International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878, Impact Factor (2015): 3.791

A Survey on Dynamic Group Communication for Public Cloud

Jueeli Dangur[1], S. M. Jaybhaye[2]

[1]P.G. Student, Sinhgad College of Engineering, Pune- 411041, India

[2]Assistant Professor, Sinhgad College of Engineering, Pune- 411041, India

Abstract: ***In today's technology drive world cloud computing provides remote services using internet. Hence most of the people are going towards public cloud for secure data storage as well as sharing. With these several advantages, there are many issues associated with storage & sharing of data in public cloud. The user should able to transfer and control the remote data which is still lacking in today's public cloud infrastructures. Other problems are related to privacy, security, integrity, privilege management, confi dentiality etc. So the solution to all these is to encrypt the keys along with the data and then the grant the permission to access the data, which can be revoked at any time. Also it is possible to update the group key pair even though not all the members of group online. In this paper we analyzed different methods and parameters used for secure group communication.***

Keywords: Cloud Computing, public cloud, secure group sharing, forward secrecy, backward secrecy, group key agreement

1. Introduction

Cloud computing is defined as a internet based, cost saving computing which relies on sharing of resources like memory, OS, IP addresses, VM's etc instead of having local servers to operate applications. Figure1 shows requirement of any secure group communication where group authentication is first step toward the security. In any secure group communication system second and most important management is admittance management where group leader have all authorities toward the group admin selection. Third one is the group secrecy where some kinds of access policies are define that is forward secrecy and backward secrecy.

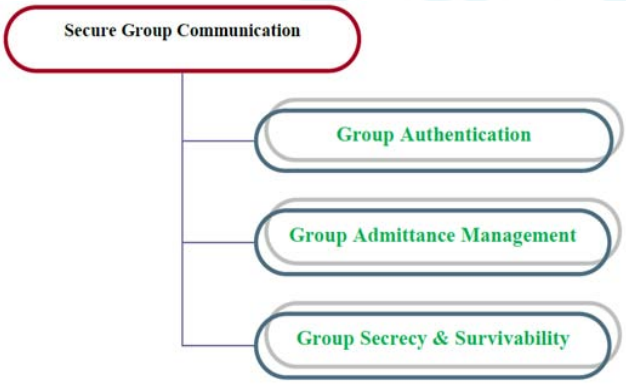

Figure 1: Requirement of any secure group communication

Cloud computing system provides end users as well as enterprises to store and process their data in third-party data centers. With number of advantages, there are several security issues associated with cloud computing system. Cloud computing system has a big risk to the confidentiality of the data because the cloud servers managed by cloud service providers (CSP's) does not completely trusty by end users whereas the data kept in cloud servers could also be very confidential and sensitive. As a result, existing security storage methods cannot be directly applied to the cloud storage. For sharing of data, data owner should able to grant or revoke permission to access particular file for the other users. Data owner should share the private data to intended user only.

In the single-owner manner only the group leader has a right to store and modify data in cloud whereas the multiple-owner manner is more useful and flexible in practical real time applications. In multiple owner manners, each user in the group has a permission not only to read the data but also to modify the entire data which has been shared by the enterprise. Groups are always dynamic in nature e.g., new member addition or current member revocation in a company can be done. This dynamic nature makes secure data sharing very difficult in cloud. Firstly Data owners store the encrypted data in untrusted storage and secondly share the decryption keys only to authorized users. Hence only authorized users which are having decryption keys can access that data.

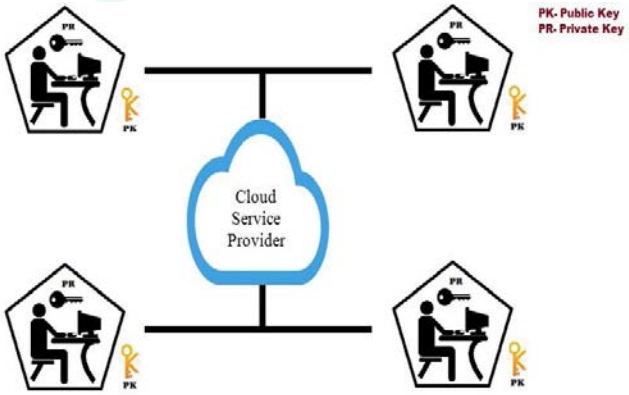

Figure 2: Traditional Group communication

Granting and revoking users is a continuous process. Usually new member are allowed to decrypt any data files which are uploaded just before their addition in the group without communicating with rest of the data owners in the group. However, member revocation is achieved via a novel revocation list without updating the secret keys of the evocated users. User is given certain privacy-preserving secure and access control which ensures that user can continuously use the available resources over the cloud.

