Survey on Implementing Secure & Efficient Auditing Protocol for Cloud Storage

[1]Manisha Narad, [2]Prof. Amurta Amune

[1,2]G. H. Raisoni College of Engineering and Management, Ahmednagar, Maharashtra, India.

[1]*Manishanarad14@gmail.com*, [2]*amurta.amune@raisoni.net*

Abstract: In cloud storage environment, data owners host their data on cloud servers and users can access the data from cloud servers. Due to the data outsourcing, this process of data hosting service introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. Because, owner need to be convinced that the data are correctly stored in the cloud. Two-Party storage auditing system could not be guaranteed to provide proper auditing result thus Third-Party auditing is the better choice for the storage auditing in cloud computing. A Third-Party auditor is capable to do a more efficient work and convinces both the cloud service providers and the owner. There are chances of data being lost or get misplaced in cloud storage environment. For this we propose replication mechanism to third party auditing such that it will enhance the data availability. We divide a data file into fragments and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Furthermore, the nodes storing the fragments are separated with certain distance to prohibit an attacker of guessing the locations of the fragments. Hence user will get the belief that his data is safely stored on the cloud and could retrieve data without any modification.

Keywords: Cloud, Fragmentation.

I. INTRODUCTION

Cloud storage refers to saving data to an off-site storage system which is maintained by the third party. The information is stored on computer's hard drive or other local storage device, and it is the saved to the remote database through Internet connection between your computer and the database. Cloud storage has several advantages over traditional data storage. For example, if we store the data on a cloud storage system, it is easy to get that data from any location that has Internet access. We need not to carry any physical storage device or use the same computer to save and retrieve your information. With the right storage system, we could even allow other people to access the data, turning a personal project into a collaborative effort. Cloud storage is convenient and offers more flexibility. Cloud storage provides benefits of greater accessibility and reliability, rapid deployment, strong protection for data backup and disaster recovery and also reduces the cost as no purchase is required to manage and maintain the expensive hardware.

Data Integrity is the basic requirement of the information technology. As Data Integrity is an essential in databases similarly integrity of Data Storages is an essential in the cloud, it is a major factor affecting the performance of the cloud. The data integrity provides the validity of the data, assuring the consistency or regularity of the data. It is the complete mechanism of writing of the data in a reliable manner to the persistent data storages which can be retrieved in the same format without any changes. As described above, in cloud, the complete storage of data provided by the end-user is done at the data centres or data storages, and the security and integrity of the data lies on the vendor storing

data in the data centres but not the cloud. hosts. Cloud Storage is gaining popularity for the outsourcing of day-to-day management of data. Therefore integrity monitoring of data in cloud storages is as essential for any data centre, to avoid any data corruption or data crash. Data corruption or data failure can occur at any storage level. Therefore just storing data at cloud data storages or data centres doesn't ensure the integrity of data, but some mechanisms need to be implemented at each storage level to ensure the data integrity. Data Integrity is most important of all the security issues in cloud data storages because it not only ensures completeness of data but also ensures that the data is correct, accessible, consistent and of high quality.

Secure cloud storage was firstly studied by Juels and Kaliski [4] and Ateniese et al[5]. In cloud computing, data owners host their data on cloud servers and users can access these data from cloud servers. That means data moves or outsource from its local computing system to the cloud. This data outsourcing, introduces new security challenges.

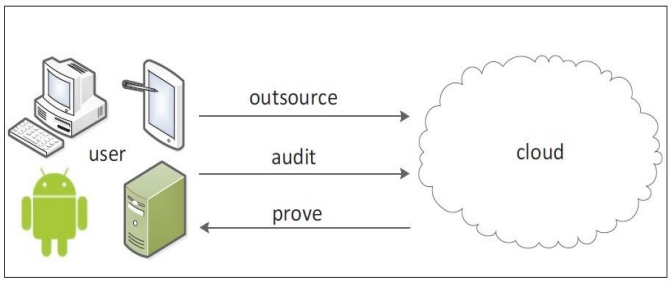

Figure 1.1 A Secure Cloud Storage System [1]

The above Figure 1.1 shows the Secure Cloud Storage System. This system consists of two entities Cloud and its user[1]. Cloud could be any Cloud Service Provider such as Amazon's S3, Dropbox, Google Drive, etc. and user could be any individual or company or an organization that uses PC or mobile phone. To extend this model, a third-party auditor could be introduced [4] to shift the auditing task from the user to the third-party auditor.

A secure cloud storage system that enables a user to check the integrity of its data is expected to have the following properties[1]:

1. Correct

If the cloud indeed stores the complete data of the user, then cloud can always prove to the user that the data remains intact.

2. Secure

If the user's data is changed, the user can detect it as an abnormal event with high probability in the audit query even if the cloud tries to cover the event.

3. Efficient

The computation, storage and communication cost of both the user and the cloud should be as low as possible.

