ISSN No. 0976-5697

Volume 4, No. 10, September-October 2013

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Security and Privacy Enhancing For Dynamic Groups in the Cloud Using Batch Auditing

M. Tamil Selvan*
PG Scholar
Department of Computer Science and Engineering
Anna University Regional Center Coimbatore
Coimbatore, Tamil Nadu, India
tamilselvan.madasamy@gmail.com

G. Nanthini
PG Scholar
Department of Computer Science and Engineering
Anna University Regional Center Coimbatore
Coimbatore, Tamil Nadu, India
nanthiniganesan@gmail.com

M. Newlin Rajkumar
Assistant Professor
Department of Computer Science and Engineering
Anna University Regional Center Coimbatore
Coimbatore, Tamil Nadu, India
newlin_rajkumar@yahoo.co.in

Abstract: Cloud computing is a type of computing through which data can be stored, managed and processed remotely rather than locally with essentially the internet. The key characteristics it possesses are numerous like centralized network access, cost, low maintenance, resource-sharing, scalability, etc., are the reasons why the entire world is relayed on cloud computing. In this paper, we propose a secure; privacy enhances multi-owner data sharing for dynamic groups in the cloud. In addition, we propose an auditing service to perform audits for multiple users simultaneously and efficiently, a process called Batch Auditing. As the emerging trend of forming dynamic groups for multi-owner data sharing, finding the odd person in the group is the biggest task. Our implementation performs well relative to the underlying security, privacy enhancing issues for dynamic groups using batch auditing.

Keywords: Cloud Computing, Access Control, Batch Auditability, Privacy Preserving, Data Sharing, Dynamic Groups.

I. INTRODUCTION

CLOUD computing is an adaptive technology with an idea of parallel and distributed systems which offers resource-sharing at lower cost. Low Maintenance is the key feature. For the purpose of securing the data and to enhance the privacy of each individual participant most of the Information Technology organizations, especially, started shifting their applications to the centralized cloud computing environment. To ensure the security and dependability for cloud data storage we aim to design an efficient mechanism for data sharing among dynamic groups with the following design goals as:

A. Storage :

To ensure the data owners that, the data are indeed stored appropriately and placed inside the cloud for easy access at any time.

B. Identifying errors:

We can able to locate the malfunctioning server or the data owner when the data corruption is detected.

C. Dynamic data sharing:

To provide support to maintain the level of correctness in data storage ensuring data privacy and integrity even if group members modify, delete or append their files into the cloud.

D. Data Redundancy and dependability:

We possibly ensure the availability of data over multiple data owners even against the data loss due to modifications by any group members, also we may be provided with redundant data due to participation of different users at the same time, and i.e. same data may be accessed by multiple users of different groups.

E. Light weight:

To enable users for data storage with minimum overhead due to multi-owner participation in the cloud.

II. PROBLEM DEFINITION

On considering a cloud storage service with multi-owner data sharing among dynamic groups , we propose a auditing system to address the security issues during unwanted sharing of data with group members who does not need to know any knowledge about the data content, the new users of the group can directly read the files from the cloud even before their participation, revoked users are incapable of accessing to the content entered into the cloud during their absence inside the cloud and finally we also identify repetition of data among the multiple owners of the cloud[1][4].

III. PROPOSED SYSTEM MODEL

In cloud data storage model, user can upload or stores the data into cloud or use services from the cloud. User stores data into set of cloud server. The data placed in the

cloud is accessible to everyone, security is not guaranteed. To ensure data security at the data owners we could use the cryptographic techniques. These techniques cannot be adopted directly and the cloud service provider (CSP) may hide the data corruptions to maintain data reputations among the dynamic groups in the cloud. To avoid this issue we introduce the batch auditing technique [2] (i.e. an effective third party auditor) to perform multiple auditing tasks simultaneously. Here the data is split into different data blocks and signing the data blocks is necessary to maintain data security. We have used the randomized public key based authenticator to achieve privacy among the data blocks and between the group members i.e. data users of the cloud.

The access privileges to the data users of the dynamic group may increase server overhead due to redundancy of data content found on the cloud [2] [3]. These redundant data may be removed to protect the dynamic groups from fault failure and cloud server crashes. Users can perform manipulations on stored data using block level updating and deletions are allowed with token generation for each members of the dynamic group. Hence in a multi-owner sharing environment, the batch auditing protocol provides the same level storage correctness and privacy preserving guarantee as like that of a single user [6].

Secondly, the new users of the groups can directly read, modify the data content which is to be restricted to only data owners of the cloud [5]. We know that data is not present at users place and it's being stored at cloud servers, it may lead to security threats such as internal and external attacks by the users of the dynamic groups. Internal attacks are from the cloud service provider (CSP), those servers that are considered malicious and lead to complex data failures and hide data loss. The external attackers are those who have illegal access to CSP from outside without their permissions. These outside attackers may modify the data or deleting the data users and their privileges on data access which are hidden from the CSPs. Hence here we proposed trusted party auditing scheme because once the cloud server is compromised, the data over the cloud is polluted with fraudulent data and users cannot able to retrieve the original data from the clouds.

