud. The user sends the id to the group manager as a request with the public key. The group manager chooses a random number and sends the message to the user for verification using asymmetric encryption algorithm as ECC. After successful registration, user becomes a group member.

Asymmetric Encryption Algorithm (ECC-Elliptic Curve Cryptography)

ECC is one of the most efficient types of public key cryptography. This algorithm is mainly depending on algebraic structure of elliptic curves. The advantage of this algorithm is smaller key size (160 bit key)

When compared to RSA (1024 bit key), reducing in storage and transmission requirement that is it provides same level of security provided by RSA.

File Upload: The file upload operation can be done by group member. First of all, the group member chooses a file. Then the file can be encrypted by group member and send to the group manager.

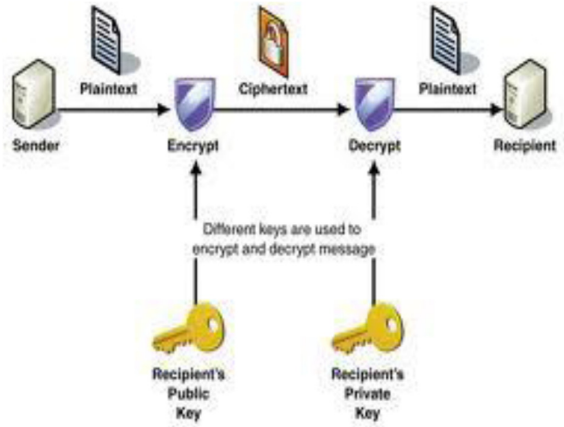

Fig.3 Asymmetric Encryption

After receiving the file group manager decrypts the file and checks the legal group member in the cloud. Then using the polynomial function group manager re-encrypts the file and sends it to the cloud.

User Revocation: This operation can be performed by the group manager and the cloud. When a user in the group can be revoked, the group manager performs the following operation: 1.Removing the user from the local list and update the new user list to the cloud. 2. Verify the new user list in the cloud, whether the users are legal group members or not. Registration for New User: This can be performed by the group manager and the operations can be performed as same as existing users registration. Then all the files in the cloud should be updated by the group manager. After that manager checks all the legal users in the group and construct the new polynomial function. Then new random re-encryption key can be selected by group manager and constructs encryption key and encrypts the cipher text and sends to the cloud.

Finally group manager updates all the files in the group file list and sends new file list to the cloud. File Download: File download can be performed by the group member and the cloud. To decrypt the original file, group member needs to perform two decryptions. Decrypt the re-encrypted file using his private key. Then he finds the re-encryption key. Finally the group member can decrypt the encrypted file and receive the original file by influence the encryption key.

4. Conclusion

In this paper, we design a scalable secure file sharing system for dynamic groups in the cloud computing. In our system, the users can acquire their private keys securely from the group manager certificate authorities and secure communication channels. Likewise, our system is able to support the dynamic group efficiently, when another user joins in the group or a user denied from the group, the other users private keys need not to be recalculated and updated. In addition, our system can accomplish secure user revocation, the users who are revoked from the group cannot be get the original files even if they intrigue with the untrusted cloud.

5. Future Scope

In this paper, we provide a secure way for sharing files in the group where the file owner can share their file with group members. Accountability is a potential for future enhancement in the substance of file sharing in the cloud. The users in the group can perform illegal activities such as sharing the files with other users who are not in the group. A plausible research way is to identify the method to protect and store the file in a way that does not crack the privacy and security act of the cloud.

References

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Commun. ACM, vol. 53, no. 4, pp. 50–58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Proc.Int. Conf. Financial Cryptography Data Security, Jan. 2010, pp. 136–149.

[3] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable secure file sharing on untrusted storage,"in Proc. USENIX Conf. File Storage Technol., 2003, pp. 29–42.

[4] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. Netw. Distrib. Syst. Security Symp., 2003, pp. 131–145.

[5] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. Netw. Distrib. Syst. Security Symp., 2005, pp. 29–43.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. ACM Conf. Comput. Commun. Security, 2006, pp. 89–98.

[8] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure provenance: The essential of bread and butter of data forensics in cloud computing," in Proc. ACM Symp. Inf., Comput. Commun. Security, 2010, pp. 282–292.

[9] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in Proc. Int. Conf. Practice Theory Public Key Cryptography Conf. Public Key Cryptography, 2008, pp. 53–70.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yang, "Mona: Secure multiowner data sharing for dynamic groups in the cloud," IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 6, pp. 1182–1191, Jun. 2013.

[11] D. Boneh, X. Boyen, and E. Goh, "Hierarchical identity based encryption with constant size ciphertext," in Proc. Annu. Int. Conf. Theory Appl. Cryptographic Techn., 2005, pp. 440–456.

[12] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully collusion secure dynamic broadcast encryption with constant-size Ci-phertexts or decryption keys," in Proc. 1st Int. Conf. Pairing-Based Cryptography, 2007, pp. 39–59.

[13] Z. Zhu, Z. Jiang, and R. Jiang, "The attack on mona: Secure multiowner data sharing for dynamic groups in the cloud," in Proc. Int. Conf. Inf. Sci. Cloud Comput., Dec. 7, 2013, pp. 185–189.

[14] L. Zhou, V. Varadharajan, and M. Hitchens, "Achieving secure role-based access control on encrypted data in cloud storage," IEEE Trans. Inf. Forensics Security, vol. 8, no. 12, pp. 1947–1960, Dec. 2013.

[15] X. Zou, Y.-S. Dai, and E. Bertino, "A practical and flexible key management mechanism for trusted collaborative computing," in Proc. IEEE Conf. Comput. Commun., 2008, pp. 1211–1219.

[16] M. Nabeel, N. Shang, and E. Bertino, "Privacy preserving policy based content sharing in public

clouds," IEEE Trans. Know. Data Eng., vol. 25, no.
11, pp. 2602–2614, Nov. 2013.