International Journal of Science Engineering and Advance Technology

To Provide A Privacy Preserving Auditing Protocol In Cloud Computing Using Tpa

1 M.Vamsi Krishna, 2 Dr.K.V.V.S.Narayana Murthy, 3V.Sailaja
Dept. of CSE, Chaitanya Institute of Science & Tech., Madhavapatnam, Kakinada. E.g.dt, AP, India

Abstract:
To completely make sure the data honesty and save the cloud users' calculation possessions as well as online burden it is of significant importance to facilitate public auditing service for cloud data storage so that users may alternative to an independent third-party auditor (TPA) to review the outsourced data when needed. The TPA who has know-how and potential that users do not can episodically check the integrity of all the data stored in the cloud on behalf of the users which provides a much more easier and reasonable way for the users to make sure their storage correctness in the cloud. Furthermore in addition to help users to evaluate the hazard of their subscribed cloud data services the audit results from TPA would also be advantageous for the cloud service providers to recover their cloud-based service platform and even serve up for independent negotiation purposes. In a word facilitate public auditing services will participate an important role for this promising cloud economy to become fully established where users will need ways to measure risk and gain trust in the cloud.

Keywords: Data storage, privacy preserving, public auditability, cloud computing, delegation, batch verification, zero knowledge.

Introduction:

The concept of public auditability has been proposed in the background of make sure remotely stored data integrity under different system and security models. Using cloud storage users can tenuously 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 reliability protection in cloud computing a terrifying task particularly for users with constrained computing resources. Additionally users should be able to just use the cloud storage as if it is local without perturbing about the need to verify its reliability. Therefore enabling public auditability for cloud storage is of significant importance so that users can option to a third-party auditor (TPA) to check the integrity of outsourced data and be worry free. To strongly bring in an effective TPA the auditing process should bring in no new vulnerabilities toward user data privacy and bring in no additional online burden to user. In this paper we suggest a secure cloud storage system supporting privacy-preserving public auditing. We additional make bigger our result to facilitate the TPA to perform audits for multiple users concurrently and efficiently.

Related Work:

RSA-based homomorphic linear authenticators for auditing outsourced data and propose randomly sampling a few blocks of the file. Though amid their two proposed schemes the one with public auditability representation the linear combination of sampled blocks to external auditor. When used directly their procedure is not provably privacy preserving and thus may escape user data information to the external auditor. Juels et al. explain a "proof of retrievability (PoR) model where spot-checking and error-correcting codes are used to make sure both possession and retrievability of data files on remote records service systems. Nevertheless the number of audit challenges a user can carry out is fixed a priori and public auditability is not supported in their main scheme. Although they portray a straightforward Merkle-tree construction for public PoRs. This approach only works with encrypted data. Shacham and Waters design an improved PoR scheme put up from BLS signatures with proofs of security in the security model defined. Similar to the construction in they use publicly demonstrable homomorphic linear authenticators that are built from provably secure BLS signatures.

Literature Survey:

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It is in motion the application software and databases to the centralized large data centres where the management of the data and services may not be completely dependable. This exclusive paradigm brings about many new security challenges which have not been well understood. This work studies

the problem of ensuring the integrity of data storage in Cloud Computing. In exacting we consider the task of allowing a third party auditor (TPA) on behalf of the cloud client to confirm the integrity of the dynamic data stored in the cloud. The introduction of TPA eradicate the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact, which can be important 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 significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design.

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. Though most of these systems do not regard as the privacy protection of users data against exterior auditors. Public audit ability permits an external party in addition to the user himself to confirm the accuracy of remotely stored data. 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 unaccessed data and might be delayed to improve the data loss or damage.

Proposed Method:

We motivate the public auditing system of data storage security in cloud computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content.

To the best of our knowledge, our scheme is the first to support scalable and efficient privacy-preserving public storage auditing in cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.

ADVANTAGES:

Users may resort to an independent third-party auditor to audit the outsourced data.

TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users.

TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform.

Our scheme enables an external auditor to audit user's cloud data without learning the data content.

By using Data regaining algorithm recovering the users lost data in cloud

System Architecture:

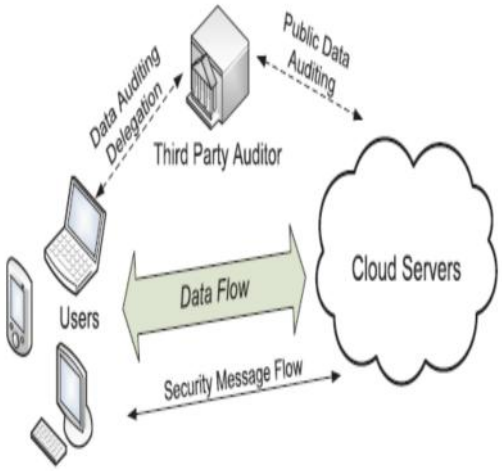


Fig. 1. The architecture of cloud data storage service.

The cloud user who have large amount of data files to be stored in the cloud. The cloud server which is handled by the cloud service provider to present data storage service and has significant storage space and computation resources. The third-party auditor who has proficiency and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. They may also dynamically interrelate with the CS to access and inform their stored data for various application purposes. As users no longer possess their data locally it is of critical importance for users to ensure that their data are being correctly stored and maintained. To save the computation resource as well as the online burden potentially brought by the periodic storage correctness verification cloud

users may resort to TPA for ensuring the storage integrity of their outsourced data, while hoping to keep their data private from TPA.

