International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Dynamic Auditing Protocol For Data Storage in Cloud Computing

Mr. Thakur P. S.[1], Mr. Thorat A. V.[2], Gore V. A.[3], Shinde R. C.[4]
[1] *Mr. Thakur P. S.,Department of Information Technology, SNDCOE&RC, Yeola, pranitbhai@rediffmail.com*
[2]*Mr.Thorat A. V.,Student, Department of Information Technology, SNDCOE&RC, Yeola, avthorat3536@gmail.com*
[3]*Mr. Gore V. A.,Student,Department of Information Technology, SNDCOE&RC, Yeola,vikasgore92@gmail.com*
[4]*Mr. Shinde R. C.,Student,Department of Information Technology, SNDCOE&RC, Yeola, rowdyshinde007@gmail.com*

Abstract - In a cloud computing a user of cloud host their data on cloud servers and the users who stored the data on a cloud server can access data from cloud server from anywhere with the help of the network. As data is stored on the cloud servers it increases the new challenges regarding the security, this needs an auditing service to verify the data integrity in cloud, the dynamic auditing protocol is desired to understand data owner that the data is securely and correctly stored in the cloud. In this paper, we design an auditing framework for cloud systems and propose privacy-preserving auditing protocol. Then we enlarge our auditing protocol to help the dynamic operations of data. Then we enlarge our auditing protocol to help batch auditing for multiple clouds, without depending any trusted user.

Keywords- cloud server, dynamic auditing, third party auditing, integrity protocol, unbiased auditing.

I. INTRODUCTION

Cloud Storage is a service of the Cloud computing. Cloud computing allows data owner (owners of the data) to send the data from local computing system to the cloud. As more and more number of owners starts to store the data on cloud the more no of security challenges are increased. Owner gets more worried about the chances of lost of the data[1].The cloud service provider might be dishonest for the owner. They can remove the data of the owner for the purpose storage space and the can claim the owner that the data is still in the cloud. Therefore the owner need to verify that the data is securely stored.

Traditionally, owners can verify their data integrity with the help of the two-party storage protocols. in the cloud computing system it is essential that either cloud service provider or data owners conducts the auditing of the data. Because either data owner or the service provider can not guarantee to provide unbiased auditing results[2].In the case of guarantee of auditing results Third Party Auditing(TPA) is the natural choice for auditing the storage in the cloud computing.

For third party auditing there are some important requirements which are proposed from some previous work. The third party auditing protocol should have the following properties:

1.1 Confidentiality:-

The owners data should keep confidential against the auditor.

1.2 Batch Auditing:-

The auditing protocol helps the batch auditing for multiple owners and also the multiple clouds.

1.3 Dynamic Auditing

The dynamic updates are supported in the dynamic auditing protocol.

II. LITERATURE SURVEY

Recently some remote integrity checking protocols were introduced to allow the auditor to check the integrity of the data on remote server. The remote integrity checking protocols may includes PDP which is the privacy preserving but its not a dynamic[3].And IPDP is a integrity protocol with both of privacy preserving and dynamic auditing but the problem of the both PDP and IPDP is that they do ant supports the multiowner and multi cloud. Audit is also a integrity checking protocol which supports both privacy and dynamic and it also supports the multi owner but it didn't support the multicloud[4].And our scheme is proposed as it supports all of these such as privacy and dynamic and it could supports to multiowner and also multicloud.

III. SYSTEM MODEL

In the section of system model, we describes the system model and then we defines the storage auditing protocol. After that we define the threat model and security model for the Storage auditing protocol.

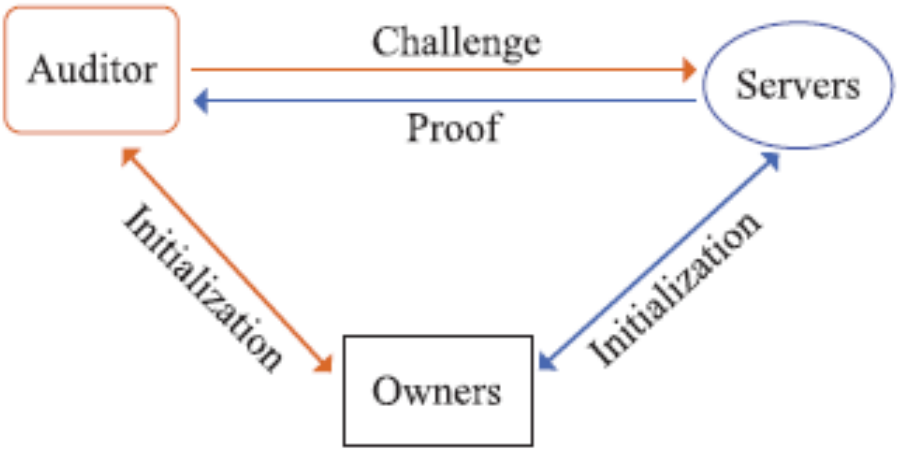

Fig 1. System Model For Auditing Of The data Storage

Consider an auditing system as Shown in the fig.1.The fig involves cloud server,the data owner and third party auditor,the owner creates the data and then the owner hosts the data on the cloud.the cloud server is providing the service of data storing the data of the data owner and provide the access to the user.The auditor is the trusted third party that has the capabilities of providing the data storage auditing service for both the cloud server and the user[5]. The auditor can also be organization that can be managed by the government,this organization provide the unbiased result of auditing for both data owner and the cloud server[6].

