Data Possession Of Multiple Replicas Across The Distributed Storage System By Third Party Auditor

A.Sasidhar 2D.Vijay
1,2Dept. of CSE, Pydah College of Engineering, Patavala, Yanam Road, E.G.Dt.AP, India

ABSTRACT:
Cloud computing has four models as Public cloud through which the service is obtainable to all public use. Private cloud through which service is accessible to private enterprise or organization. Community Cloud permits us to share infrastructure among various organizations through which we can achieve security, compliance and jurisdiction. Users should be able to just use the cloud storage as if it is local without worrying about the need to authenticate its integrity. Thus enabling public audit capability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA the auditing process should bring in no new vulnerabilities towards user data privacy and introduce no additional online burden to user. In this we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to execute audits for multiple users simultaneously and efficiently.

KEYWORDS: Data storage, privacy preserving, public audit ability, cloud computing, delegation, batch verification, zero knowledge.

INTRODUCTION:
The cloud data storage service contains different entities as cloud user, Third party auditor and cloud server / cloud service provider. Cloud user is a person who stores huge amount of data or files on a cloud server. Cloud server is a place where we are storing cloud data and that data will be handled by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data. The proposed system identifies that user can access the data on a cloud as if the local one without disturbing about the integrity of the data. Therefore TPA is used to make sure the integrity of data. It supports privacy preserving public auditing. It ensures the integrity of the data storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & evasion of capital outflow on hardware, software & personal maintenance.

RELATED WORK:
The method is to support scalable and well-organized privacy-preserving public storage auditing in cloud. Purposely our scheme attains batch auditing where numerous delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner. We prove the security and justify the performance of our proposed schemes through tangible experiments and comparisons with the state of the art. We inspire the public auditing system of data storage security in cloud computing and provide a privacy-preserving auditing protocol. Our scheme facilitates an external auditor to audit user’s cloud data without learning the data content. The work utilizes the method of public key-based homomorphism linear authenticator which enables TPA to execute the auditing without demanding the local copy of data and thus considerably reduces the communication and computation overhead as compared to the straightforward data auditing approaches.

LITERATURE SURVEY:
Cloud Computing has been visualized as the next-generation structural design of IT Enterprise. It progresses the application software and databases to the centralized large data centers where the management of the data and services may not be completely responsible. This exclusive pattern carries out about many new security challenges which have not been well understood. This work studies the difficulty of ensuring the reliability of data storage in Cloud Computing. In meticulous we deem the task of allowing a third party auditor (TPA) on behalf of the cloud client to confirm the reliability of the dynamic data stored in the cloud. The introduction of TPA get rid of the participation of the client through the inspection of whether his data stored in the cloud is indeed intact which can be significant in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation such
as block modification, insertion and deletion is also a important step toward practicality since services in Cloud Computing are not inadequate to archive or backup data only. While previous works on ensuring remote data reliability often be short of the support of either public audit ability or dynamic data operations. We first recognize the complexities and potential security problems of direct extensions with fully dynamic data updates from previous works and then show how to build a graceful authentication scheme for the seamless integration of these two salient features in our protocol design. In particular to attain efficient data dynamics we perk up the existing proof of storage models by manipulating the classic Merkle Hash Tree construction for block tag authentication.

EXISTING METHOD:

From the viewpoint of protecting data privacy, the users who own the data and rely on TPA just for the storage safety of their data do not want this auditing process bring in new vulnerabilities of unofficial information seepage in the direction of their data security. Public audit ability permits an external party in addition to the user himself to confirm the accuracy of remotely stored data. Though most of these systems do not regard as the privacy protection of users data against exterior auditors. Certainly they may potentially disclose user data to auditors. This rigorous disadvantage deeply influence the safety of these protocols in cloud computing.

DISADVANTAGES:

Especially downloading all the data for its reliability confirmation is not a sensible solution due to the expensiveness in I/O and transmission cost across the network. Moreover, it is frequently inadequate to notice the data corruption only when accessing the data as it does not give users accuracy declaration for those un accessed data and might be delayed to improve the data loss or damage. Unofficial data seepage still remains possible due to the potential exposure of decryption keys.

PROPOSED METHOD:

Extensive protection and performance analysis shows the proposed schemes are probably safe and highly proficient. To maintain proficient handling of various auditing tasks we further look at the technique of bilinear aggregate signature to expand our chief result into a multi-user setting where TPA can do various auditing tasks concurrently.

