ISSN: 0976-3104
SPECIAL ISSUE: Emerging Technologies in Networking and Security (ETNS)
Raghavan et al.

THE IIOAB JOURNAL

ARTICLE OPEN ACCESS

CLUSTER BASED PUBLIC AUDITING FOR SHARED DATA WITH EFFICIENT GROUP USER REVOCATION IN THE CLOUD

Parimala Raghavan*, Subasree, Sakthivel

Dept. of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Thrissur, Kerala, INDIA

ABSTRACT

Cloud computing is a very familiar term used for the recent development of internet. It is computed in which very large group of remote servers is networked and provide centralized data storage and online access to computer services. Considering Cloud computing, Data security becomes more and more important. When users put their large size of data in the cloud, the data integrity protection is challenging. Public auditing of cloud data storage security is very essential. In the existing system users who share data as a group. In that group, one original user and number of group users. The original user creates data and other user's shares and accesses that data. The TPA (Third Party Auditor) verifies the data and after verification process cloud stores that verified data. TPA will help the data owner to make sure that his data are safe in the cloud and less burdening to the data owner. In the case of a large number of users single TPA can do the verification process it is very much time consuming process. To overcome this problem we modify the existing system. In that users can be grouped and each group has its own third party auditor. In the modified system the verification time is less as compared to the existing system. From the analysis we have identified that modified system is best for cloud environments.

Published on: 28th– August-2016

KEY WORDS

computing; Public Auditing; Third Party Auditor; Verification time

***Corresponding author:** **Email:** neelima.raghavan@gmail.com

INTRODUCTION

Cloud computing, is a kind of Internet-based computing, where data, information and shared resources are provided with computers and other devices on-demand. It is the new technology that shares computer resources through internet instead of using the software. Cost saving is the main advantage of cloud computing and the prime disadvantage is data security. The data stored in the cloud are accessible to everyone so security is not guaranteed. To ensure data security effective third party auditor is introduced. Public verifier efficiently checks the correctness of data without downloading the entire data this is commonly referred to as a public auditing mechanism. In the existing system single TPA performs audits for multiple users simultaneously and efficiently [1],[11]. But sometimes users create a large number of data in that case single TPA can make the auditing process it is time consuming process. To overcome this problem we modified the system.

In the modified system users can be grouped and each group has its own TPA. Group users upload large number of data to the cloud. To ensure the integrity of data cloud saves these data only after the verification process. TPA collects these data and verifies without downloading the entire data. Each user group has its own specified TPA. . In the public auditing system single TPA can do the auditing process of all uploaded data, but in the cluster based public auditing system multiple number of TPA can auditing the uploaded data. From the analysis we have identified in the modified system the verification time is less as compared to the existing system.

RELATED WORKS

Cloud service providers provide mainly three services including Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a Service (IaaS). The cost for users to rent cloud service is cheaper than the cost for users to build cloud environment. Cloud storage service is the most common and popular service among many cloud services (e.g. Google Drive, Dropbox, Amazon S3 and Microsoft OneDrive) for general users.

To protect the integrity of data in the cloud, numbers of mechanisms have been proposed. All these mechanisms, each block of data

THE IIOAB JOURNAL
ISSN: 0976-3104

a signature is attached, and the integrity relies on the correctness of these signatures. Most of the previous work focus on auditing the integrity of personal data but some works [2],[3],[4],[9],[10] focus on how to preserve identity privacy when auditing the integrity of shared data. The public mechanism proposed by Wang *et al.* [7] is able to preserve confidential data from the TPA based on random masking. In that paper use the technique of providing more security by using the TPA. The TPA allows the user to know the information about the data stored in the cloud. When anyone tries to modify the data TPA informs the user by verifying the data. The TPA does not even allow CSP (cloud service provider) to read the data of the user. To operate multiple auditing tasks from different users efficiently this mechanism support batch auditing.

One recent work [2] proposed a mechanism for public auditing shared data in the cloud for a group of users. This is based on a ring signature scheme with homomorphism authenticators, the TPA can verify the integrity of shared data, but is not able to reveal the identity of the signer on each block. It supports an external auditor to audit user's outsourced data in the cloud. The main advantages of this mechanism are public auditability, storage correctness and privacy preserving but one main drawback is it is not supported user revocation when auditing the data [5],[8]. The auditing mechanism in [6] is designed to preserve identity privacy for a large number of users. However, it fails to support public auditing.

