ISSN 2395-1621

Secure Dynamic Group Data sharing for Multi-owner in Cloud

[#1]Nilam Jadhav,[#2]Vidya Bhatane,[#3]Madhuri Shinagare,[#4]Pooja Kundekar

[1]nilam9793@gmail.com
[2]vidyabhatane15@gmail.com
[3]madhurishinagare@gmail.com
[4]poojakundekar94@gmail.com

[#1234]Department of Computer Engineering,PVPIT, Pune-41

ABSTRACT

Cloud Computing provides the services over the Internet. It provides economical and efficient solution for sharing group resources. Unfortunately sharing data from untrusted cloud .While preserving data and identify privacy is challenging issue in multi-owner system because of Dynamic membership.In this paper, we propose secure dynamic group data sharing for multi-owner in cloud by using group signature and dynamic broadcast encryption technique.Encryption computation cost and storage overhead of our scheme are independent with number of revoked users . We demonstrate efficiencyandanalyse the security of our scheme with rigorous proof.

Keywords: Cloud computing,Data sharing,Dynamic Group, Access Control,Privacy Preserving.

ARTICLE INFO

Article History

Received :15th April 2016

Received in revised form :

17th April 2016

Accepted : 19th April 2016

Published online :

23rd April 2016

I. INTRODUCTION

Cloud is nothing but the internet based computing. Which provides the storage of data in very lower cost & available for all time over the internet[8]. Also it provides shared resources, software & information of computer and devices on demand. In cloud computing the cloud service provides various services for users. Such as, amazon with their powerful datacenters.so users can enjoy high quality services. Cloud provider provides the major service is data storage. One organization allow its staff member to store and share data files within a same group or department in cloud. By using the cloud staff members completely free from the troublesome maintenance and local data storage.But it may create problem for confidentiality of those stored files. Particularly, the cloud servers managed by cloud providers which are not fully trusted by user. The data files shared in cloud may be sensitive andconfidential, may be business plan. To handle the data privacy, one of the solution is encrypt all the data files and then that encrypted data uploaded into the cloud. Unfortunately, design of an efficient and secure data sharing method for group in cloud is not an easy task. It has following challenging issues.First is the identity privacy ,It is the one of the major obstacle in the cloud computing. Without giving the guarantee of identity privacy, the users are not intrested to join in cloud computing system. Because when dispute occurs, the real identity of users could be easily disclosed by cloud providers or attackers. On the other hand, unconditional identity privacy may be create the obuse of privacy. For example, the misbehaved staff can generate the fake files in company without being identified. Therefore identification enables group manage to reveal the real identification of the user is also highly adorable.

Second thing is multi-owner manner in which all group members can efficiently sharing services and data files with others also can fully enjoy the data storing. In single owner only group manager can store and update data files in cloud, but multiowner manner system is more flexible in practical application[2]. In this each and every user in the group can store and modify the data shared by the company.

The last is the dynamic groups.The new staff can join the company and current employee can revoke the company. The changes of membership may create problem for the data security. Here we have some issues one is the newly joined user can directly decrypt the data without

contact the data owners and second thing is there is no need to update the secret key of other users when any user revoked from the company. It minimizes the complexity of key management.

With the number of data owner and revoked user linearly increasing the complexities of new user participation and user revocation repeatedly. Lu et al.[6] proposed secure provenance scheme based on cipher text attribute based encryption technique. By setting a group with single attribute which allows all member of the group to share data with others. However, user revocation is not mentioned in this scheme. Yu et al.[2] proposed scheme for the scalable and fine grained data access control in cloud computing system by using KP-ABE technique.In this single owner method is presented where the user can store and share the data.

To overcome with above described challenges we propose the Secure dynamic group data sharing for multi-owner in cloud.

II. LITERATURE SURVEY

In [5],Wang et al. proposed a privacy preserving public auditing for secure cloud storage with large groups. In this group signature is utilize to compute verification information on shared data. Because of that TPA able to audit the correctness of shared data but it cannot reveal the identity of the signer on each block. TPA may handle multiple audit session for different users. By using private key of group manager the original user can efficiently add new user in the group and disclose the identities of signers on all block.

In [4], Waters et al. proposed scheme for one grained sharing of encrypted data they develop new cryptosystem that call key-policy attribute based encryption (KP-ABE). In cryptography, a cipher texts are labelled with set of attributes & private keys are associated with access the control. In hierarchical identity-based encryption supportsdelegation of private keys. The data owner uses a random key which is encrypted with a set of attributes using KP-ABE. The group manager assigns a secret key to authorized users by using that key users can only decrypt a ciphertext. To achieve user revocation manager can update the users secret key to cloud server. By using this a single owner ,any member in a group should be allowed to store & share data files with others.