ADVANTAGES:

Batch auditing to allow TPA with secure and proficient auditing capability to deal with multiple auditing delegations probably large number of different users concurrently. Public audit ability consent to TPA to confirm the accuracy of the cloud data on demand without retrieving a copy of the whole data or bring in additional online burden to the cloud users. Storage accuracy to make certain that there exists no corrupt cloud server that can pass the TPA’s audit without indeed storing user’s data integral. Privacy preserving to make certain that the TPA cannot gain users data content from the information gathered during the auditing process.

SYSTEM ARCHITECTURE:

Assuming that the data reliability threats towards user data can come from both internal and external attack at CS. These may contain software bugs, hardware failures, bugs in the network path, economically motivated hackers, malicious or accidental management errors etc. CS might even choose to hide these data corruption incidents to users. Auditing service deliver a cost-effective method for users to get trust in cloud. Considering the TPA is reliable and independent.

PRIVACY-PRESERVING PUBLIC AUDITING MODULE:

To attain privacy-preserving public auditing we suggest to exclusively integrating the homomorphic authenticator with random mask technique. The linear combination of sampled blocks in the server’s response is covered with randomness generated by a pseudo random function (PRF). Homomorphic authenticators are remarkable authentication metadata generated from individual data blocks which can be strongly aggregated in such a way to guarantee an auditor that a linear combination of data blocks is appropriately
computed by verifying only the aggregated authenticator.

**BATCH AUDITING MODULE:**

Batch auditing not only permits TPA to carry out the multiple auditing tasks concurrently but also significantly reduces the calculation cost on the TPA side. Establishment of privacy-preserving public auditing in Cloud Computing TPA may concurrently handle various auditing allocation upon different user requirements. The individual auditing of these errands for TPA can be monotonous and very incompetent.

**DATA DYNAMICS MODULE:**

This technique is designed to achieve privacy-preserving public risk auditing with support of data dynamics. Supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. The main system can be modified to build upon the obtainable work to support data dynamics with block level operations of modification, deletion and insertion.

**ALGORITHMS USED:**

**TOKEN PRE-COMPUTATION:**

1: procedure  
2: Choose parameters l, n and function f, _;  
3: Choose the number t of tokens;  
4: Choose the number r of indices per verification;  
5: Generate master key K p rp and challenge k chal;  
6: for vector G(j), j ← 1, n do  
7: for round i ← 1, t do  
8: Derive _i = fk chal (i) and k(i) prp from KPRP .  
9: Compute v(j)i = Pr q=1 _qi * G(j)[k(i)prp (q)]  
10: end for  
11: end for  
12: Store all the vi.s locally.  
13: end procedure

10: else  
11: for (j ← 1, n) do  
12: if (R(j)i ≠ v(j)i ) then  
13: return server j is misbehaving.  
14: end if  
15: end for  
16: end if  
17: end procedure

**ERROR RECOVERY:**

1: procedure% Assume the block corruptions have been detected among % the specified r rows; % Assume s ≤ k servers have been identified misbehaving  
2: Download r rows of blocks from servers;  
3: Treat s servers as erasures and recover the blocks.  
4: Resend the recovered blocks to corresponding servers.  
5: end procedure.

**CONCLUSION:**

Using cloud storage, user can distantly store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources without the burden of local data storage and maintenance. Though the fact the user on longer have physical control of the outsourced data makes the data integrity protection in cloud computing a formidable task particularly for the users with constrained computing resource. Facilitate public audit ability for cloud storage is of significant importance so that user can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To steadily introduce an effective TPA the auditing process should bring in no new vulnerabilities towards user data privacy and bring in no additional online burden to user.

**REFERENCES:**


Mr. A. Sasedhar is a student of Pydah College of Engineering, Patavala. Presently he is pursuing his M.Tech [Computer Science Engineering] from this college and he received his B.Tech from Adarsh College of Engineering, affiliated to J N T University, Kakinada in the year 2012. His area of interest includes Computer Networks and Object oriented Programming languages, all current trends and techniques in Computer Science.

Mr. D. Vijay, well known Author and excellent teacher Received M.Tech (CSE) from Pragati Engineering College is working as Assistant Professor, Department of M.Tech Computer science engineering, Pydah College of Engineering. He is an active member of ISTE. He has 3 years of teaching experience in various engineering colleges. To his credit couple of publications both national and international conferences/journals. His area of Interest includes Information security, Computer Networks and other advances in computer Applications.