The figure 2 shows the basic any to any communication between the group members. Each member consists of its own private and public key. This is the traditional approach

for any to any communication between two and more than two group member.

Our contributions in this paper are as follows. (1) Bringing out the various group communication methods in cloud computing system. (2) Bringing out and differentiate various key generation methods proposed in cloud computing system on the basis of various parameters. (3) To give an overview on proxy signature, proxy re-encryption and key synchronization techniques available in cloud. (4) To facilitate new researchers to work on research problem with the help of various key generation techniques, methods and also various cloud parameter.

The organization of the report is Section I Introduces cloud computing and group communication. Section II gives Literature survey with drawbacks of the existing system Section III shows Comparisons of various methods used before in previous papers. Section IV describes the problem addressed in group communication till now. Finally conclusion & references are given.

2. Literature Survey

1) Duc H. Tran et al.[1] introduced a secure framework to efficiently share data among multi-users which is based on proxy re-encryption scheme. It requires data encryption before uploading to the cloud. Same public key is provided to all the members to encrypt their data and decryption is done by using different private keys. ElGamal-based Proxy Re-encryption is used to pre-decrypt the data using user' s private key before sending the requested file.
2) A key management system for secure data outsourcing applications based on attribute-based re-encryption is proposed which uses attribute based policy to access secure content from cloud based application. In this scheme, data owner as well trusted authorities cooperate is involved in key generation and encryption. Message encryption based on a group key is also allowed by using hybrid protocol. User revocation is done without changing keys of remaining users. This schemes can be used efficiently for securing mobile cloud computing.[2]
3) Kan Yang et al. [3] proposed a Privacy-Preserving Data Publish-Subscribe Service for Cloud-based Platforms. In this, a novel attribute based encryption known as Bi-Policy ABE is used which supports access and subscription policy. In this scheme, access policy is defined by publishers of the data by using attributes and subscription policy is defined by the subscriber of the data using data tags.
4) Kaitai Liang[4] proposed a method that uses deterministic finite automata-based functional PRE for the general representation of PRE. Initially message is encrypted using random length index string and the decryptor is only allowed to decrypt ciphertext if DFA asscocited with the secret key accepts the string. The main advantage of this method is that it provides flexibility and confidentiality for data sharing and data access respectively.
5) Mohamed Nabeel , Elisa Bertino et al. [5] introduced a method for Privacy preservation through Delegated Access Control policy. Suggested method provides two layers of encryption where data owner and cloud executes coarse-grained encryption and fine-grained encryption respectively. It is very easy to modify the data because only the outer or external layer of encryption needs to be change. Subset-cover algorithm and complete sub tree algorithm is used for the decomposition of access control policies
6) Xinyu Lei, Xiaofeng Liao et al.[6] Suggested a method based on Matrix Inversion Computation (MIC). In this method privacy is preserved by transforming the matrix into an encrypted matrix and then the encrypted matrix is sent to the cloud. Again the matrix can be re-encrypted to access original matrix. Finally result verification is done using Monte Carlo verification algorithm.
7) A proxy provable data procession technique for public cloud is a framework proposed to control user data remotely stored on cloud. This method is mainly useful or has a importance when the end user do not perform remote data possession check. Proxy Provable data Procession (PPDP) system is consists of client, PCS and proxy.[7]
8) Lan Zhou, Vijay Varadharajan et al.[8] proposed the Role Based Access Control (RBAC) technique for preventing the unauthorized access of users data. A role-based encryption (RBE) scheme is proposed which is composed of integration of RBAC and cryptographic technique. Basically they have given two mapping i.e. users to roles and roles to privilege on data objects. This method keeps sensitive information of user in private cloud and data files in public cloud.
9) W. Jia et al.[9] introduced a secure data sharing mechanism known as secure mobile user-based data service mechanism (SDSM) which is based on identity based proxy re-encryption scheme. Initially user encrypts the data and then forwards the cipher text as well as access control capability to the public cloud. The cost of access policy updating is low.
10) V.Sathana, J.Shanthini et al.[10] proposed Enhanced Security System for Dynamic Group in Cloud which use AES encryption while uploading the data. Initially user has to select text based password according the OTP is generated automatically and sent to associated email account of the user. The main advantage of this system is encryption computation cost as well as storage overhead are independent according to the number of revoked users. It also provides multiple levels of security. The limitation of this system is computation overhead is high.
11) Ameena Mehar, M. S. V. V. Ramesh et al.[11] proposed A Cloud Security Framework For Data Sharing In Dynamic Groups which focuses on revocation of the user. They have designed a framework where revocation is achieved using revocation list without updating private keys of rest of the users. But new users can also decrypt file before their actual participation.
12) Tresorium: cryptographic file system for dynamic groups over untrusted cloud is proposed where file are encrypted before uploading to cloud and hence CSP has not a chance to access the data. It also supports ACL-like abstraction. It uses key lock- boxes and a lazy re-encryption approach for handling modification of files

and to do changes in group membership. But this design has weak backward secrecy.[12]