In[3],Goyal et al. presented fine grained access control, set of users allows the flexibility in specifying the access. Secret sharing schemes are used to divide a secret for a set of parties who should be able to reconstruct the secret by using their shares. The identity based encryption is also called as fuzzy identity based encryption (FIBE). In this identity is viewed as a set of attributes FIBE is allows a private keys.one disadvantage of encryption data is that ability of users to share their encrypted data at a fine-grained level.In[7],Atenise et al. proposed scheme for encrypted file systems fast and secure re-encryption schemes that realise a stronger notion of security and proxy re-encryption as a method of adding access control to a secure file system. In this only limited amount of trust is placed in the proxy. For example, it is not able to decrypt the cipher texts it re-encrypt, and we prove our schemes secure even when the proxy publishes all the re-encryption information it knows. These schemes realise the proxy re-encryption is giving proxy capabilities to the key server of a confidential distributed file system.

In[2], Yu et.al proposed secure , scalable and fine grained data access control scheme in cloud computing by utilizing the KP-ABE technique.In this by using the rand key data owner decrypt the file where that random key is again encrypted with group of attributes using KP-ABE and respected secret key to the authorized users.If the data files attributes match with access structure then only user can decrypt the cipher text for achieving the user revocation. The cloud servers takes the responsibility from managers of the task such as update secret key and file re-encryption.In this all the users can share data with others so because of that single owner manner may create the problem with implementation of application.

III.SYSTEM ARCHITECTURE

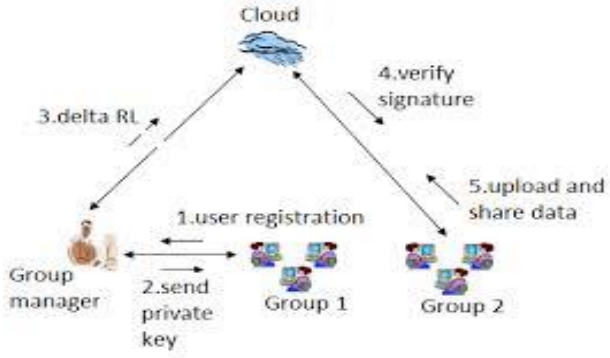

Fig: System Model

In this,we consider cloud computing architecture by combining with an example that a organization or company uses cloud which allow it's staff in same group or department to share files.

The System model consist of three entities.The cloud,group manager(i.e. company manager) and number of group member(i.e. staff).

Cloud service provider provides the cloud and storage services.But cloud is not fully trusted,since the CSP are very likely to be outside of cloud user's trusted domain. Similarly,[2][6] we Consider that cloud server is honest but curious.That is due to the protection of data auditing schemes [5] the cloud server will not maliciously delete or modify user data but it will try to know the identity of cloud user and content of stored data.

Group Manager take the charge of system parameter initialization,new user registration,user revocation and revealing the identity of user when dispute occurs.In the given example,the group manager acts as a administrator of the organization or company. Therefore we consider that the group manager is fully trusted by other parties.

Group member are nothing but set of registered users that will store the data into the cloud and share with other group members.In the given example the staff acts as a group members. The group members are dynamically change,because of new employee participation and current employee revocation.

Design goals:
The main design goals of proposed schemes are access control,data confidentiality,anonymity,traceability and efficiency.

Access Control:
Group member uses the cloud for data operations and unauthorized user will not access the cloud resources any time . Once user revoked,that revoked user will be incapable of using cloud again.

Data Confidentiality:
Data confidentiality requires that unauthorized users cannot learn the content of stored data. Data confidentiality is challenging issue due to dynamic group. Specifically before the user participation new user should decrypt the data stored in the cloud and after revocation revoke user unable to decrypt the data moved into the cloud.

Anonymity and Traceability:
Anonimity guarantees that group members in a group can access the cloud without revealing the real identity ,it also provides an protection for user identity.Anonymity poses a protected inside attack to the system. Means inside attack may store and share wrong information to derive substantial benefit. Therefore ,to tackle that inside attacker,the group manager able to reveal the real identifies of data owner.

Efficiency:
Efficiency is nothing but all group member can store and share the data with other within a groups by using cloud. User revocation is achieved without involving the remaining users, Means there is no need to update private keys of remaining users. Newly joined user can decrypt the data files before the participation without contacting with data owner.

IV. CONCLUSION

In this user, we design a secure data sharing in dynamic group for multi-owner in untrusted cloud. It allows user to store and share data with other users in same group without revealing the identity of users. It also supports new user participation and user revocation efficiently. Specially, user revocation is achieved by using the revocation list without updating the secret key of remaining users and new user can directly decrypt the files before participation in cloud storage.

REFERENCES

1. Xuefeng Liu, Yuqing Zhang, Member, IEEE, Boyang Wang, and Jingbo Yan," Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", VOL. 24, NO. 6, JUNE 2013.

2. 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.

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

4. B. Waters, "Ciphertext-Policy Attribute-Based Encryption: An Expressive, Efficient, and Provably Secure Realization," Proc. Int'l Conf. Practice and Theory in Public Key Cryptography Conf. Public Key Cryptography, http://eprint.iacr.org/2008/290.pdf, 2008.

5. 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.

6. 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.

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

8. 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.

