Data Handling Between Dynamic Groups

Mr. Jaya S Pujar
Lecture, Department of Computer Science & Engineering,Krishna Murthy Institute of Technology And Engineering, Ghatkesar

ABSTRACT

The characters of low maintenance and little management cost, cloud computing offers an effective and economical approach for data sharing in the cloud among group members. However, since the cloud is untrustworthy, the security guarantees for the sharing data become our concerns. Unfortunately, because of the frequent change of the membership, sharing data while providing privacy-preserving is still a challenging issue. It will easily suffer from the collusion attack, which can lead to the revoked users getting the sharing data and disclosing other legitimate members' secrets.

Keywords- User Revocation; Access control; privacy-preserving; cloud computing;

I. INTRODUCTION

Cloud computing, with the characteristics of intrinsic data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud servers provide a infinite storage space for users to store data. It can help clients lessen their financial output of data managements by outsourcing the local storage into the cloud. However, as we now upload data to the cloud, we lose the physical control of the data storage. To achieve privacy- preserving, a common approach is to use cryptography data files before the clients outsource the sensitive data to the cloud. It is difficult to design a secure and efficient data sharing scheme, especially for dynamic members.

II. PROBLEM STATEMENT

- In the existing system data owners store the encrypted data files in the untrusted storage and distribute the corresponding decryption keys only to authorized users.
- The unauthorized users as well as storage servers cannot access the content of the data files because servers have no knowledge of the decryption keys.
- However, the complexities of user participation and revocation in these schemes are linearly increasing with the number of data owners.
- The changes of membership make secure data sharing extremely difficult the issue of user revocation is not addressed.
- Identity privacy plays a major role, users may be unwilling to join in cloud computing systems.
- It is not possible to trace which user converts as a false file.
- The storage overhead and the encryption computation cost increases with the no of users.

III. METHODOLOGY

Cloud Module

Cloud provides 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 system parameters generation, user revocation, user registration, revealing the identity of dispute data owner.

Group Member Module:

Group members are a set of registered users that will store their private data into the cloud server and share them with others in the group. The group membership is dynamically changed, due to the staff resignation and new employee participation in the company.

File Security Module:

It includes encrypting the data file using Advanced Encryption Standard (AES) and Data Encryption Standard (DES). The files stored in the cloud can be deleted by either the group manager or the data owner.

Group Signature Module:

A group signature scheme allows any member of the group to sign messages while keeping the identity secret from verifiers.

User Revocation Module:

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. A secure data sharing scheme for dynamic groups can be used

IV. IMPLEMENTATION

This project provides security for multi-owner data sharing scheme. User revocation is achieved through a revocation list without updating the secret keys of the remaining users. The size and computation overhead of encryption are constant and independent with the number of revoked users. The real identities of data owners is revealed by group manager when disputes and also to avoid anti-collusion of data by managing keys. Efficiently share data between multiple users.

