International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
NATIONAL CONFERENCE on Developments, Advances & Trends in Engineering Sciences
(NCDATES- 09th & 10th January 2015)

RESEARCH ARTICLE OPEN ACCESS

Processing and Regaining Storage of Secured Data in Cloud

A.V.H. Sai Prasad, S.Naga Chandra Sekhar , S. Naga Sindhu
Associate Professor, Associate Professor, Assistant Professor

Abstract:
Using cloud storage, users can remotely 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. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in cloud computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability 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 toward user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design
Keywords: Data storage, privacy preserving,public auditability, cloud computing, delegation, batch verification, zero knowledge.

INTRODUCTION:

CLOUD computing has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transfer-ence of risk [2]. As a disruptive technology with profound implications, cloud computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data are being centralized or outsourced to the cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with location independence, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etcfor data security and combating unwanted access.

Though data encryption makes effectual data consumption a very demanding task .The objective is to deploy the most basic data services include data management and data utilization with included dependability and privacy assurance as well as high level service performance, usability and scalability.

RELATED WORK:

The proposition allow a TPA to remain online storage sincere by first encrypting the data then distribution a number of pre computed symmetric-keyed hashes over the encrypted data to the auditor.

The auditor verifies both the integrity of the data file and the server's control of a previously committed decryption key. This system only works for encrypted files and it suffer from the auditor state fullness and bounded usage which may potentially carry in online load to users when the keyed hashes are used up. The dynamic version of the prior provable data possession (PDP) scheme using only symmetric key cryptography but with a enclosed number of audits. Consider a alike support for partial dynamic data storage in a spread scenario with added feature of data error localization.

EXISTING METHOD:

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. 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.

DISADVANTAGE 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 unaccessed 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:

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. Extensive protection and performance analysis shows the proposed schemes are probably safe and highly proficient.

ADVANTAGES:

Public auditability 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. Batch auditing to allow TPA with secure and proficient auditing capability to deal with multiple auditing delegations probably large number of different users concurrently.

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:

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. Summary 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).

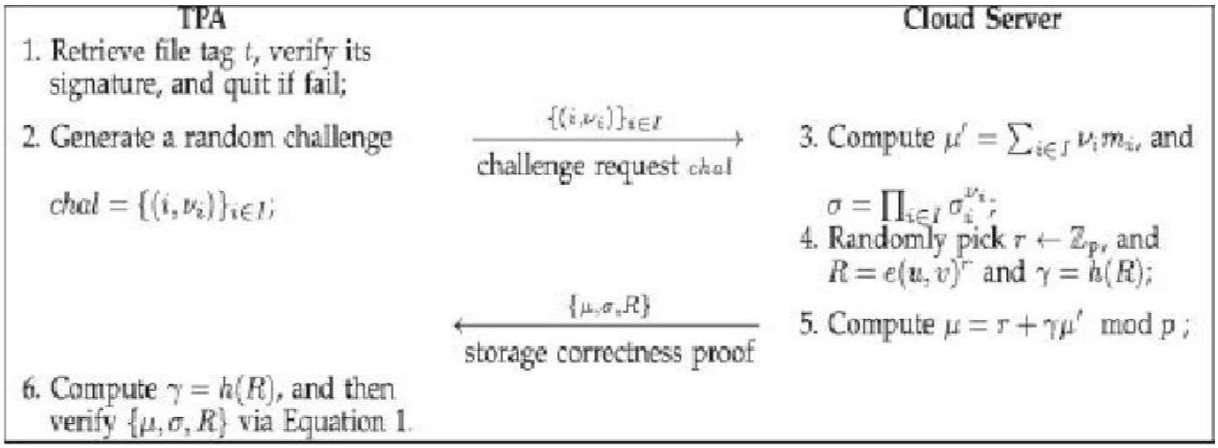
BATCH AUDITING MODULE:

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. 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.

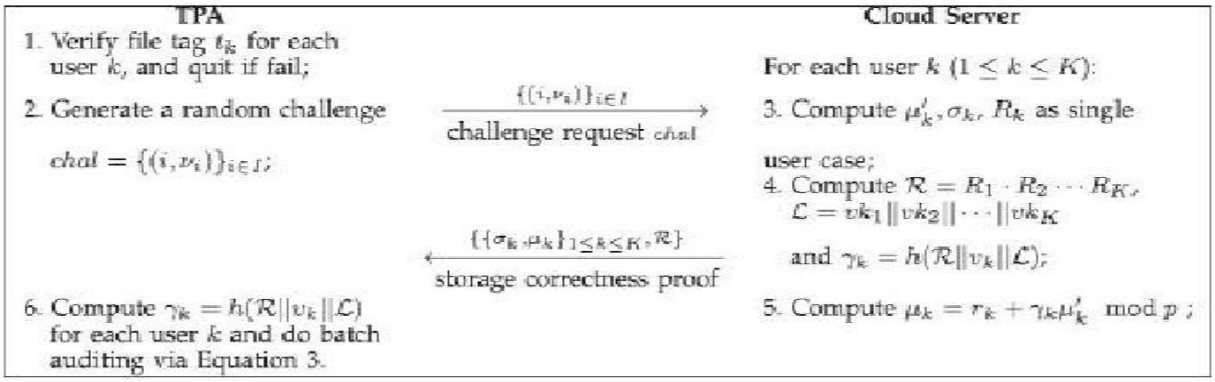
DATA DYNAMICS MODULE:

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. This technique is designed to achieve privacy-preserving public risk auditing with support of data dynamics.

The Privacy-Preserving Public Auditing Protocol



The Batch Auditing Protocol



RESULT:

In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud comput-ing. We utilize the homomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently.

REFERENCES:

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.

[2] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/ index.html, June 2009.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above theClouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

[4] Cloud Security Alliance, "Top Threats to

Cloud Computing," http://www.cloudsecurityalliance.org,2010.

[5] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.

[6] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http:// www.techcrunch.com/2008/07/10/mediamaxt helinku p-closesits-doors/, July 2008.