Third Party Auditing (TPA) for Data Storage and Maintaining Integrity of Data in Cloud

Madhuri R. Rokade[1] Siddaling B.Natikar[2]
[1,2]Department of Computer Engineering
[1,2]Vishwabharati Academy's College of Engineering, Ahmednagar-414201

Abstract— Cloud storage enables users to remotely store their data. Many users place their data in the cloud and so data integrity is very important issue in cloud storage. After moving the data to the cloud, owner hopes that their data and applications are in secured manner. But that hope may fail sometimes that is the owner's data may be altered or deleted. Numerous present remote integrity inspection methods can only serve for static collection data and not to the audit service as the data in the cloud can be dynamically updated. Thus, an efficient and secure dynamic auditing protocol is desired to convince data owners that the data are correctly stored in the cloud. Thus, design an auditing framework for cloud storage systems can be built and put forwards an efficient and privacy-preserving auditing protocol. Then, here extend auditing protocol to support the data dynamic operations, which is efficient and provably secure. Again, further extending to provide the data integrity to the data present in cloud by using algorithms. Again to preserve integrity of file stored in cloud and provide better privacy for user slicing technique is added.

Key words: TPA, Wind Turbine, Blade hub

I. INTRODUCTION

Cloud storage becomes an increasing attraction in cloud computing paradigm, which enables users to store their data and access them wherever and whenever they need using any device in a pay-as-you-go manner[1]. Moving data into cloud offers great conveniences to the users since they do not have to care about the large capital investment in both the maintenance and management of the hardware infrastructures. The confidentiality and integrity of the outsourced data in clouds are of paramount importance for their functionality. The reasons are listed as follows [5]:1) the CSP, whose purpose is mainly to make a profit and maintains a reputation, has intentionally hide data loss an incident which is rarely accessed by the user's 2) The malicious CSP might delete some of data or is able to easily obtain all the information and sell it to the biggest rival of Company. 3) An attacker who intercepts and captures the communications is able to know the user's sensitive information as well as some important business secrets. Encrypting the data before storing in cloud can handle the confidentiality issue. However, verifying integrity of data is a difficult task. Third Party Auditor is kind of inspector. To achieve data storage security, AES and DES algorithm is used. This algorithm is efficient and safer than the former algorithms. Here TPA is allowed to perform multiple auditing tasks for different users at the same. Protocols were proposed to allow the auditor to check

II. LITERATURE SURVEY

In order to achieve the correctness of cloud data integrity and availability and enforce the quality of cloud storage facility, effective methods that enable on-demand data correctness verification on behalf of cloud users have to be designed. Though, the fact that users no longer have physical possession of data in the cloud prohibits the direct adoption of traditional cryptographic primitives for the purpose of data integrity protection. Henceforth, the verification of cloud storage correctness must be conducted without explicit knowledge of the whole data .Meanwhile; cloud storage is not just a third party data warehouse. The data in the cloud could not only be accessed but also be frequently updated by the users, including insertion, modification, deletion, appending, etc. So, it is also overbearing to support the integration of this dynamic feature into the cloud storage correctness guarantee, which makes the scheme design even more challenging. Next, the deployment of cloud computing is powered by data centers running in a simultaneous, co-operated, and distributed way. It is more useful for individual users to store their data redundantly across multiple physical servers so as to reduce the data integrity and availability threats. Thus, distributed protocols for storage exactness assurance will be of most importance in achieving robust and secure cloud storage systems. However, such important area remains to be fully explored in the works. Recently, the importance of ensuring the remote data integrity has been highlighted by the following research works under different system and security models. These methods, while can be useful to ensure the storage correctness without having users possessing local data, are entirely pointing on only one server situation. They may be useful for quality-of-service testing, but does not guarantee the data availability in case of server failures. While direct applying these techniques to distributed storage multiple servers could be direct, the resulted storage verification in the clouds would be linear to the number of servers. By way of an corresponding approach, researchers have also proposed distributed protocols for ensuring storage correctness across multiple servers or peers.

III. IMPLEMENTATION DETAILS

In this paper, we consider data storage and sharing services in the cloud with three entities: the cloud, the third-party auditor (TPA), and users who participate as a group (as shown in Fig. 1). Users in a group include one original user and a number of group users. The original user is the original owner of data, and shares data in the cloud with other users. Based on access control policies [5], other users in the group are able to access, download and modify shared data. The cloud provides data storage and sharing services for users, and has ample storage space. The third party auditor is able to verify the integrity of shared data based on requests from users, without downloading the entire data. When a user (either the original user or a group user) wishes to check the integrity of shared data, she first sends an auditing request to the TPA. After receiving the auditing

request, the TPA generates an auditing message to the cloud, and retrieves an auditing proof of shared data from the cloud. Then the TPA verifies the correctness of the auditing proof. Finally, the TPA sends an auditing report to the user based on the result of the verification.

