

# Review: A Secure Anti-Collusion Data Sharing Scheme for Dynamic Groups in the Cloud

Mohd.Zameer<sup>1</sup> Prof. Nitin Choudhary<sup>2</sup>

<sup>1</sup>Student <sup>2</sup>Assistant Professor

<sup>1,2</sup>Department of Computer Science & Engineering

<sup>1,2</sup>Kopal Institute of Science & Technology, Bhopal (M.P), India

**Abstract**— Cloud computing provide security, insuring for the transformation of data file. Unfortunately, because of the repeatedly changes of the membership, sharing data while providing privacy-preserving is still a challenging issue, mainly for an untrusted cloud due to the collusion attack. Moreover, for occurring schemes, the security of key distribution is based on the secure communication channel, however, to have such channel is a strong presumption and is difficult for practice. In this paper, review on a safe information sharing plan for dynamic members. Our scheme is proposed a type of fine efficiency, which means previous users need not to update their private keys for the situation either a new user joins in the group or a user is revoked from the group.

**Key words:** Cloud Computing, Security, Private Keys, Public Keys

## I. INTRODUCTION

Cloud computing, having characteristics of inherent data sharing and low maintenance, provides a better utilization of resources. In cloud computing, cloud service providers offer an abstraction of infinite storage space for clients to host data. By storing their data into the cloud, the data owners can be relieved from the burden of data storage and maintenance, so as to enjoy the on-demand high quality data storage service cloud server are not in the same trusted domain may put the outsourced data at risk. To preserve data privacy, a common approach is to encrypt data files before the clients upload the encrypted data into the cloud. Unfortunately, it is difficult to design a secure and efficient data sharing scheme, especially for dynamic groups in the cloud. Below figure show System model of Key Exchange

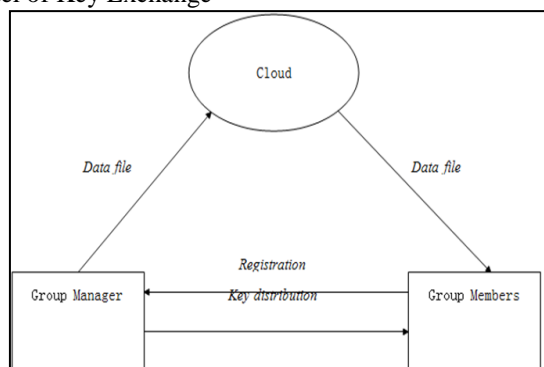


Fig. 1: System Model

The system model consists of three different entities: the cloud, a group manager and a large number of group members. The clouds, sustaining by the cloud service providers, provides storage space for hosting data files in a pay-as-you-go manner. On the other hand, the cloud is untrusted since the cloud service providers are easily to become untrusted. Therefore, the cloud will try to learn the

content of the stored data. Group manager will obtain charge of system parameters generation, user registration, also, client repudiation. Bunch individuals (clients) are an arrangement of sign up clients that will store their own particular information into the cloud and impart them to others. In the plan, the gathering enrollment is powerfully changed, because of the new client call-up and client denial.

## II. LITERATURE SURVEY

Miss. Dive Pratibha, Miss. Pinjari Afrin, Miss. Kadam Pallavi, Miss. Kaygude Shital Author propose a novel server-side de-duplication scheme for encrypted data. It allows the cloud server to control access to outsourced data even when the ownership changes dynamically by exploiting randomized convergent encryption and secure ownership group key distribution. The proposed scheme guarantees data integrity. Proof-of-ownership scheme allows any owner of the same data to allow to cloud server that he owns the data in robust way.

Wee Keong Ng, Yonggang Wen, Huafei Zhu Author show that the proposed private data reduplication protocol is provably secure assuming that the underlying hash function is collision-resilient, the discrete logarithm is hard and the erasure coding algorithm can erasure up to  $\alpha$ -fraction of the bits in the presence of malicious adversaries in the presence of malicious adversaries. To the best our knowledge this is the first reduplication protocol for private data storage.

Wei Song, Hua Zou, Haowen Liu, Jun Chen Author enable the authenticated users to access the encrypted cloud data, a practical group key management algorithm for the cloud data sharing application is highly desired. The existing group key management mechanisms presume that the server is trusted. But, the cloud data service mode does not always meet this condition. How to manage the group keys to support the scenario of the cloud storage with a semi-trusted cloud server is still a challenging task. Moreover, the cloud storage system is a large-scale and open application, in which the user group is dynamic. To address this problem, we propose a practical group key management algorithm based on a proxy re-encryption mechanism in this paper.

## III. PROBLEM STATEMENTS

Data security requires that unauthorized users including the cloud are not able to learn the content of the stored data. To maintain the availability of data privately for dynamic groups is still an important and challenging issue. Specifically, withdraw users are not able to decrypt the stored data file after the revocation.

A cryptographic storage system that enables assured data sharing on dishonest servers based on the techniques that dividing files into file groups and encrypting each file category with a file-block key.

#### IV. CONCLUSION

In this review paper, we reviewed a protected against agreement information sharing plan for element bunches in the cloud. Enterprises or individuals use cloud storage services to share data, the most concerning issue is data security and privacy. We can do in future propose a novel and practical group key management algorithm for encrypted cloud data sharing with dynamic groups. Considering a semi-trusted cloud server, our design does not depend on a trusted third party entity or a secure communication channel.

#### REFERENCES

- [1] Miss. Dive Pratibha , Miss. Pinjari Afrin , Miss. Kadam Pallavi , Miss. Kaygude Shital “Secure Data-Deduplication with Dynamic Ownership Management in Cloud Storage” Volume 5 Issue III, March 2017 IC Value: 45.98 ISSN: 2321-9653
- [2] Wee Keong Ng, Yonggang Wen, Huafei Zhu“Private data deduplication protocols in cloud storage”SAC’12, March 25-29, 2012, Riva del Garda, Italy. Copyright 2012 ACM 978-1-4503-0857-1/12/03 ...\$10.00.
- [3] Wei Song, Hua Zou , Haowen Liu, Jun Chen”A Practical Group Key Management Algorithm for Cloud Data Sharing with Dynamic Group”China Communications • June 2016.
- [4] 4.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,” *Comm. ACM*, vol. 53, no. 4, pp. 50-58, Apr.2010.
- [5] 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.
- [6] Zhongma Zhu, Zemin Jiang, Rui Jiang, “The Attack on Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud,” *Proceedings of 2013 International Conference on Information Science and Cloud Computing (ISCC 2013)*, Guangzhou, Dec.7, 2013, pp. 185-189.
- [7] Shucheng Yu, Cong Wang, Kui Ren, and Weijing Lou, “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” *Proc. ACM Symp. Information, Computer and Comm. Security*, pp. 282-292, 2010.
- [8] 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
- [9] 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
- [10] Xukai Zou, Yuan-shun Dai, and Elisa Bertino, “A practical and flexible key management mechanism for trusted collaborative computing,” *INFOCOM 2008*, pp. 1211-1219.