Improved Data Integrity Protection Regenerating-Coding Based Cloud Storage

Miss. Sherkar Snehal R[1] Miss. Gagare Sital J[2] Mr.Babre Tanmay A[3] Mr. Bhangare Rohan S[4]
[1,2,3,4]Department of Computer
[1,2,3,4]SCSCOE, Rahuri Factory

Abstract— In today's world a huge amount of data is loaded on the cloud storage. The protection of such type of data is main concern. It is somewhat difficult to protect such data against corruption, checking the integrity of data and also representation of failure data. Together with this it is also critical to implement fault tolerance among such type of data against corruptions. The private auditing for regenerating codes which is nothing but the existing system, developed to address such types of problems. The private auditing for regenerating codes can generate codes for such corrupted and incomplete data, but for this, data owners always have to stay online for checking completeness as well as integrity of data. In this paper, we are introducing the public auditing technique for regenerating code, based on cloud storage. The proxy is the main component in public auditing to regenerate failed authenticators in the absence of owner of the data. A public verifiable authenticator is also designed, which is generated by a several keys and can be regenerate using partial keys. We are also using pseudorandom function to preserve data privacy by randomizing the encode coefficient. Thus our technique can successfully regenerate the failed authenticators without data owner. Experiment implementation also indicates that our scheme is highly efficient and can be used to regenerate code in cloud based storage.

Key words: Cloud server, regenerating codes, public auditing, private auditing, proxy agent

I. INTRODUCTION

Nowadays cloud storage is very popular concept for storing huge amount of data at cloud. This is due to the flexibility of cloud to provide services at any time, at any location. Security, in particular, is one of the most argued about issues in the cloud computing field; several enterprises look at cloud computing warily due to projected security risks [1]. These security risks may be lower, because, data is stored on cloud and it is difficult to find out exact location of the data on cloud.

Data owner always surfing on the internet and probably comes in contact with attackers, thus the security of data is main concern. The data stored on the cloud storage should be complete & correct. The data owner stored their data on third party cloud server probably due to flexibility, to get their data back to them whenever required. During transformation of data to cloud, data comes in contact with malicious activity which affects the integrity of data and user is completely unaware of such activity. To check the corruptions and completeness of data the user must perform auditing in order to check the integrity of data; thus it is necessary to have efficient protocol for checking the integrity and completeness of data. There are many schemes which provides the facility to data owners, to check the completeness of data and also to repair the corrupted data. Provable data possession (PDP) or proofs of retrievability (POR) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of client's data without downloading data [2].

In this paper, the focus is mainly on data corruption repair using regenerating codes. The owner of the data which wants to check the integrity as well as to repair their data send signal to Third Party Agent(TPA).TPA then checks the completeness of the data and if it founds any corruption then its send acknowledgement to proxy agent to repair the data. TPA is fully trusted and it verifies only the hash code which was send by the user for their corresponding data. The proxy agent then repairs the corrupt data and then stored on cloud server. To provide full integrity and avoid corruption on data, the public auditing is very efficient method which provides the regeneration of code using proxy agent. This scheme completely frees the online workload of user for verifying data integrity.

II. RELATED WORK

Henry C. H. Chen, Y. Hu, Patrick P. C. Lee , and Yang Tang ,"NCCloud: A Network-Coding-Based Storage System in a Cloud-of- Clouds" in that case to provide failure reparation, to detect fault across cloud servers while providing protection against internal and external attacks[3]. This purpose is deals with uploading data safely on cloud servers. However there are chances of lifetime permanent failure. This weakness causes to losses their confidential data. The drawback of this system that there is need to repair the lost data with the help of the other surviving clouds to preserve data redundancy[6]. Therefore this paper represented a term of proxy-based storage system for fault-tolerant multiple-cloud storage known as NCCloud.

Qian Wang, Cong Wang, KuiRen , Wenjing Lou, Senior, and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing"In cloud servers moves number of application software's huge data within the databases to the centrally localized large data centers where to manage the data within the database and services may not be completely reliable or trustworthy. It has a problem of security challenges regarding the problem of assuring the reliability, integrity, and completeness of the data storage in cloud computing. This paper shows the integrity to verify dynamically storage of data by allowing an TPA(Third Party Auditor) on behalf of cloud user[4]. TPA can able to perform auditing on different users from different locations.