V. EXPERIMENTAL RESULTS

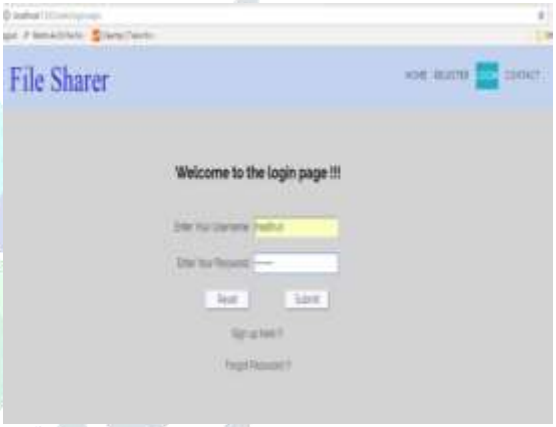

Figure 1: Login page

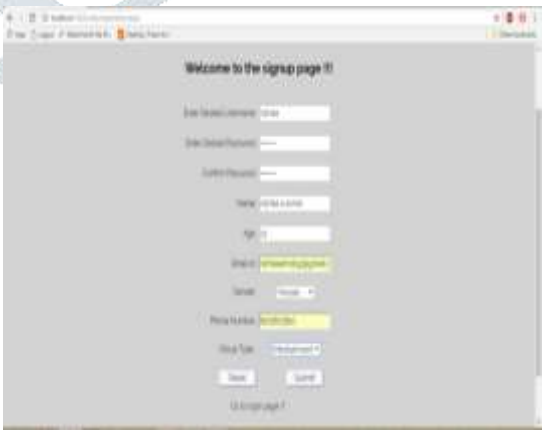

Figure 2: Creating an account

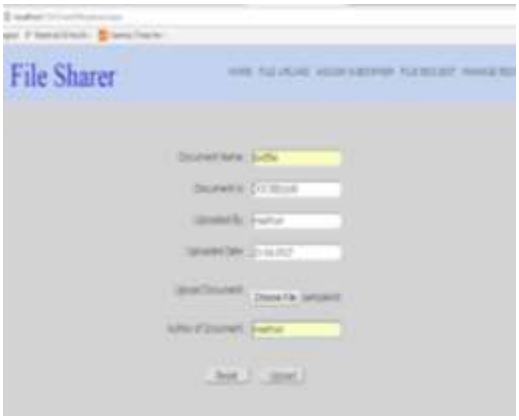

Figure 3: Upload Page

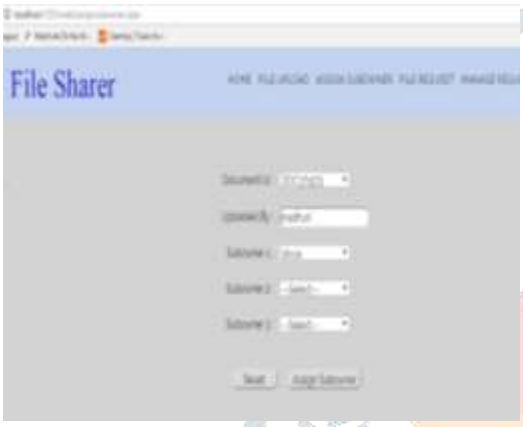

Figure 4: Assign Sub ownership

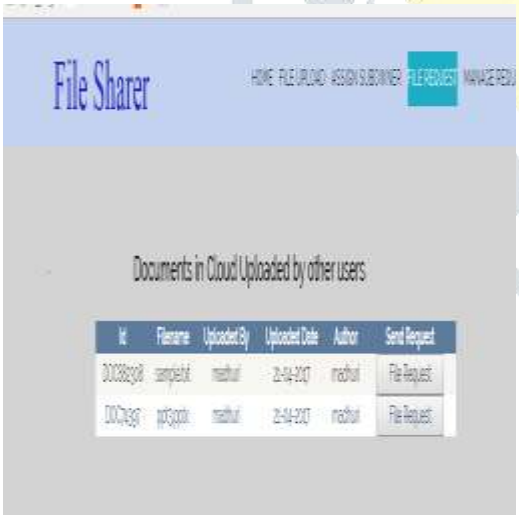

Figure 5: File Request

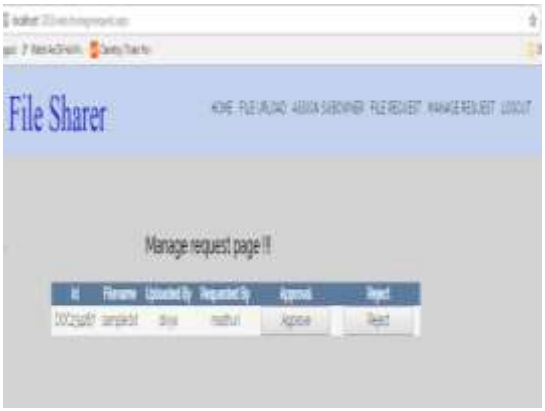

Figure 6: Manage Request

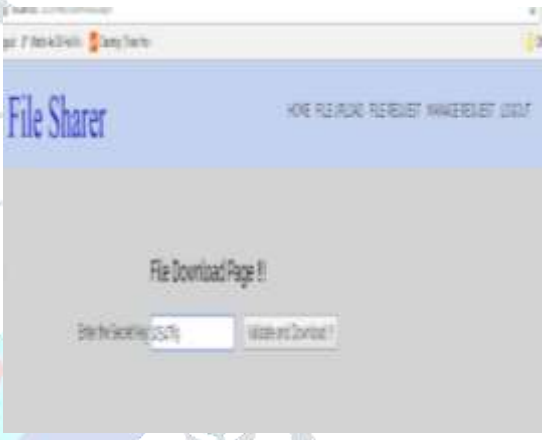

Figure 7: Download page

VI. CONCLUSION

Secure data sharing scheme for dynamic groups in an untrusted cloud will be designed. A user is able to share data with others in the group without revealing identity privacy to the cloud. Supports efficient user revocation. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. Extensive analyses show that our proposed scheme satisfies the desired security requirements and guarantees efficiency as well.

