International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

A Efficient Data Sharing Scheme for Dynamic Groups in the Cloud

Fasi Ahmed Parvez & K. Pallavi

[1] Assistant Professor & HOD ,Department of CSE, Balaji Institute of Technology & science, Warangal District, Telangana, India.

[2] M.Tech Student, Department of CSE, Balaji Institute of Technology & science, Warangal District, Telangana, India

Abstract:

As per the rapid growth and essentiality for providing security in cloud. In this we propose A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud by using Identity based Encryption. Meanwhile, we must provide security guarantees for the sharing data files since they are outsourced. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue, especially for an untrustedclouddue to the collusion attack.Firstly, we propose a safe route for key dispersion with no safe correspondence channels, and the clients can safely acquire their private keys from gathering administrator. Besides, the plan can accomplish fine-grained access control, any client in the gathering can utilize the source in the cloud and refused clients can't get to the cloud again after they are rejected. Thirdly, we can protect the plan from trickery attack, which implies that rejected clients can't get the first information record regardless of the possibility that they scheme with the untrusted cloud. In this methodology, by utilizing polynomial capacity, we can achieve a protected client denial plan.

Keywords: Access control, Privacy-preserving, Key distribution, Cloud computing

1. Introduction:

Intrinsic resource sharing and low maintenance characteristics the cloud computing is an alternative to traditional information technology. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. For the data privacy it is important to encrypt the data and upload the encrypted data on the cloud. In cloud it is not easy to design efficient and secure data sharing scheme in multi owner system due to the following challenging issues. Identity, revocation and new member participation i.e. the changes of membership make securely data sharing extremely difficult.

On the other hand an efficient member revocation without updating the secret key of remaining user to minimize the complexity of key management. Signed receipt is caused after every member revocation in group that minimizes multiple copy of encrypted file it can help to minimize computation cost.

2. Literature Survey:

- Kallahalla et al presented a cryptographic storage system that enables secure data sharing on untrustworthy servers based on the techniques that dividing files into file groups and encrypting each file group with a file-block key.
- Yu et al exploited and combined techniques of key policy attribute-based encryption, proxy re-encryption and lazy re-encryption to achieve fine-grained data access control without disclosing data contents.
- C. Wang, Q. Wang, K. Ren, and W. Lou presented To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements. To support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously.

3. Existing System:

The file-block keys need to be updated and distributed for a user revocation; therefore, the system had a heavy key distribution overhead. The complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners and the revoked users. The single-owner manner may hinder the implementation of applications, where any member in the group can use the cloud service to store and share data files with others.

4. Proposed System:

In this paper, we propose a secure data sharing scheme, which can achieve secure key

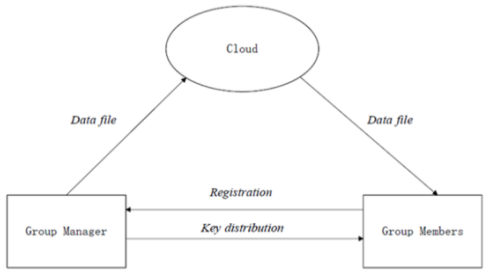
distribution and data sharing for dynamic group. We provide a secure way for key distribution without any secure communication channels. The users can securely obtain their private keys from group manager without any Certificate Authorities due to the verification for the public key of the user. Our scheme can achieve fine-grained access control, with the help of the group user list, any user in the group can use the source in the cloud and revoked users cannot access the cloud again after they are revoked. We propose a secure data sharing scheme which can be protected from collusion attack. The revoked users can not be able to get the original data files once they are revoked even if they conspire with the untrusted cloud. Our scheme can achieve secure user revocation with the help of polynomial function. Our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated. We provide security analysis to prove the security of our scheme.

4.1 Advantages of Proposed System:

- The computation cost is irrelevant to the number of revoked users in RBAC scheme. The reason is that no matter how many users are revoked, the operations for members to decrypt the data files almost remain the same.
- The cost is irrelevant to the number of the revoked users. The reason is that the computation cost of the cloud for file upload in our scheme consists of two verifications for signature, which is irrelevant to the number of the revoked users. The reason for the small computation cost of the cloud in the phase of file upload in RBAC scheme is that the verifications between communication entities are not concerned in this scheme.
- In our scheme, the users can securely obtain their private keys from group manager Certificate Authorities and secure communication channels. Also, our scheme is able to support dynamic groups efficiently, when a new user joins in the group or a user is revoked from the group, the private keys of the other users do not need to be recomputed and updated.

