ISSN: 2321-7782 (Online)
Impact Factor: 6.047

Volume 4, Issue 5, May 2016

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Efficient and Secure Multi Owner Data Sharing Scheme with Load Balancing for Dynamic Groups in the Cloud

Rajendra Kumar
Department of Computer Science
Jamia Millia Islamia
New Delhi – India

Abstract: One of the primal services offered by cloud computing is data sharing. Data sharing is sometimes a crucial requirement, for businesses and organizations and becoming increasingly important for many users. Cloud computing provides an efficient and economical solutions for sharing resources between users with characteristics of low maintenance. Due to frequently change in the membership, the sharing of data in multi-owner manner while preserving data and privacy from un-trusted cloud is still a challenging issue. The main problem of existing MONA Scheme is to stop working of the group manager due to not able to handle the large number of requests coming from various groups of owners. In this paper, we propose an efficient and secure load balancing multi-owner data sharing scheme for dynamic group in the cloud.

Keywords: Cloud computing, Data sharing, load balancing, multi-owner, dynamic group.

I. INTRODUCTION

The rapid development of cloud computing technology enables users depositing their data and application on the cloud. However the numerous cloud security problems create hindrance to the development of cloud computing. The Cloud computing is used to compute and outsource the data of organizations in cost effective and flexible manner. One of the primal services offered by cloud computing is data sharing. Data sharing is sometimes a crucial requirement, for businesses and organizations and becoming increasingly important for many users.

The cloud computing in general is a kind of Internet-based computing where different services such as storage, servers and applications are delivered to an organization's through the Internet. Data sharing and storage are the most fundamental services offered by cloud providers. In cloud computing, the cloud service providers are able to deliver various services to cloud users or organizations through powerful datacenters. Data storage and sharing in cloud possess some risk to confidentiality. To preserve the privacy of data, user can encrypt the data files before uploading it to the cloud. After encrypting the data files the users can upload the data files into the cloud [1].

Due to so many challenging issues, the development of an efficient and secure data sharing with load balancing scheme for dynamic groups in the cloud is not an easy task [2]. One of the most considerable obstacle for the broad development of cloud computing is the Identity privacy. Without the surety of identity privacy, organizations or users may be unwilling to use the cloud computing systems because the user’s real identities could be easily disclosed to attackers and cloud service providers [2].

The multi-owner manner implies that any user in the dynamic group can securely share the confidential data with other users by the un-trusted cloud. In single-owner manner, only the single user like group manager can modify and store the data in the cloud, whereas in multi-owner manner the many users can simultaneously store and modify the data in the cloud. In many practical applications the multi-owner manner is more flexible than the single-owner [2].

In multi-owner manner each user of the group is not only able to read the data file, but also they can modify their part of data in the entire data file shared by the organization. In the dynamic group the membership change due to joining of the new members in the group and leaving of the older members from the group [2]. To make secure data sharing is extremely difficult due to changing the membership dynamically. The main drawback of existing MONA Scheme is to stop working of the group manager due to not able to handle the bulk number of requests coming from various groups of owners [3].

In this paper, we propose an efficient and secure load balancing multi-owner data sharing scheme for dynamic group in the cloud. Hence in this paper we are extending the basic concept of MONA by dividing the group manager load among the subgroup managers. The subgroup managers handle all the requests coming from group of owners. The subgroup managers pass the information of group of owners to group manager.

The remainder of this paper is organized as follows: the related work is described in Section 2. In Section 3, the proposed scheme is described in detail. The performance analysis is given in section 4. Finally the conclusion of the paper is given in section 5.

II. Related Work

In 2003, the authors, E. Goh, H. Shacham, N. Modadugu, and D. Boneh, proposed a system called “Sirius: Securing Remote Untrusted Storage,”.[1]. In “SIRIUS” a security mechanism is designed that improves networked file system security without any changing to network server or file system. The system is developed to handle multi-user file systems where the files are frequently shared by users. The proposed system is easy for end users to deploy and minimize the trust in file server. In SIRIUS the Files on remote server include two parts: md-file contains the file Meta data and d-file contains the file data.