VII. ACKNOWLEDGEMENT

We would like to thank Dr. ReshmaBanu, Head of the department, Information Science and Engineering, GSSSIETW, Mysuru for her guidance and consistent support. We would also like to thank our guide Chaya P for her guidance and consistent support. We would also like to thank all the teaching and non-teaching staff members of Information Science and Engineering, GSSSIETW, Mysuru for their constant support and co-operation.

VIII. REFERENCES

[1] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," Ieee Internet Computing, vol. 16, no. 1, pp. 69–73, 2012.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in IEEE INFOCOM 2010

[3] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yang, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 6, pp. 1182-1191, June 2013

[4] 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.

[5] Lan Zhou, Vijay Varadharajan, and Michael Hitchens, "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage," IEEE Transactions on Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, December 2013.

[6] 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 " Cryptographic Cloud Storage".

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

[8] M. Kallahalla, E. Riedel, R. Swami Nathan, 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] Zhongma Zhu, Rui Jiang, "A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud", IEEE Transactions on Parallel and Distributed Systems, 2015.

[10] 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.

[11] M. Kavitha Margret, "Secure Policy Based Data Sharing for Dynamic Groups in the Cloud" ISSN: 2278 – 1323 International Journal of Advanced Research in Computer Engineering and Technology (IJARCET) Volume 2, Issue 6, June 2013 (Access on dated:13-sep-2013).

[12] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," in Proc. of NDSS, 2005, pp. 29-43.

[13] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance:The Essential of Bread and Butter of Data Forensics in CloudComputing,", in Proc. of AISIACCS, 2010, pp. 282-292.

[14] C. Delerablee, P. Paillier, and D. Pointcheval, "Fully Collusion Secure Dynamic Broadcast Encryption with Constant-Size Ciphertexts or Decryption Keys," Proc. First Int'l Conf. Pairing-Based Cryptography, pp. 39-59, 2007.

[15] D. Chaum and E. van Heyst, "Group Signatures," in Proc. Of EUROCRYPT, 1991, pp. 257-265.

[16] A. Fiat and M. Naor, "Broadcast Encryption," in Proc. Of CRYPTO, 1993, pp. 480-491.

[17] 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.

[18] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[19] Dan Boneh and Matthew K. Franklin. Identity-based encryption from the Weil pairing. In Joe Kilian, editor, CRYPTO 2001, volume 2139 of LNCS, pages 213–229, Santa Barbara, CA, USA, August 19–23, 2001. Springer-Verlag, Berlin, Germany.

[20] Yevgeniy Dodis and Nelly Fazio. Public key trace and revoke scheme secure against adaptive chosen ciphertext attack. In Yvo Desmedt, editor, PKC 2003, volume 2567 of LNCS, pages 100–115, Miami, USA, January 6–8, 2003. Springer-Verlag, Berlin, Germany

[21] 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.

[22] Eiichiro Fujisaki and Tatsuaki Okamoto. How to enhance the security of public-key encryption at minimum cost. In Hideki Imai and Yuliang Zheng, editors, PKC'99, volume 1560 of LNCS, pages 53–68, Kamakura, Japan, March 1–3, 1999. Springer-Verlag, Berlin, Germany.

[23] Antoine Joux and Kim Nguyen. Separating decision Diffie-Hellman from computational diffie-hellman in cryptographic groups. Journal of Cryptology, 16(4):239–247, 2003

[24] Dani Halevy and Adi Shamir. The LSD broadcast encryption scheme. In Moti Yung, editor, CRYPTO 2002, volume 2442 of LNCS, pages 47–60, Santa Barbara, CA, USA, August 18–22, 2002. Springer-Verlag, Berlin, Germany.

[25] N. Cao, S. Yu, Z. Yang, W. Lou, and Y. T. Hou, "LT Codes-Based Secure and Reliable Cloud Storage Service," Proc. IEEE INFOCOM,2012.

[26] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.

[27] Y. Zhu, H. Wang, Z. Hu, G. -J. Ahn, H. Hu, and S. S Yau,"Dynamic Audit Services for Integrity Verification of Outsourced Storages in Clouds," Proc. ACM Symp. Applied Computing (SAC'11), pp. 1550-1557, 2011.

[28] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-610, 2007.

[29] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009