MATERIALS AND METHODS

The below figure shows the Cluster based public auditing system model. In this users can be grouped in the cloud network. Each group has its own Third Party Verifier.

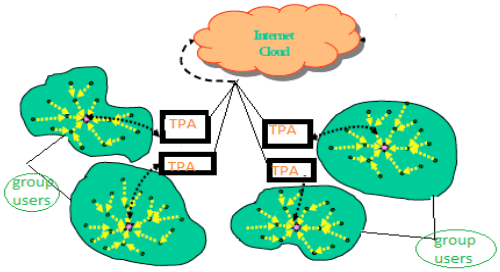


Fig: 1. Cluster based public auditing system model

System architecture consisting three entities: the cloud, TPA or public verifier and users who share data as a group.

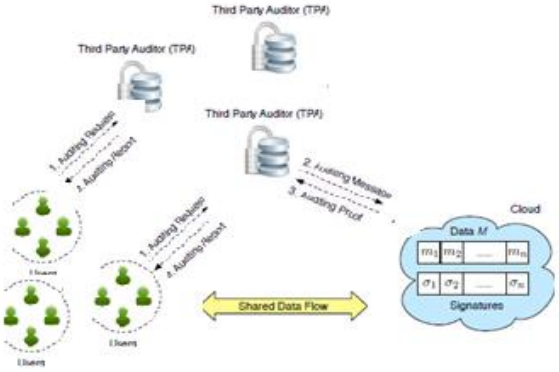


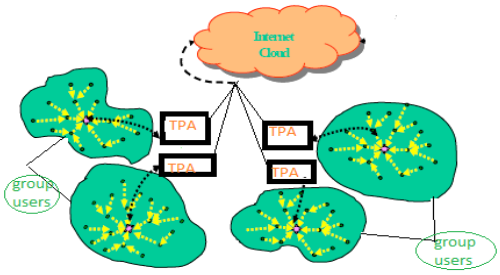
Fig: 2. System Architecture

The cloud provides data storage and sharing services. The public verifier or third party auditor utilizes cloud data for particular purposes such as searching, computation and data mining, etc. TPA provides verification services via challenge-and-response protocol. In a group, there is one original user who creates the data and share data with other users in the group through the cloud. In the modified system number of groups creates and each group consisting number of group members. Each group has its own TPA. Once a user is revoked in the group, the signatures computed by the revoked user become invalid. In this case the cloud is able to re-sign the blocks, which were already signed by the revoked user.

The important design objectives are correctness, efficient user revocation, public auditing, scalability and network security. The public verifier checks the correctness of data. The cloud data can be efficiently shared among group users. In the existing system

THE IIOAB JOURNAL
ISSN: 0976-3104

single TPA is able to handle large number of auditing tasks simultaneously this is time consuming. Considering this paper one of the important design goals is to decrease the auditing time using multiple number of TPA to increase the efficiency of the system



each block of data this mechanism commonly referred to as a public ntly checks the correctness of data without downloading the entire data. copy the data. In the verification process simply downloading the data rty auditor. TPA can do it and provide an audit report. In the auditing ase user uses keys and computes MAC (message authentication code) PA. In auditing phase TPA gives a key to cloud service provider and nand the random number of blocks and code from the cloud service see the data so data in cloud keep being confidential.

In cluster based public auditing system the internal architecture is same as a public auditing mechanism. In public auditing scheme introducing third party verifier. Single TPA can do the auditing process and they provide audit report. In cluster based public auditing mechanism using multiple TPA'S for the auditing process. In this case multiple audit report provides simultaneously so the efficiency of the system will increase. In cluster based public auditing system has two phases setup phase and audit phase. In the setup phase KeyGen, SigGen algorithm using and the audit phase using GenProof and VerifyProof. TPA sends Challenge-response protocol to the CSP. Challenge-response protocol helps the verifier for verification process of blocks of data. Multiple TPA sends multiple numbers of challenge-response protocols so the verification process became fast as compared to using single TPA.

