Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Improved Data Integrity Public Auditing for Regenerating-Code-Based Cloud Storage

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

Abstract-Cloud Computing is very important vision of computing as a utility. Using cloud storage, users can store their data into cloud. So they can enjoy high quality applications and services. Users can outsource data without the burden of local data storage and maintenance. In Cloud computing, users should be able to use cloud storage without worrying about the need to check it's integrity.so enabling public auditability for Cloud data storage should have critical importance.so users can use external audit party to check the integrity of data in Cloud Storage. Using Third Party Auditor(TPA) for checking integrity of data, the users or data owners should not have to stay online and the users are be worry-free. For using TPA the auditing process should provide security to cloud storage. Hence TPA preserves to user data privacy. In this paper, we motivate the public Auditing system of data storage security in cloud computing. Also secure Cloud storage system supports privacy preserving.TPA also supports for Batch Auditing. In public Auditing, after checking Integrity to solve the Regeneration problem of failed Authenticators, proxy agent can introduce. This is used to regenerate Authenticators in public Auditing. Hence using this scheme can completely release data owners from online burden. Also this scheme is to support scalable and efficient public Auditing. We prove the security and justify the performance of our proposed schemes.
Keywords-Cloud computing, Public Auditing, Data integrity, privacy-preserving.

I. INTRODUCTION

In today's world, Cloud storage is very important concept in Cloud Computing, in Cloud Computing huge amount of data is loaded at Cloud. Cloud Storage is now gaining popularity because it offers a flexible on-demand data outsourcing services [1].In Cloud Computing field security is main concern. Security risks may be lower, because the data stored on cloud can be easily lost or corrupted. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security cannot be directly adopted[2].In that Integrity verification of all data is not a practically possible, because when accessing the data that time it is often insufficient to detect the data corruption. It does not give the users correctness Assurance, if it is too late to recover the data loss. To protect the integrity of cloud data it is best to perform public Auditing by introducing TPA [3].TPA is nothing but an Auditing service with more powerful computation and communication Abilities. Provable data possession (PDP) mechanism is used to perform public Auditing in which PDP is designed to check the correctness of data stored in a cloud server without Retrieving the whole data. TPA can fully ensure the data integrity and save the Cloud users computation resources as well as online burden. TPA can periodically check the Integrity of all data which is stored in cloud on the behalf of the users.

In this paper, important concept is integrity verification problem in regenerating-code-based cloud storage. For checking integrity and save computation resources, we propose a public Auditing scheme for regenerating code based cloud storage, in which integrity verification are implemented by a Third-party auditor which is fully trusted and regeneration are implemented a semi-trusted proxy separately on- behalf of the data owner. After checking the integrity of data TPA send acknowledgement to proxy agent. If the data is corrupted or loss, the proxy agent then repairs the corrupted data and then stored in cloud server. Therefore to checking integrity and provide fully security and avoid corruption the public Auditing is very useful method which can regenerate the code using proxy agent.

II. LITERATURE SURVEY

H.C.H. chen and P.P.C. lee, "Enabling data integrity protection in Regenerating-coding-based cloud storage: Theory and Implementation."in that case [4] provide protection to the users data I the cloud storage against corruptions, internal or external attacks and ultimately adding failure reparation to the cloud storage along with data integrity checking ,verification and to recover faults ,becomes a crucial task. Regenerating code provides failure toleration by segmenting logical sequential data across multiple number of servers also uses minimum repair traffic than traditional remover during failure reparation code. since we are going to discuss the problem of checking the integrity and verification of Regenerating-coding-based data against internal and external attacks under a real time life cloud storage setting .we design data integrity protection DIP scheme for regenerating code and the

privacy preserving properties fault tolerance and repairing the minimum traffic.