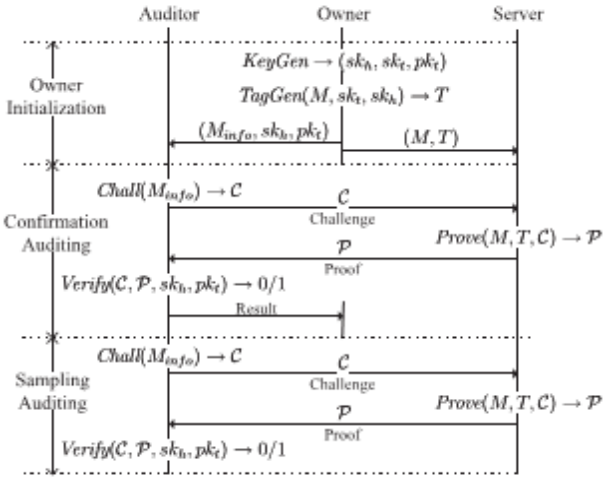

Fig. 1: Framework of our privacy-preserving auditing protocol.

The main challenge in the design of data storage auditing protocol is the data privacy problem (i.e., the auditing protocol should protect the data privacy against the auditor.). This is because: 1) for public data, the auditor may obtain the data information by recovering the data blocks from the data proof. 2) For encrypted data, the auditor may obtain content keys somehow through any special channels and could be able to decrypt the data. To solve the data privacy problem, our method is to generate an encrypted proof with the challenge stamp by using the bilinearity property of the bilinear pairing, such that the auditor cannot decrypt it, but the auditor can verify the correctness of the proof without decrypting it.

A. Algorithm for Auditing Protocol:

A storage auditing protocol contains of the following five algorithms:

1) KeyGen(λ) =(sKh,sKt, pKt)This key generation algorithm takes no input other than the implicit security parameter. It outputs a secret hash key sKh and a pair of secret-public tag key (sKt, pKt).
2) TagGen (M,skt,skh)=T. The tag generation algorithm takes as inputs an encrypted file M, the secret tag key skt, and the secret hash key skh. For each data block mi, it computes a data tag ti based on skh and skt. It outputs a set of data tags T={ti}iε[1,n]
3) Chall(Minfo)=C. The challenge algorithm take s as input the abstract information of the data Minfo (e.g., file identity, total number of blocks,etc.). It outputs a challenge C.
4) Prove (M,T,C)=P. The prove algorithm takes as inputs the file M, the tags T, and the challenge from the auditor C. It outputs a proof P.
5) Verify(C,P,skh,pkt, Minfo)=0/1. The verification algorithm takes as inputs P from the server, the secret hash key skh, the public tag key pkt, and the abstract information of the data Minfo. It outputs the auditing result as 0 or 1.

