International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

Survey Paper on Security for Data Storage and Regeneration of Code by Adopting Auditing Scheme in Cloud

Chaitra s[1], Dr. Shantharam Nayak[2]

[1]*Mtech Scholar, Software Engineering, R.V College of Engineering, Bengaluru, Karnataka, India*

[2]*Professor –RV College of Engineering, Bengaluru, Karnataka, India*

Abstract- ***Using cloud storage users can store their data in the cloud. The clients can see their information anyplace whenever in the wake of putting away the information in the cloud. In the wake of putting away, the clients won't have any physical access to their put away information. Regardless of the way that disseminated stockpiling gives immense focal points to customers, there are security stresses moreover. The proposed plan is to make open review capacity with the goal that clients can securely assign the respectability checking undertakings to outsider inspectors. The other system utilized is recovering codes by which erased information can be recovered and put away back to the cloud. Accordingly this plan can make information proprietors free up them from their obligation of taking care of their information in the cloud. Gigantic zone of security shows that proposed arrangements are provably secure and successful.***

Keywords: Implementation, auditing, regenerating codes.

1. INTRODUCTION

Cloud storage offers data whenever required, and it is becoming popular because of its flexible use and low maintenance cost. Data can be accessed by users remotely from anywhere and anytime. Cloud service providers make users to apply only for the resources they use. There are many cloud service providers such as Google, Amazon etc. Despite the fact that these online administrations are giving much storage room to the clients to store information, they need in giving security to information [1]. On the off chance that the information is undermined, clients won't have the capacity to recuperate the information as information proprietors won't get any duplicate of information once put away in cloud. There are many hackers who may delete or corrupt user data from cloud. Multiple servers have been created for storage. If corruptions are detected in outsourced data, then corrupted data should be restored and the original data should also be restored. If data is deleted from one server the remaining servers will retain the data. The deleted data will be again regenerated in the proxy server. There is also a third auditing scheme (TPA) [2]. Protection for data is given through encryption against the auditor [3].

2. BACKGROUND RESEARCH

Security is given more productively so that no one other than information proprietor can see the substance of the document. For this purpose files are encrypted. One more technique which is used in this scheme for security purpose is random key generation. This goes about as great security worry since just this key can be utilized for downloading the document from the cloud which might be known by the client. The key will be generated immediately after user uploads file in the cloud. Proxy will be used for regenerating code if deleted/corrupted. The file can be regenerated after deleting by proxy. When data owner is not available online, proxy will take place of data owner and will regenerate code.

3. METHODOLOGY

Regenerating codes and public auditing scheme has been created to give privacy to data stored in the cloud. The owner must register his/her details before he/she can login to store the data. Once the client login's and transfer the document, the key will be produced. At the point when the client needs to roll out improvements to the information put away in the cloud, the client needs to enter the key created amid the record transfer. The client can send the issues to evaluator and the reviewer will send the mail to proprietor in regards to the erasure of the record in the cloud. In existing system, Cloud storage will allow users to store data and access data flexibly from anywhere and can modify data from anywhere anytime. Even though cloud provides so much storage benefits it lacks in providing security. Information proprietors will lose control over the information once they store in the cloud. They won't know anything about the code whether it is sheltered or it is being erased/tainted by programmers. The proposed plan is of making numerous servers so that the information won't just be put away in one serve.

4. ADVANTAGE

In proposed system, data will be stored in every server, which can be one security technique. When data is stored in multiple servers, even if the hacker delete's or corrupts user's data, the data will be safe at other servers.

5. ARCHITECTURE

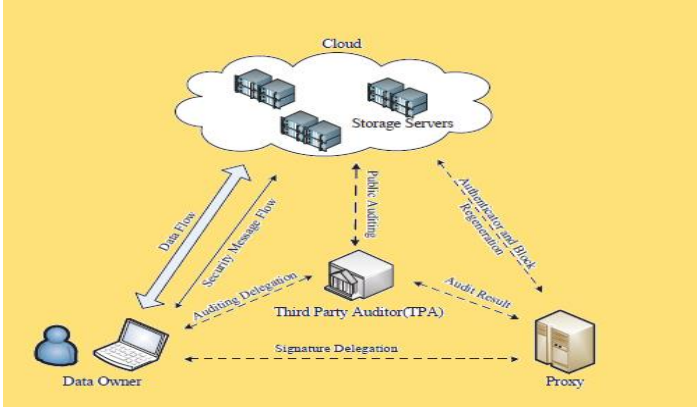

Figure1: System model

As shown in figure 1, data will be stored in the cloud by data owner. Auditor will have access to user's data. He will act as a trusted party. Auditor verifies data and then sends data to cloud. Since storage is important factor, cloud offers storage for data. Proxy plays the role as data owner. The data deleted/corrupted can be regenerated in proxy.