F. sabahi Faculty of computer engineering Azad University Iran." Cloud Computing Security Threats and Responses": [5]many IT organizations facing the critical issues such as security and integrity that exist with extended implementation with the cloud computing. These types of concepts initiate which is remotely stored from the customer's location. Cloud computing extended due to projecting security risks. some problem arises that users' needs to understand as they should observes these things seriously moving business towards cloud computing.There is a solution to solve this problems is RAS issues. These are projected security risks Reliability, Security and Availability.

Yuchong Hu Student Member, IEEE, Lee, P.P.C. Student Member, IEEE; Shum, K.W, "Analysis and construction of functional regenerating codes with uncoded repair for distributed storage systems":[6] In that case the distributed storage systems applies the overabundance coding techniques to store their data. Redundancy can minimize the repairing bandwidth. i.e., the large amount of data transferred when repairing a failed storage device. Existing regenerating codes mainly require surviving storage nodes encode data during repair. This paper shows the functional minimum storage regenerating (FMSR) codes, which enables the uncoded repair. while preserving the less repair bandwidth guarantees our data and also minimizing disk reads time. FMSR codes provides intended FMSR codes.

Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloud-of-clouds": in that case ,this paper[7] provides fault tolerance to spread data across multiple cloud vendors. However, if a cloud suffers from a permanent failure and loses all its data, it is necessary to repair the lost data with the help of the other surviving clouds to preserve data redundancy. This paper presented a proxy-based storage system for fault-tolerant multiple-cloud storage called NCCloud, which achieves cost-effective repair for a permanent single-cloud failure.NCCloud is built on upper layer of network-coding-based storage and its known as functional minimum storage regenerating codes which maintains fault tolerance. FMSR provides monetary cost saving in repair over RAID-6 codes, while having comparable response time performance in cloud storage operations such as upload or download.

III. EXISTING SYSTEM

In existing system Cloud Service Providers (CSP) are separate administrator level existences. Data which is actually uploading handover or yields users ultimate over their data. However, the completeness and correctness of the data in the cloud storage is increasing the number of risks, due to following reasons. First of all, though cloud storage is powerful and reliable than personal PCs mobile phones or other devices, they are still facing the large range of attacks. The attacks which may be internal or external attacks for data integrity.

IV. DISADVANTAGES OF EXISTING SYSTEM

Cloud storage does not immediately offers the guarantee on users data integrity, completeness and availability, Though uploading confidential data to the cloud storage is primarily and economically attractive for large scale storage of data on cloud,Users cannot able to possess their storage of their data. In particular cases, simply downloading of users confidential data for its integrity and security verification is cannot be a practical solution due to highly expenditure in input and output and flow of file transfer cost across the network. As it does not able to give users correctness and completeness assurance for those data which is unassessed data and it might be late to recover the damage of files. Since it is not sufficient to detect the data faults only when accessing the data.

V. PROPOSED SYSTEM

In this paper, we introduce TPA Which is a third party auditor which audits the data stored on cloud and maintain its integrity and correctness. TPA is efficient as it removes the complete burden of user to stay online for checking the integrity of data. TPA is fully automated and perfectly monitor the confidentiality and integrity of data , stored on cloud. The Data Owner or User shared the data on cloud and it also sends the original copy of data to the proxy agent. While uploading data on cloud the data gets encrypted using RSA algorithm and Hash Code is generated using SignGen Algorithm which is send along with file on cloud, this Hash Code is also shared to the TPA. The TPA randomly audits the data stored on cloud. It challenge the data stored on cloud and as response to this the cloud service sends proof of that file to the TPA. This Proof is nothing but the Hash Code which is generated using SignGen algorithm which was already send along with the file during upload process. The TPA Compares this Hash Code with the Hash Code Shared by User or Data Owner and if it founds the data is incomplete then it simply sends acknowledgement to the Proxy Agent and as response to this Proxy Agent which is Semi-Trusted replace this incomplete file with the original file. The TPA is fully trusted and it does not gain any knowledge from cloud about user data.Thus the storage correctness is maintained.