B. Activity Diagram:

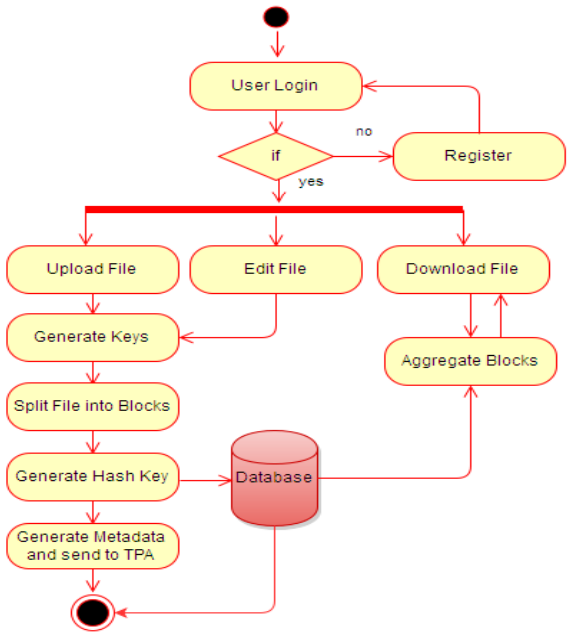

Fig. 2: Activity Diagram

IV. RESULTS

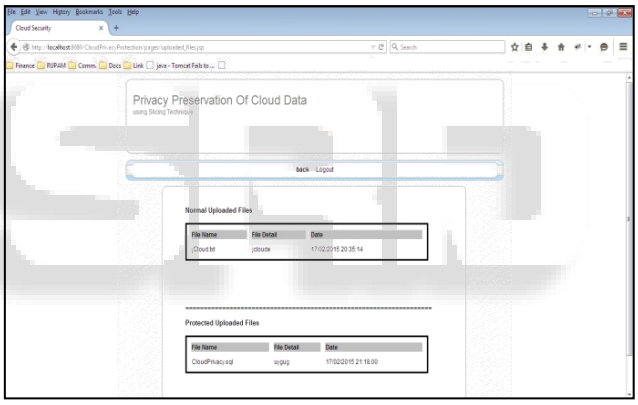

Fig. 3: User Uploaded Files

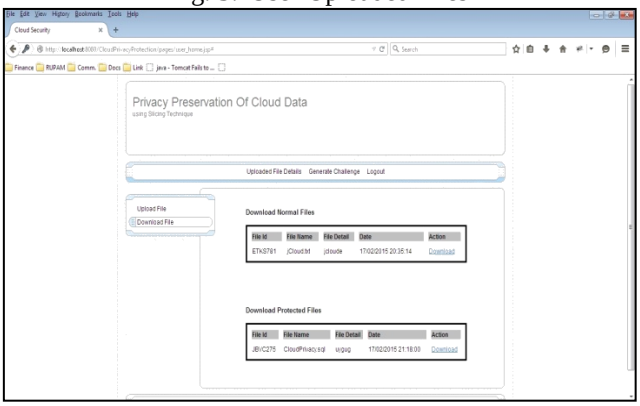

Fig. 4: User Downloaded Files

V. PERFORMANCE ANALYSIS OF AUDITING PROTOCOLS

As shown in the graph below, we can see the difference between existing system and our proposed system. Here comparison is done on the basis of file size and time to upload file on cloud server. In this paper we presented the novel technique which is used to store information on cloud and also slicing technique gives one more mile stone step to

securely store data if data is protected one. Here we can analysis the auditing protocol on the basis of performance. Here performance is measured on the basis of file size. This graph shows our proposed system gives better results than existing system.

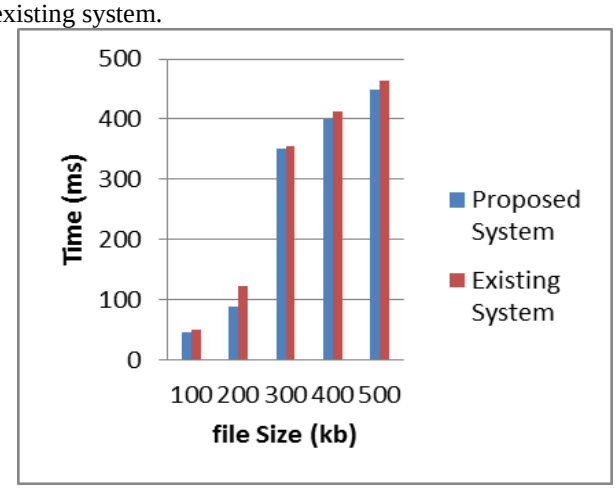

Fig. 5: Graph showing file sized with respect to time

Storage Cost			Communication Cost		Computation Cost	
Verifier	Server	Verifier	Server	User	Verifier	Server
O(1)	O(n)	O(1)	O(1)	O(1)	O(1)	O(1)

Table 1: Costs

Above table gives information regarding the computation cost, communication cost and storage cost. This represents the efficiency of this technique as compared to existing techniques.

VI. Conclusion

We have seen how delegation of responsibility trusted 3rd party which provides security services secures user data. It reliefs the client from maintaining any kind of key information and allowing the client for using any browser enabled device to access the cloud services. It allows the client to verify the integrity of the data stored on download or retrieval of its own stored data in cloud. The client can share the data securely with specific band of people without any overhead of key distribution.

References

[1] Kan Yang, Student Member , IEEE , and Xiaohua Jia, Fellow, IEEE, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE TRANSAC TIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 9, SEPTEMBER 2013.

[2] Tiancheng Li, Ninghui Li, Jian Zhang, Ian Molloy Purdue University, West Lafayette, IN 47907, "Slicing: A New Approach to Privacy Preserving Data Publishing," IEEE 2012 Transactions on Knowledge and Data Engineering, volume: 24, Issue:3.

[3] T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010

[4] J. Li, M.N. Krohn, D. Mazie`res, and D. Shasha, "Secure Untrusted Data Repository (SUNDR)," Proc. Sixth Conf. Symp. Operating Systems Design Implementation, pp. 121-136, 2004

[5] G.R. Goodson, J.J. Wylie, G.R. Ganger, and M.K. Reiter, "Efficient Byzantine-Tolerant Erasure-Coded Storage," Pro c. Int 'l Conf. Dependable Systems and Networks, pp. 135-144, 2004.

[6] V. Kher and Y. Kim, "Securing Distributed Storage: Challenges, Techniques, and Systems," Proc. ACM Workshop Storage Security and Survivability (StorageSS), V. Atluri, P. Samarati, W. Yurcik, L. Brumbaugh, and Y. Zhou, eds., pp. 9-25, 2005.

[7] L. N. Bairavasundaram, G.R. Goodson, S. Pasupathy, and J. Schindler, "An Analysis of Latent Sector Errors in Disk Drives," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of Computer Systems, L. Golubchik, M.H. Ammar, and M. Harchol-Balter, eds., pp. 289-300, 2007.

[8] B. Schroeder and G.A. Gibson, "Disk Failures in the Real World: What Does an MTTF of 1,000,000 Hours Mean to You?" Proc. USENIX Conf. File and Storage Technologies, pp. 1-16, 2007.

[9] M. Lillibridge, S. Elnikety, A. Birrell, M. Burrows, and M. Isard, "A Cooperative Internet Backup Scheme," Proc. USENIX Ann. Technical Conf., pp. 29-41, 2003.

[10] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J.