In traditional approach, owners can check the data integrity based on two-party storage auditing protocols. In cloud storage system, it is inappropriate to let the cloud or user to conduct such auditing, because they could not be guaranteed to provide auditing result. In this situation, third-party auditing is a natural choice for the storage auditing in cloud computing[9]. A third party auditor has some capabilities to provide a more efficient work and convince both cloud service providers and owners. For the third-party auditing in cloud storage systems, there are several important requirements. The auditing protocol should have the following properties:

1) Confidentiality

The auditing protocol should keep owner's data confidential against the auditor.

2) Dynamic auditing

The auditing protocol should support the dynamic updates of the data in the cloud.

3) Batch auditing

The auditing protocol should also be able to support the batch auditing for multiple owners and multiple clouds.

There are some existing remote integrity checking methods which can only serve for static archive data and therefore they cannot be applied to the auditing service because the data in the cloud can be dynamically updated[12]. Thus, an efficient and secure auditing protocol is desired to convince data owners that the data are correctly stored in the cloud.

To verify whether the cloud lies to an audit query, the user needs to have some secret information on its side, which is computed according to a certain security level parametersing the probability of successful cheating. A secure cloud storage (SCS) protocol, a keyed protocol used for the user to generate data to be outsourced and subsequently query for auditing.

II. LITERATURE SURVEY

A. Analysis of literature

This section presents a summary of some existing review articles related to secure data sharing in the Cloud. Become increasingly important with the advancements and growing popularity of the Cloud as well as the growing need to share data between people[3].

B. Definition of a System Model

Below Fig 2.1 shows the data hosting process. This process involves communication among three entities Cloud server, Owners and Auditor. The data verification is done by creating challenges and proofs for data integrity.

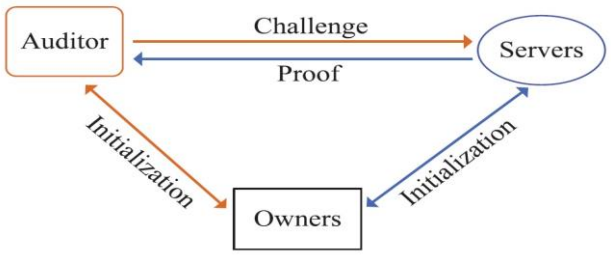

Fig 2.1 System model of the data storage auditing [2]

C. Definition of a Security Model

We assume that the auditor is honest but strange. It performs honestly during the whole auditing procedure, but it is curious about the received data. But the server could be dishonest and may launch the following attacks:

1. Replace attack

The server may choose another valid and uncorrupted data block to replace the challenged data block when it already discarded the message.

2. Forge attack

The server may forge the data tag of data block and deceive the auditor; if the owner's secret tag keys are reused for the different versions of data.

3. Replay attack.

The server may generate the proof from the previous proof or other information, without retrieving the actual owner's data.

D. Review of Existing System

In recent paper Chen, Xiang, et al [2], have designed a general construction of secure cloud storage protocol based on any secure network coding protocol. There have been a number of reviews on security and privacy in the Cloud. Xiao and Xiao [7]identifies the five concerns of Cloud computing; confidentiality, integrity, availability, accountability, and privacy. Chen and Zhao [8] outline the requirements for achieving privacy and security in the Cloud and the requirements for secure data sharing in the Cloud[3].

Oza et al. [9] gave a survey on a number of users to determine the user experience of Cloud computing and found that the main issue of all users was trust and how to choose between different Cloud Service Providers. There are many examples [6]of insider attacks such as Google Docs containing a flaw that inadvertently shared user documents, MediaMax going out of business in 2008 after losing 45 % of stored client data due to administrator error, Salesforce.com leaking a customer list and falling victim to phishing attacks on a number of occasions. It's clear from many of the reviews, that the Cloud is very susceptible to privacy and security attacks and currently there is on-going research that aims to prevent and/or reduce the likelihood of such attacks.

III. PROPOSED SYSTEM

This section presents the system model of storage auditing protocol which gives the solution for data integrity checking and security model for a storage auditing system.

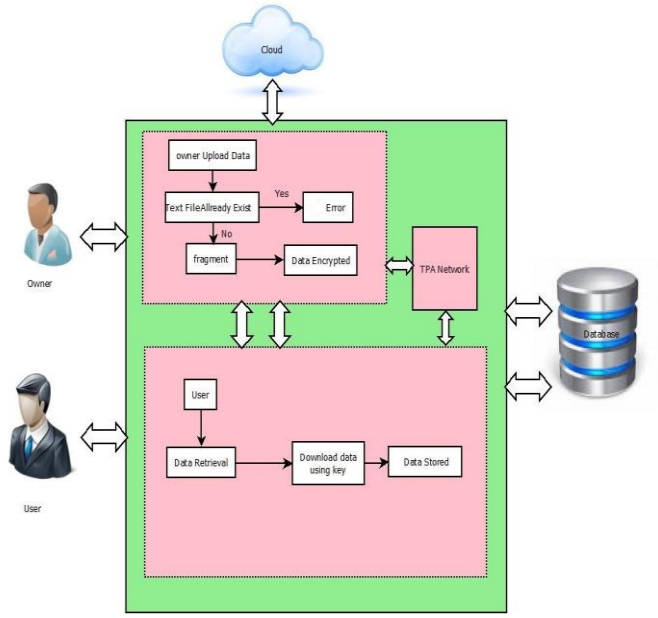

Fig 2.2 System model for efficient and secure auditing protocol in cloud storage.