In 2003, Mahesh Kallahalla, Erik Riedel, Ram Swaminathan, Qian Wang, Kevin Fu, “PLUTUS” , a system is proposed for securely sharing files. It reduces the key exchange between users; access methods i.e. read and write are distinguished, efficiently handles membership changes and allowed to authorize file writes by an un-trusted server. It provides scalable key management to have control on the users who access files of the other users. Study shows that PLUTUS is highly secure than other system.

In 2013, Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, ”MONA”, a scheme is proposed in un-trusted cloud for dynamically created group. In this scheme, user can share data with other members without get to know them their identity. It can also efficiently manage any membership change i.e. joining or leaving. Moreover, when user leaves, it can efficiently manage by the publicly available revocation list without changing the private keys of the existing users. Before any participation, a new user is able to decrypt files stored in the cloud. Storage and computation cost are constant. Proposed scheme provides security and also efficient.

In 2014, P. Kiranmai, Y. Ramu, extend the MONA scheme to achieve more scalability and reliability. The Proposed scheme solves the risk of failure or hanging of group manager due to bulk number of requests coming from group of owners. In the proposed scheme the efficiency, scalability and reliability increases by dynamically increasing the group managers.

In 2010, Shucheng Yu, Cong Wang, Kui Ren, Wenjing Lou proposed a scheme by combining Attribute-Based Encryption(ABE), proxy re-encryption and lazy re-encryption which addresses problems like achieving fine-grainedness, scalability and data confidentiality. This paper defines and enforces access policies and allows data owner to give access of computation task to the un-trusted cloud server without disclosing the data contents. It has features of user secret key accountability and user access privilege confidentiality. Existing survey shows that the proposed scheme is secure and efficient.

By observing above literature we conclude that the main challenging issue in sharing of data in multi-owner manner is how data will be shared securely among various groups of owners in the un-trusted cloud. In this paper we are proposing a scheme for sharing of data between dynamic groups in the cloud computing.

III. PROPOSED SCHEME

In this section, we present a propose approach for handling the problems found in MONA scheme like securely sharing of data among group of owners in multi-owner manner and rebalancing the load of group manager. When there are bulks number of requests came from different group of owners to group manager for registration and simultaneously access the cloud for storing and sharing their respective data files. In this type of scenario the load on the group manager is increases and there may be some chances of failure/hanging of group manager and due to failure of group manager the entire security of MONA will be fail.

3.1 Description of Method

The proposed scheme is designed by dividing the pool of group members (Me) in to different subgroups and each subgroup has its subgroup controller(SGC) and these subgroup controller forms a group controller(GC) which is same as group manager(GM) and responsible for all operations i.e. registration, distribution of keys etc.

The group public key is generated by the Group controller and is propagated to all the members through subgroup controller (SGC). In proposed scheme Group controller does not need to maintain all the members of group. The GC has to only manage SGC's. The members of each subgroup send their respective factors to SGC of their respective group. The SGC after verification of factors send it to Group controller for final verification.

3.2 Proposed Model

The proposed model of the scheme is given in figure below:

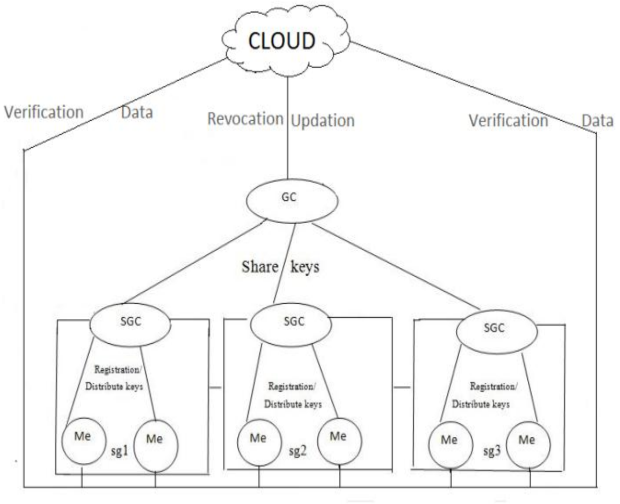

Fig. 1: Proposed Model for rebalancing the load

There are several steps that are used in the proposed model for rebalancing the load of the group manager.