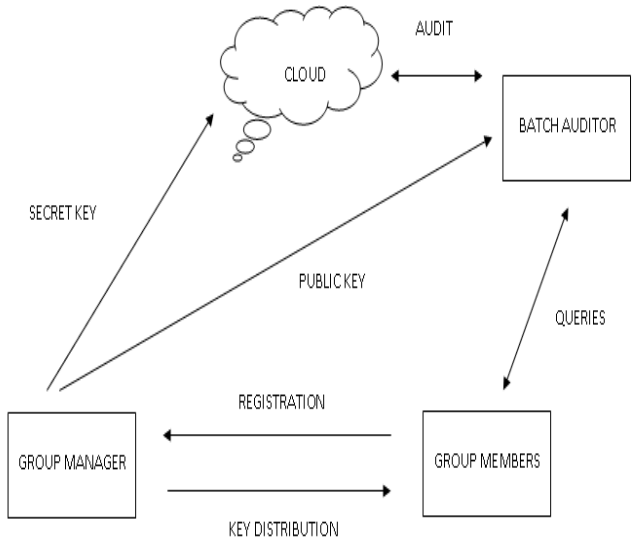

Figure 1. Architecture of the proposed System Model

IV. PRELIMINARY RESULTS

The proposed model increases the security of dynamic groups in the cloud and also provides privacy of data content among the new and revoked users using public key based authenticator. The experimental results are shown in Figure 2.

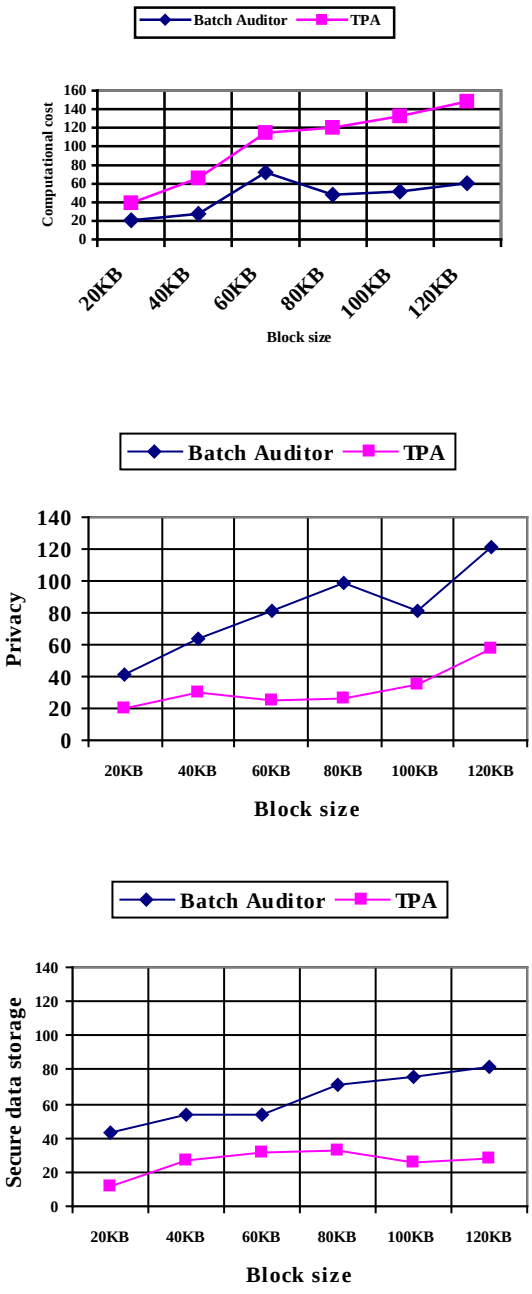

Figure 2. Results on the Computational Cost

V. CONCLUSION

In this paper, we have preserved the privacy of data among the dynamic group using public key authentication through batch auditing. In our system the data are split into blocks which ensure integrity of the data content during the modifications by the group users. We also provide authentication for the new and revoked users for decrypting the file before their participation in the cloud. Finally in our proposed model we have measured the computational

overhead of the data storage using multi-owner and e have improved the security of the dynamic groups in the cloud.

VI. 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," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 6, pp. 1182-1191 JUNE 2013.

[2]. Balakrishnan.S, Saranya.G, Shobana.S, and Karthikeyan.S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud," IJCST Vol. 2, ISSUE 2, June 2011.

[3]. Yan Zhu, Member, IEEE, Gail-Joon Ahn, Senior Member, IEEE, Hongxin Hu, Member, IEEE, Stephen S. Yau, Fellow, IEEE, Ho G. An, and Chang-Jun Hu, "Dynamic Audit Services for Outsourced Storages in Clouds," IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 6, NO. 2, pp. 227-238 APRIL-JUNE 2013.

[4]. D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[5]. Rakhi Bhardwaj, Vikas Maral, "Dynamic Data Storage Auditing Services in Cloud Computing," International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-4, April 2013.

[6]. 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.