As shown in following Fig 2.2, upon receiving the file, the cloud manager system performs:

(a) Fragmentation,

(b) First cycle of nodes selection and stores one fragment over each of the selected node,

(c) Second cycle of nodes selection for fragments replication.

The cloud manager keeps record of the fragment placement and is assumed to be a secure entity[10]. The fragmentation threshold of the data file is specified to be generated by the file owner. The file owner can specify the fragmentation threshold in terms of either percentage or the number and size of different fragments.

As we are not considering secure network coding protocol, data checking process will be done at the receiver end which will helps to reduce the load of network level coding. In cloud storage when owner wants to share and maintain his data files on cloud server securely and efficiently, the flow will be

1] At the sender end data to be shared, gets divided into number of chunks and then encrypted along with the owner name, last modification and owner signature if required.

2] On the auditing server machine, data get processed to check whether it is not being modified.

3] At the receiver end when receiver access required data from cloud, he decrypts the data by combining divided data chunks together to get the original data file.

In this scenario there are chances of data loss due to system crashes or any disaster. In such situation owner's data should be protected from this and should be kept safely on the cloud server. For this purpose we divide a data file into fragments, and replicate the fragmented data over the cloud nodes. Each of the nodes stores only a single fragment of a particular data file that ensures that even in case of a successful attack, no meaningful information is revealed to the attacker. Furthermore, the nodes storing the fragments, are separated with certain distance to prohibit an attacker of guessing the locations of the fragments. Hence user will get the belief that his data is safely stored on the cloud and could retrieve data without any modification. Although, the replication does not improve the retrieval time to the level of full-scale replication, it significantly improves the security[11].

So that owner would remain unaware about such data loss situations and get his original data. Thus it helps to achieve data integrity.

IV. CONCLUSION

In this paper, we proposed an efficient and secure storage auditing protocol. It protects the data privacy against the various security concerns. It also assures the data integrity as we are taking back up of this data into slave cloud server. As most of computation is processed on auditing server, the load on cloud server gets reduced. This paper presents the replication mechanism to the third party auditing that it will enhance the data availability.

The data file was fragmented and the fragments are dispersed over multiple nodes. The nodes were separated by certain distance. The fragmentation and ensured that no significant information was obtainable by an adversary in case of a successful attack. Hence, the owner would remain unaware about such data loss situations and get his original data. Thus

it helps to achieve data integrity, data availability as well its confidentiality.

It is strategic to develop an automatic update mechanism that can identify and update the required fragments only. The future work will save the time and resources utilized in downloading, updating, and uploading the file again.

REFERENCES

[1] Fei Chen,Tao Xiang,Yuanyuan Yang,Sherman S. M. Chow, "Secure Cloud Storage Meets with Secure Network Coding", IEEE INFOCOM 2014 - IEEE Conference on Computer Communications.

[2] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 9, pp. 1717–1726, 2013..

[3] Danan Thilakanathan, Shiping Chen, Surya Nepal and Rafael A. Calvo,"Secure Data Sharing in the Cloud", DOI: 10.1007/978-3-642-38586-5_2,©Springer-Verlag Berlin Heidelberg 2014.

[4] A. Juels and B. Kaliski Jr, "Pors: Proofs of retrievability for large files," in *ACM Conference on Computer and Communications Security (SP)*, 2007, pp. 584–597.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in *ACM Conference on Computer and Communications Security (CCS)*, 2007, pp. 598–609.

[6] Huang R, Gui X, Yu S, ZhuangW (2011) Research on privacy-preserving cloud storage framework supporting cipher text retrieval. International conference on network computing and information security 2011:93–97

[7] Xiao Z, Xiao Y (2012) Security and privacy in cloud computing. IEEE Commun Surveys Tutorials 99:1–17

[8] Chen D, Zhao H (2012) Data security and privacy protection issues in cloud computing. International conference on computer science and electronics, engineering, pp 647–651.

[9] Oza N, Karppinen K, Savola R (2010) User experience and security in the cloud-An empirical study in the finnish cloud consortium. IEEE second international conference on cloud computing technology and science (CloudCom) 2010:621–628.

[10] Sarathy R, Muralidhar K (2006) Secure and useful data sharing. Decis Support Syst 204–220.

[11] Butler D Data sharing threatens privacy, vol 449(7163).Nature Publishing, Group, pp 644–645.

[12] Feldman L, Patel D, Ortmann L, Robinson K, Popovic T (2012) Educating for the future: another important benefit of data sharing. Lancet 1877–1878.