Steps:

1. All the Members of Different subgroups make registration request to their respective Subgroup controller (SGC).

2. After verification of parameters given by members, the subgroup controllers forward it to Group controller.

3. After verification, the group controller shares the common keys of different subgroups to respective subgroup controllers.

4. Subgroup controller then distributes group keys to respective subgroups.

5. The members, after activation from group controller directly decrypt data from cloud using respective subgroup keys.

IV. Comparative Analysis

In this section, we compare the Response time of Members, Computation cost with existing scheme MONA [2].

4.1 Based on response time

It is defined as the response given by group manager after receiving the requests from users. In existing Scheme if there are ‘n’ users requesting for registration than Response time is O (n). In proposed Scheme if there are ‘n’ users requesting for registration than Response time is O (n/s + St)

Where s = no. of Sgc’s and st= total setup time of Sgc’s

In Table 4.1 we compare the Response time with existing Scheme MONA [2].

Table I: A comparison of Response time

No. of users	Existing Scheme	Proposed Approach(Assuming 3 SGC’s and initial setup time for each SGC’s=1)
100	100	36.33
300	300	103
900	900	303
1000	1000	336.33
1200	1200	403
1900	1900	636.33

4.2 Based on Computation cost

As subgroups are independent of each other, so managing joining and leaving of members is belong to specific group and hence resulting in to lesser computation cost.

In Existing Schemes if there are ‘n’ users then computation cost is O(n).Where as in proposed approach the computation cost is depends on Members in specific group where joining and leaving take place i.e. here computation cost is O(m)where ‘m’ is total numbers of members in that subgroup.

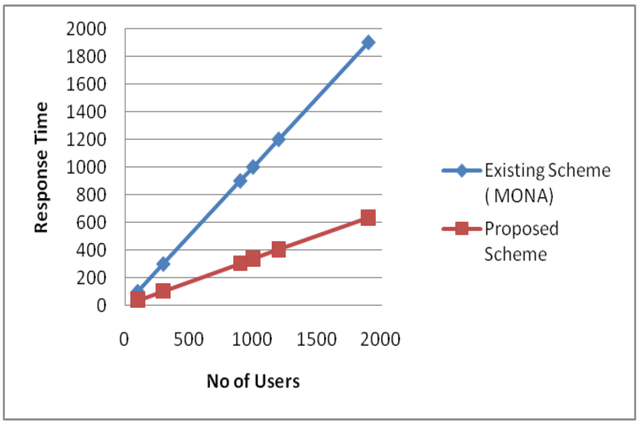

Fig. 2: Comparison Based on Response time

V. Conclusion

The proposed approach will provide the scheme using which the members in a group can share and store data efficiently and securely. For bulk number of request proposed scheme use the methodology by dividing group members (Me) in to different subgroups and each subgroup has its subgroup controller (SGC) and these subgroup controller now responsible for member registration and member account activation and key distribution. The group controller (manager) has to manage the subgroup controller (SGC's). In this way the proposed scheme is an efficient and secure load balancing multi-owner data sharing scheme for dynamic group in the cloud.

References

1. 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.
2. Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "MONA: Secure Multi-owner Data Sharing For Dynamic Groups in Cloud", IEEE Transactions On Parallel And Distributed Systems, Vol. 24, No. 6, June 2013,pp. 1182-1191
3. M. Kallahalla, R. Swaminathan E. Riedel, Q. Wang, and K. Fu, "Plutus Scalable Secure File Sharing on Untrusted Storage," Proc. Conf. File and Storage Technologies, pp. 29-42, 2003.
4. P. Kiranmai, Y. Ramu "Secured Multi-Owner Data Sharing for the Dynamic groups in the Cloud", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 12, December 2014, PP- 493-496.
5. 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.
6. 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.
7. 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.
8. S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc. Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136- 149, Jan. 2010.
9. Ziyuan Wang, "Security and privacy issues within the Cloud Computing" International Conference on Computational and Information Sciences, pp.175-178, 2011.
10. K.U.V. Padma, J.Anitha, K. Balaji, "A novel Multi-owner Data Sharing Group key protocol", International Journal of Research in Computer and Communication Technology, Vol 2, Issue 10, October-2013.