RESULTS

In this paper, we are focusing public auditing in the cloud using multiple TPA's with efficient user revocation. Public auditing mechanism single TPA performs audits for multiple users simultaneously, but it is a time consuming process. To overcome this problem user in the network can be grouped and each group has its own individual TPA. In this scheme we have been using a different range of users and we analyze the auditing time of these range users using single TPA and multiple TPA'S.

Table: 1. Verification time Comparison between Public auditing mechanism Vs Cluster based public auditing mechanism using less than 100 users.

Number of existing users	Auditing Time in ms(Cluster Based Public Auditing Mechanism)	Auditing Time in ms(Public Auditing Mechanism)
20	190	280
40	220	440
60	300	720
80	350	800
100	400	980

Table: 2. Verification time Comparison between Public auditing mechanism Vs Cluster based public auditing mechanism using 100 to 1000 users.

Number of existing users	Auditing Time in seconds(Cluster Based Public Auditing Mechanism)	Auditing Time in seconds(Public Auditing Mechanism)
200	3	22
400	6	35
600	8	42
800	11	48
1000	13	58

Table: 3. Verification time Comparison between Public auditing mechanism Vs Cluster based public auditing mechanism using 1000 to 5000 users.

THE IIOAB JOURNAL
ISSN: 0976-3104

Number of existing users	Auditing Time in minutes(Cluster Based Public Auditing Mechanism)	Auditing Time in minutes(Public Auditing Mechanism)
2000	1	15
3000	2	24
4000	6	37
5000	9	45

The above table shows auditing time for different range of users using public auditing and cluster based public auditing mechanism. Public auditing mechanism using single TPA and the cluster based public auditing mechanism using multiple TPA'S. The auditing time can be taken in milliseconds, seconds and minutes depend upon the uploaded data. The above three tables showing three categories of users. The first table shows less than 100 users. In that auditing time can be taken in milliseconds. The second table shows range of users is in between 100 and 1000 and the auditing time taken in seconds. The last table the existing users are less than 5000 in that case auditing time taken in minutes. The auditing time for uploaded data files using different range of users is different for using single TPA and multiple TPA. The following figure shows the graphical representation of the table values.

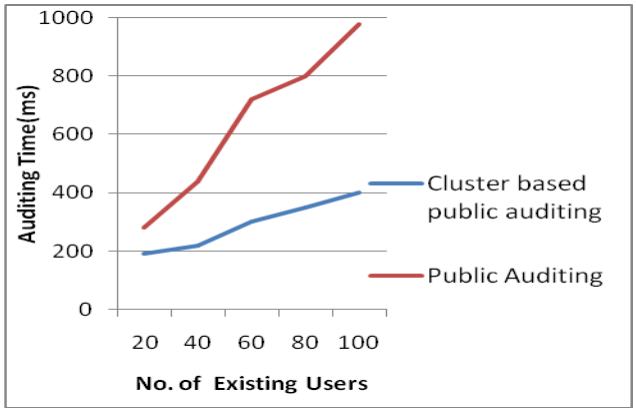


Fig: 3. Verification time between Public auditing mechanism Vs Cluster based public auditing mechanism(<100 users)

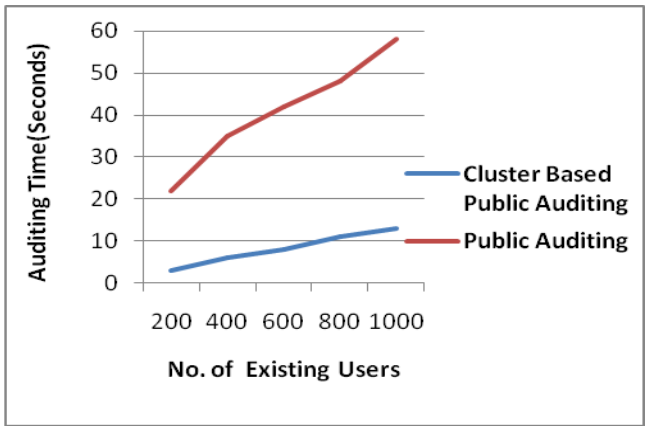


Fig: 4. Verification time between Public auditing mechanism Vs Cluster based public auditing mechanism (upto 1000 users)