Design Goals:

Public auditability to permit TPA to confirm the rightness of the cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to the cloud users. Storage correctness to ensure that there exists no cheating cloud server that can pass the TPA's audit without indeed storing users' data intact. Privacy preserving to ensure that the TPA cannot derive users' data content from the information collected during the auditing process. Batch auditing to enable TPA with secure and efficient auditing capability to cope with multiple auditing delegations from possibly large number of different users simultaneously. Lightweight to allow TPA to perform auditing with minimum communication and computation overhead.

Privacy-Preserving Public Auditing Module:

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). 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:

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. Establishment of privacy-preserving public auditing in Cloud Computing TPA may concurrently handle various auditing allocation upon different user requirements.

Data Dynamics Module:

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. Supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance.

PRIVACY PRESERVING PUBLIC AUDITING PROTOCOL:

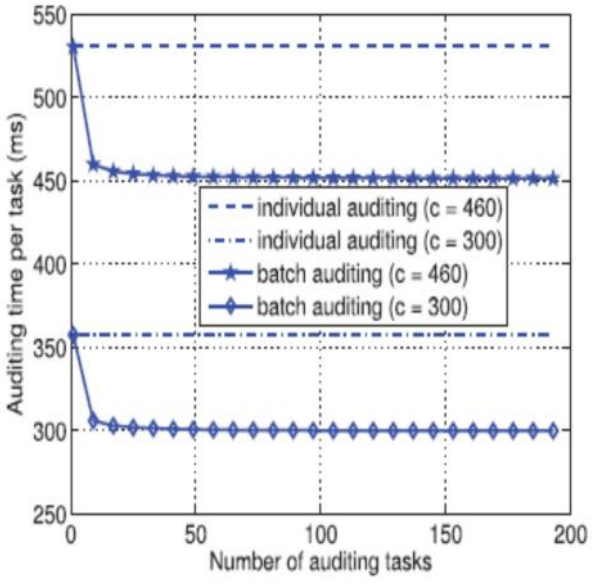
1. The user blinds each file block data before file distribution k is the secret key for data vector is generated
2. Based on the blinded data vector, the User generates k parity vector via the secret matrix P.
3. The user calculates the ith token for server j.
4. The user sends the token secret matrix P, permutation and challenge key Kmaster key, and kchal to TPA for auditing delegation.

The blinding values in the servers are not taken by TPA response of the server are verified directly. As TPA does not know the secret blinding key there is no way for TPA to learn the data content information during auditing process. Thus the privacy-preserving third party auditing is achieved.

Data Regaining Algorithm

1: procedure
% Assume the block corruptions have been detected
among % the specified r rows;
% assumes 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

Batch Auditing Efficiency:



Conclusion:

TPA may simultaneously handle numerous audit sessions from dissimilar users for their outsourced

data files. We additional extend our privacy-preserving public auditing protocol into a multiuser setting where the TPA can execute multiple auditing tasks in a batch manner for better competence Extensive analysis shows that our schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 illustration further shows the quick presentation of our design on both the cloud and the auditor side. We depart 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. We propose a privacy-preserving public auditing system for data storage security in cloud computing. 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 saddle of cloud user from the boring and possibly expensive auditing task but also improve the users panic of their outsourced data outflow.

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 the Clouds: 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/mediamaxthelinkup-closesits- doors/, July 2008.
[7] Amazon.com, "Amazon s3 Availability Event: July 20, 2008," http://status.aws.amazon.com/s3-20080720.html, July 2008.
[8] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011.
[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 598-609, 2007.
[10] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-Preserving Audit and Extraction of Digital Contents," Cryptology ePrint Archive, Report 2008/186, 2008.
[11] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.
[12] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance. org, 2009.
[13] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.
[14] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[15] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th USENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.
[16] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," http://aspe.hhs.gov/ admnsimp/pl104191.htm, 1996.

Sri. M. Vamsi krishna, well Known Author and excellent teacher Received M.Tech (AI &R), M.Tech (CS) from Andhra university is working as Professor and HOD, Department of CSE, Chaitanya Institute Science and Technology. He has 13 years of teaching & research experience. He has 20 publications of both national and international conferences /journals. His area of Interest includes AI, Computer Networks, information security, flavors of Unix Operating systems and other advances in computer Applications.

Dr.K.V.V.S.Narayana Murthy M.Tech, Ph.D. Professor of CSE department in Chaitanya Institute of Science & technology. He has 15 years of teaching & research experience to his credit number of publications both national and international conferences /journals. His area of interest includes compiler design, formal languages and automata theory, computer organization.

Miss.V.Sailaja is a student of Chaitanya Institute of Science & Technology, Madhavapatnam, Kakinada Presently she is pursuing her M.Tech [computer science Engineering] from this college and she received M.C.A from Andhra UniversityP.G Centre Tadepalligudem, Tadepalligudem in the year 2007.Her area of interest includes datawarehousing, cloud computing and object oriented languages, current trends in computer science.