13) A Novel Approach towards Cost Effective Region-Based Group Key Agreement Protocol for Secure Group Communication is proposed by kumar et al. [13] which provides Policy based file renewal. Attribute Based Encryption scheme with RSA key private- public key combination is used for providing access to files. But it does not provide Multi Authority Attribute based Encryption.

3. Comparison of Various Methods

The table 1 describes various methods and parameter that are used in the group communication. The most of the approaches used the public cloud for data storage. Each concept basically states the group communication in a secured way by allowing the proxy signature technique in some methods. The table also states the basic principal used for a group communication

4. Problem Addressed

The existing system has some drawbacks

1) It does not provide Multi Authority based Attribute based Encryption.
2) Previous scheme provide weak backward secrecy. Backward secrecy means group leaving member will Unable to access the files uploaded by other member and will unable to know the group key pair
3) New users can directly decrypt files stored in the cloud before their participation. This will result in the weak forward secrecy.
4) Though the communication between different users doesn't reveal any privacy information, it does not provide low computational overhead
5) Though the communication is secure but to provide robustness backup of the group leader data is stored.

5. Conclusion

The approaches that are used are different from the traditional group communication. It achieves the security issues in some extend. Basically it provides the secure uploading and downloading of the files within the group. This could be achieved by encrypting the keys along with the data and then the grant the permission to access the data, which can be revoked at any time. Also it is possible to update the group key pair even though not all the members of group are online.

References

[1] D.H.Tran,H.-L.Nguyen,W.Zha,andW.K.Ng,—Towards security in sharing data on cloud-based social networks,‖ in ICICS 2011: Proc. 8th International Conference on Information, Communications and Signal Processing. IEEE CS, 2011.

[2] P. Tysowski and M. Hasan, —Hybrid attribute -and re-encryptionbased key management for secure and scalable mobile applications in clouds,‖ IEEE Transactions on Cloud Computing, vol. 1, no. 2, pp. 172–186, 2013.

[3] Kan Yang, Xiaohua Jia —Privacy -Preserving Data Publish-Subscribe Service on Cloud-based Platforms‖, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 1, pp. 131–143, Jan. 2013

[4] Kaitai Liang, Man Ho Au, —A DFA -Based Functional Proxy ReEncryption Scheme for Secure Public Cloud Data Sharing‖, IEEE Transactions on Information Forensics and Security, vol. 9, no. 10, October 2014 .

[5] Mohamed Nabeel , Elisa Bertino, —Privacy Preserving Delegated Access Control in Public Clouds‖ IEEE Transactions On Knowledge And Data Engineering, Vol. 26, No. 9, September 2014.

[6] Xinyu Lei , Xiaofeng Liao, — Outsourcing Large Matrix Inversion‖.

[7] Huaqun Wang, —Proxy Provable Data Possession in Public Clouds‖ IEEE Transactions On Services Computing, Vol. 6, No. 4, OctoberDecember 2013 .

[8] Lan Zhou, Vijay Varadharajan,, " Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage ", IEEE Transactions On Information Forensics And Security, Vol. 8, No. 12, December 2013.

[9] W. Jia, H. Zhu, Z. Cao, L. Wei, and X. Lin, —SDSM: A secure data service mechanism in mobile cloud computing,‖ in WKSHPS 2011: Proc. 2011 IEEE Conference on Computer Communications Workshops. IEEE CS, 2011, pp. 1060–1065

[10] Sathana, V. (2014). Enhanced Security System for Dynamic Group in Cloud, 4(3), 37–42.

[11] Mehar, A., Ramesh, M. S. V. V, & Suribabu, D. D. D. (2014). A cloud security framework for data sharing in dynamic groups, (10), 652–658.

[12] Lam, Irma, Szilveszter Szebeni, and Levente Buttyán. "Tresorium: cryptographic file system for dynamic groups over untrusted cloud storage."Parallel Processing Workshops (ICPPW), 2012 41st International Conference on. IEEE, 2012.

[13] Kumar, Krishnan, and V. Sumathy. "A novel approach towards cost effective region-based group key agreement protocol for secure group communication." arxiv preprint arxiv:1007.0087 (2010).

[14] 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.

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

[16] 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.

[17] 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.