4.2 System Model:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018



The System model consist of Cloud, Group Manager and Group member.

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.

Group Manager Module :

Group manager takes charge of followings:

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

Therefore, we assume that the group manager is fully trusted by the other parties. The Group manager is the admin. The group manager has the logs of each and every process in the cloud. The group manager is responsible for user registration and also user revocation too.

3.Group Member Module :

Group members are a set of registered users that will

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

Note that, 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 they can also modify it.

Screen Shots:

Fig: Cloud Home Page

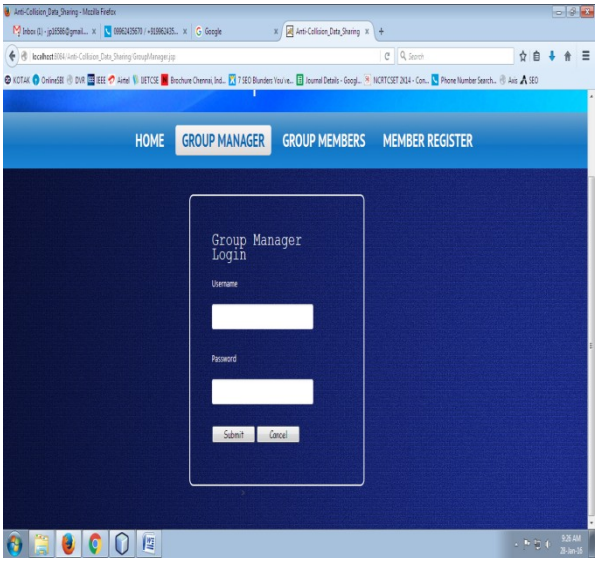


Fig: Group Manager Login page

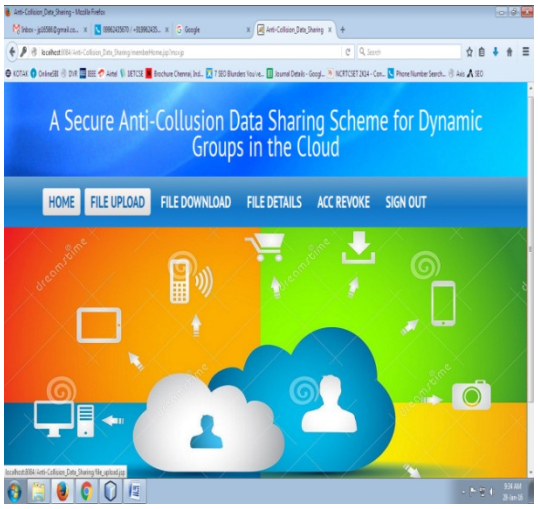


Fig: File Upload

5. Conclusion:

In this paper, we design a secure anti-collusion data sharing scheme for dynamic groups in the cloud.In our plan, the clients can safely acquire their private keys from gathering director Certificate Authorities and secure correspondence channels. Likewise, our plan can bolster dynamic gatherings proficiently, when another client joins in the gathering or a client is denied from the gathering, the private keys of alternate clients don't should be recomputed and redesigned.

6. 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. PublicKey Cryptography, 2008, pp. 53–70.

[10] X. Liu, Y. Zhang, B. Wang, and J. Yang,―Mona: Secure multi owner data sharing for
dynamic groups in the cloud,‖ IEEE Trans.ParallelDistrib. 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 multi owner data sharing for
dynamic groups in the cloud,‖ in Proc. Int. Conf.DOI:
10.18535/ijsrm/v5i7.08MutyalaRamya
Krishna, IJSRM Volume 5 Issue 07 July 2017 [www.ijsrm.in] Page 5841Inf. 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.

[17] D. Dolev and A. C. Yao, ―On the security of public key protocols,‖ IEEE Trans. Inf. Theory, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[18] B. Dan and F. Matt, ―Identity-based encryption from the weil pairing,‖ in Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol., 2001,vol. 2139, pp. 213–229.

Fasi Ahmed Parvez is 15+ years experienced Assistant Professor & HOD in the Department of Computer Science & Engineering at BALAJI INSTITUTE OF TECHNOLOGICAL SCIENCES-NARSAMPET, Warangal, India and his research area includes Data Mining.

K. Pallavi Currently doing M.Tech in Computer Science & Engineering at BALAJI INSTITUTE OF TECHNOLOGICAL & SCIENCES-NARSAMPET, Warangal, India. Her research interests includes Cloud Computing, Network Security, Mobile Computing, etc