THE IIOAB JOURNAL
ISSN: 0976-3104

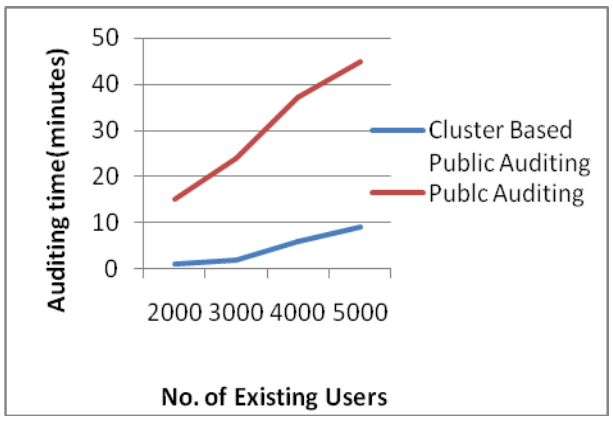


Fig: 5. Verification time between Public auditing mechanism Vs Cluster based public auditing mechanism (upto 5000 users)

DISCUSSION

In this paper, we have compared existing and modified system in terms of verification time. We have implemented public auditing in the cloud network using different ranges of users. In the existing system, all users can upload data and single TPA can do the verification process. In modified system users can be grouped and each group has its own third party verifier. We identified the modified system the verification time is less as compared to the existing system. From the analysis we have identified that modified system is best for cloud environments.

CONCLUSION

In cloud computing, data security is the biggest challenge. A number of research work carried out in this area. To ensure data security effective third party auditor is introduced. In this mechanism provides a number of advantages in cloud computing. The main advantage is TPA can save encrypted data file on cloud and perform the integrity verification without downloading the entire file. Once the user is revoked in the group, the cloud themselves re-sigh the blocks so the efficiency of the user revocation is significantly improved in this scheme. TPA can perform multiple auditing tasks simultaneously this provides better efficiency. In the cluster based public auditing system each group consist number of group members, and they are uploaded large number of data. Sometimes some TPAs are very busy and the other one is idle depends on uploaded data. In this case we have plan to implement load balancing of TPA'S for the verification process. This is much more effective than the modified system. In this paper, we have compared existing and modified system in terms of verification time. Based on the comparison results we identified the modified system verification time is less as compared to the existing system. From the analysis we have identified that modified system is best for cloud environments.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

The authors report no financial interests or potential conflicts of interest.

REFERENCES

[1] Boyang Wang, Baochun Li, and Hui Li.[2015] "Public Auditing for Shared Data with Efficient User Revocation in the Cloud," IEEE Trans. *On Services Computing*, 8(1): 92-106.

[2] B Wang, B Li, and H Li.[2014] Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud, *IEEE Tns On Cloud Computing*,2(1): 43-56.

[3] C Wang, Q Wang, K.Ren,W Lou.[2013] Privacy Preserving Public Auditing for Secure Cloud Storage, *IEEE Transactions on Computers*, 62.

[4] B Wang, H Li, M Li.[2013] Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics, *Proc IEEE Int'l Conf Comm. (ICC'13)*, 539-543.

THE IIOAB JOURNAL ISSN: 0976-3104

[5] B Wang, SS Chow, M Li, H Li.[2013] Storing Shared Data on the Cloud via Security-Mediator, *Proc. IEEE 33rd Int'l Conf. Distributed Computing Systems* (ICDCS'13), pp. 124-133,.

[6] B Wang, B Li, and H Li.[2012] 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*,June.

[7] C Wang, Q Wang, K Ren, and W Lou.[2010] Privacy-preserving public auditing for data storage security in cloud computing, in InfoCom 2010, *IEEE*.

[8] Q. Wang, C Wang, J Li, K Ren, and W Lou.[2009] Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,Proc. 14th European Conf. Research in Compute Security(ESORICS'09

[9] G Ateniese, RD Pietro, LV Mancini, G Tsudik.[2008] Scalable and Efficient Provable Data Possession, Proc. Fourth Int'l Conf. Security and Privacy in Comm. Networks (ICST SecureComm'08)

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

[11] Parimala Raghavan, Dr. S Subasree.[2016] performance analysis of public auditing for shared data with efficient user revocation in cloud using RSA and AES algorithms, *International Journal of Future Innovative Science and Engineering Research (IJFISER)* ISSN (Online): 2454- 1966, 2(1) : 257.