6. DESCRIPTION MODULES

6.1 Regenerating Codes

Regeneration can be done by proxy. Data owner need not have to be present online all the time. The intermediary will go about as information proprietor at whatever point information proprietor is not accessible and will recover the information the recovered information will be put away in the cloud once more.

6.2 Design goals

This tells about auditing scheme. Auditing scheme should be designed in the following ways.

Auditor: Auditor should be designed such that after file is uploaded by user, auditor verifies the file and sends to cloud.

Storage security: Security will be provided for the file in secure way so that data if lost from one server will be available in other servers also.

Privacy: Privacy is given with the end goal that reviewer or intermediary won't have the capacity to see the substance of the record.

Regeneration of data: The information proprietor require not be accessible online dependably. The proxy acts as data owner if owner is not available and data will be regenerated by proxy.

6.3 Application modules

Admin module:

Admin is allowed to check which user is registered and which data is stored in the cloud by the user.

TPA module:

TPA will check whether the data will be modified or not. If data is modified, the information will be sent to data owner.

User module:

User can register and he can login using his registered user id and password and upload files to cloud.

Block deletion module:

In the square erasure module client can erase the piece.

6.4 Auditing Scheme

Reviewing plan comprises of three techniques: Setup, Audit and

repair.

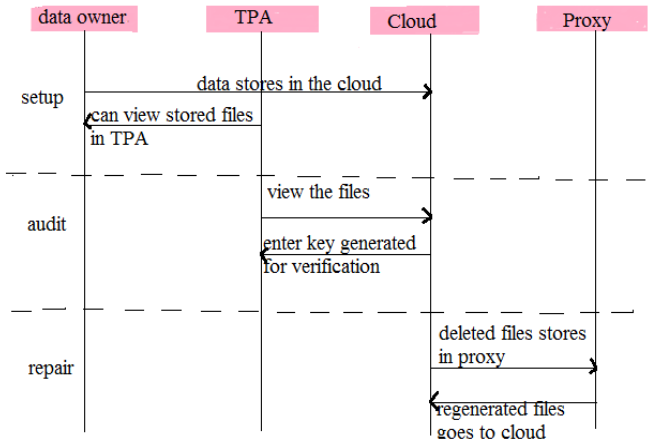

Figure 2: Sequence chart of public auditing

The sequence shown in figure 2 is explained below:

Setup: Data owner after logging in into his/her account, he/she can store their data in the cloud. The files can be viewed in the auditor. For each file stored in the cloud, a random key will be generated which the user needs whenever he wants to access his data stored in the cloud.

Audit: The data set away in the report can be seen by the customer in the commentator substance.. The auditor will ask for the secret key which was generated during file upload. If the customer enters the correct key he/she will have the ability to see the report for the most part a message will be appeared as wrong key. The auditor will send the issues related to data to the owner by sending mail.

Repair: The deleted file can be regenerated in the proxy agent. Once the information has been recovered, it will be sent to the evaluator. The auditor will send the mail regarding the data regeneration to the owner.

6. CONCLUSION

Public auditing scheme has been proposed for providing security for user uploaded files on the cloud. Nobody can view the content of the file as data is in encrypted form. Only the owner can view the file by providing secret key. Information proprietor require not need to remain on the web and continue checking records in the cloud. Proxy will act as data owner if owner is offline. This plan can make information proprietor free from taking care of his records in the cloud. It also provides good and efficient security for the files in the cloud.

ACKNOWLWDGEMENT

I would like to thank Dr. Shantharam Nayak for his valuable guidance in doing this paper.

REFERENCES

[1] C.Wang, S. S. Chow, Q.Wang, K. Ren, andW. Lou, “Privacy-preserving public auditing for secure cloud storage,” Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[2] H. Chen and P. Lee, “Enabling data integrity protection in regenerating coding- based cloud storage: Theory and implementation,” Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 407–416, Feb 2014.

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

[4] S. G. Worku, C. Xu, J. Zhao, and X. He, “Secure and efficient privacy preserving public auditing

scheme for cloud storage," Computers & Electrical Engineering, 2013.

[5] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 12, pp. 2231– 2244, 2012

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards secure and dependable storage services in cloud computing," Service Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232, May 2012.

[7] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–9.