G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession" Outsourcing of the large data storage is increasing importance which prompts a number of security issues. The main concern problem is how efficiently and securely verify that is storage cloud server is confidentially storing the client's outsourced data. The system drawback is

exacerbated by user being a tiny computing devices with limited resources [5].

III. PROPOSED SYSTEM

This system consist of two main modules which are further divided into sub modules as follows:

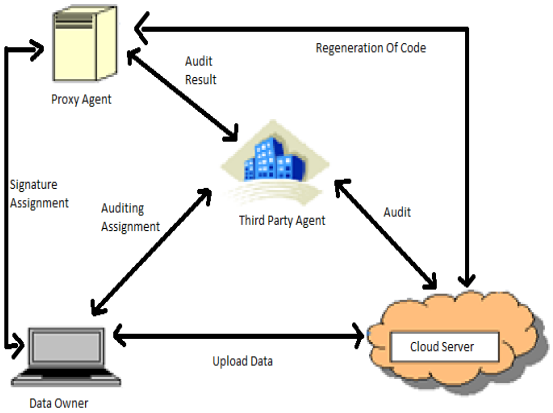

Fig. 1: System Architecture

A. Cloud Server:

Data owner sends data to cloud server, then it deals with receiving data from data owner and store the data in the encrypted form. Cloud server is responsible for give the data to read permissions to authorized user. Cloud server is used to accept and replacement of data through PA.

B. Cloud Client:

Cloud client is nothing but user or Data Owner .Data owner uploads their data on Cloud Server in the encrypted form. Cloud Client sends assignments between Data Owner and Proxy Agent .It generates a secret key and assign to the corresponding Authenticators present in the proxy agent. Data user able to see data stored on Cloud Server and it can make request to the data or file.

C. Third Party Auditor (TPA):

It is trusted to calculate and broadcast the risk of Cloud Storage Services. Data owner or user sends request to Third Party Auditor (TPA), then TPA is used to check the integrity of data stored in Cloud Server. The TPA verifies data by using Top hash value which it get from the data owner a public Auditing System consist of two phases.

1) Setup Phase:

The user or data owner initializes the public and then calculate the hash of the file and send it to the TPA.

2) Audit:

The TPA issues an audit message to cloud Server and then cloud server gives the Response message. TPA verifies the hash and if it founds the corrupted data then it sends acknowledgement to proxy agent for decision making.

D. Proxy Agent:

It accepts secret key from data Owner and it also accept Acknowledgement from the TPA and perform Re-generation of code behalf of the data Owner. The Authenticator replaces or repair the block of Data and solve integrity issue.

IV. CONCLUSION

In this paper, we used public Auditing system for Re-generating-code based cloud storage system. The Proposed System provides data integrity to the cloud; the TPA performs verification to verify the Data integrity in cloud. We introduce a Semi-trusted proxy agent. A proxy Agent is used to handle the reparation and Regeneration. Hence the system can verifies the data integrity and it secures users data.

REFERENCES

[1] Jian Liu,Kun Huang,HongRong, Huimei wang,and Ming xian, "Privacy-Preserving Public Auditing for Regenerating-code-Based cloud Storage,"IEEE Transaction on Information Forensics and security,vol.10,N0.7,July 2015.

[2] Megha Patil,Prof.G.R.Rao,"Integrity Verification in Multi-cloud storage using Cooperative Provable Data Possession ",International Journal of Computer Science and information Technoloies,vol.5(2),2014,982-985

[3] Henry C. H. Chen, Y. Hu, Patrick P. C. Lee , and Yang Tang ,"NCCloud: Network- Coding- Based Storage System in a Cloud-of- Clouds," in Proc.USENIX FAST,2012,p.21.

[4] Qian Wang, Cong Wang, KuiRen , Wenjing Lou, Senior, and Jin Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," in Computer Security.Berlin, Germany: Springer-Verlag,2009,pp. 355-370.

[5] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession"

[6] C.Wang, S.S.M. Chow, Q. Wang, K. Ren, and W.Lou,"Privacy-Preserving public auditing for secure cloud storage," IEEE Trans. Comput., vol. 62,no.2,pp. 362-375,Feb.2013.