Volume 4 Issue IV, April 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

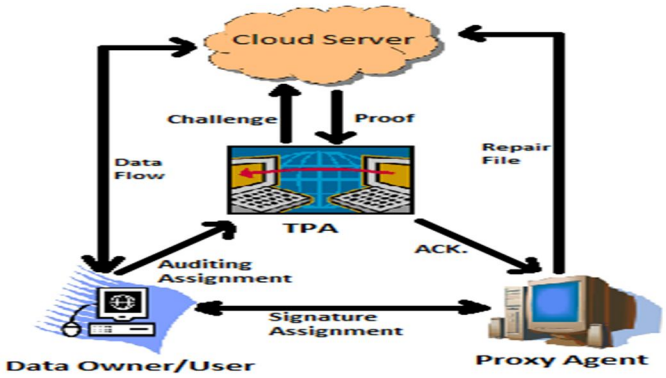


Fig: System Architecture

V. ALGORITHM

The Proposed System consists of four Algorithms (KeyGen, SignGen, GenProof, VerifyProof).

KeyGen: This algorithm is run by user to generate the key and setup the system.

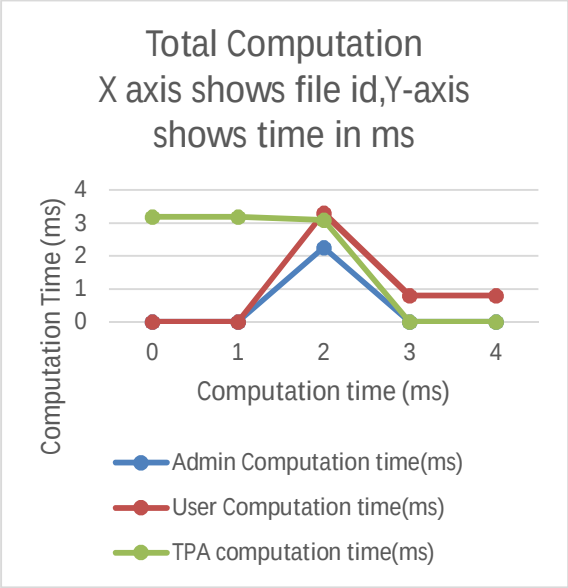
SignGen: It is used to generate Hash Code which consist of metadata. Metadata Contains parameters like File Name ,File Size, MAC Address, Signatures and other information used in auditing.

GenProof: It is generated by cloud Server. It contains the proof of file Correctness or integrity.

Verify Proof: this Scheme is run by TPA and verify whether the data is complete or not.

VI. RESULT AND ANALYSIS

Our scheme consist of three components which are 1.Data owner or user 2.Server(Admin), 3.TPA(Third Party Auditor) . The result and analysis shows the total computation of these three. The Data owner analysis shows the users download and upload time of files on cloud storage.The Server(Admin) analysis shows the privacy and integrity of outsourced data . The TPA analysis shows the computation of data integrity with File reparation.



VII. CONCLUSION

In this paper, we implemented a Public auditing system for regenerating code based cloud storage. The proposed system provide highly effective data integrity thus storage correctness is achieved. The TPA performs auditing and ensures data integrity and it does not gain any knowledge from users data so privacy gets preserved. The Proxy agent performs reparation and regeneration ,it

replaces the corrupted and incomplete data with the original one. This technique reduces the users burden to stay online for checking data integrity and replaces it with original one. The analysis shows that our technique is secured and improved in performance.

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] Boyang wang, Baochun Li, and Hui Li,"Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud."
[3] 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.
[4] H. C. H. Chen and P. P. C. Lee, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation," IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 407–416,dFeb. 2014.
[5] F. sabahi Faculty of computer engineering Azad University Iran." Cloud Computing Security Threats and Responses".
[6] Yuchong Hu Student Member, IEEE, Lee, P.P.C. Student Member, IEEE; Shum, K.W, "Analysis and construction of functional regenerating codes with uncoded repair for distributed storage systems".
[7] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloud-of-clouds".