3.1 Definition of the Security Model:-

We could assume that the auditor is honest but the auditor cold be curious about the data which is received but sever cold dishonest and may quire the following attacks:

3.1.1Replay Attack:- The server may create the proof with the help of the previous proof and from other information without accessing the owner's original data.

3.1.2 Replace attack:- the server may use another valid and uncorrupted data block to replace the challenged data blog.

3.2.3 Forge Attack:-the server forge the data tag of data block to deceive the auditor if the owner reuses the data key for the different versions of data.

IV. RESULT

The figure 2 shows that the user checks the file stored at the cloud storage is audited by the third party auditor and as per the user expectation it shows the result, if the data is attacked by the cloud service provider then it informs to the data owner.

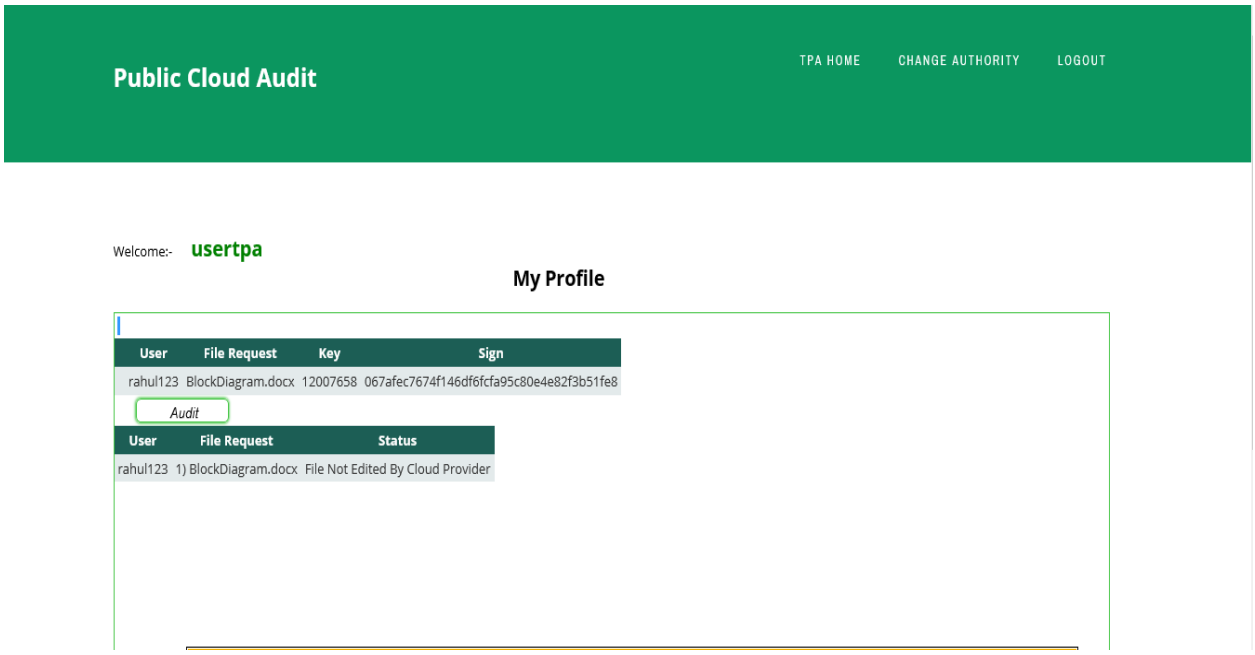

Fig 2. Auditing by TPA

CONCLUSION

In this paper,we have proposed to a secure dynamic auditing protocol.This protects the privacy of the user's data against auditor with the help of property of bilinearityand the cryptography method. So our auditing protocol supports multiowner batch auditing and can also support the multicloud batch auditing.Our scheme occurs less computation cost and also the less communication cost which improves the auditing performance and this can be applied to large number cloud storage system.

REFERENCES

[1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing,"technical report Nat'l Inst. of Standards and Technology,2009.
[2] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010.
[3] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011
[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"Proc. IEEE INFOCOM, pp. 525-533, 2010.
[5] Y. Zhu, H. Hu, G. Ahn, and M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multi-Cloud Storage," IEEE Trans. Parallel and Distributed Systems, vol. 23, no. 12, pp. 2231-2244, Dec. 2012.
[6] K. Yang and X. Jia, "Data Storage Auditing Service in Cloud Computing: Challenges, Methods and Opportunities," World Wide Web, vol. 15, no. 4, pp. 409-428, 2012

