Public Auditing System of Data Storage Securing Nature in Cloud Computing

P. Ramanjaneya Prasad [α] & M. Madhavi [σ]

Abstract - **Cloud computing, large number of computers that are connected through a real-time communication network. The users are flexible while storing their information in cloud network. At any time period they are capable of accessing their information from network. By this application the way of storage of users reduces the maintenance complexity. It works on providing the access to the users in the cloud network audit ability for cloud data storage security is key importance so that users can stay to there will be third party auditor to keep data efficiently. With the secure introduce an effective third party auditor (TPA); there are the two fundamental requirements. 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.**

I. Introduction

Cloud computing features are cost efficient, usage efficiency, comfortable managing, and service providing at any moment and importantly a key challenge is to used build secrecy that the cloud is capable of maintaining user data securely. Users needs privacy of their data, and also want to benefit from the rich computational applications that application developers will offer using that data. So, the cloud gives little platform-level support or standardization for user data protection not upto level data encryption at rest. Protecting user information while even through rich computations needs both specialized expertise and resources that may not be spot available to most developers. Keeping the platform layer protected is: the platform can gain economies of scale by less costs and distributing sophisticated security solutions in various applications and their developers. In users way of thinking organizations and normal pc user use flexibly this is advantage to them. No need to bother about personnel maintenances like hardware, software etc. While Cloud Computing makes these advantages more appealing than ever, it also brings new and challenging security threats towards users' updated data. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate privacy control on user's profile and their data which is stored in cloud computing or cloud network previously. This is the way where the efficiency of data increases. The attractive features of cloud computing they are most powerful and reliable than the normal pc, they have problems for data integrity and external threats of the broad range of both internal. And there is threat of security attacks more than the cloud services appear from time to time. And another one is for CSP untrust fully to customers of cloud in situation of their updated data. The way of working in reality, CSP might reclaim storage for monetary reasons by deleting data which was not accessed much, or may be encrypting the data that keeps reputation. In short, although outsourcing data to the cloud is economically attractive for massive data storage over a huge time period, it won't work immediately offer any guarantee on data integrity and accessibility. If this cause is not perfectly mentioned may blocks service of cloud architecture. If there is no hard disk memory with the users, for the security purpose traditional cryptographic primitives will e used. In particular, simply downloading all the data for its integrity verification is in reality it is too expensive on I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those un accessed data and might be too 2 late to backup of data. Under taking huge amount of the updated data and the user's constrained resource capability, the tasks of auditing the data correctness in a cloud network can be complex and high cost for the cloud users. Moreover, the overhead of using cloud storage should be minimized as much as possible, such that user does not need to perform too many operations to use the data (in additional to retrieving the data). For example, it is desirable that users do not need to worry about the need to verify the integrity of the data before or after the data retrieval. The TPA, the people having good experience with the users that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to explore the risks to the customers of their subscribed cloud data services, the cloud service providers to improve their cloud based service platform, and even serve for independent arbitration purposes. In a word, enabling public auditing services will become a part to create cloud economy completely developed;

Authors α, σ : M.Tech, CSE Dept, ASRA Hyderabad.
E-mail : karu197903@yahoo.com, madhavi_3101@yahoo.co.in

then customers get security among the risks and keeps trust in the cloud. Recently, the notion of public audit ability was explored in the context of ensuring remotely stored data integrity under different system and security models. Public audit ability allows another third party along with the user to modify the data which was stored in the cloud. A lot of schemes will not work out on privacy protection of users' data against external auditors. Indeed, Server gives the complete information to customers' information to the auditors. This severe drawback greatly affects the privacy schemas in Cloud network. In the case of protecting data privacy, the normal user which stores their general information won't need any of these schemas or auditing process and also exploring of threats of unauthorized accessing towards their data privacy. There are so many external or so called private organizations keeps restrictions on their data which was placed in the cloud not to share to third parties. Usage of data encryption while before uploading the data is one of privacy protecting by the cloud, this is what was best way to the privacy preserving public auditing scheme that was explored in this paper. If there is no perfect designed auditing protocol, encryption won't work out data from "flowing away" by UN authorized persons during the auditing process. Means it completely solves the problem of protecting data privacy but just reduces it to the key management. The persons which are not having permissions are accessing the information is a critical problem cause of decrypting the keys. So keeping the privacy-preserving third-party auditing protocol, not based on data encryption, is the threat which we are going to work in this paper. The workouts are on supporting on privacy-preserving public auditing in Cloud network, taking key as data storage. Apart of this, with the popularity of Cloud Computing, a increase of auditing tasks from different users may be delegated to TPA. Result of individual auditing of increasing rate can be annoying and bulky; a normal curious task is how to enable the TPA to efficiently work large number of auditing tasks in a batch parallel. Identifying these problems, our work use the of schema public key based Homomorphic linear authenticator which enables TPA to do auditing without need of data which was stored locally and computations as compared to the straightforward data auditing approaches. By integrating the HLA with random masking, our protocol guarantees that the TPA doesn't contain any records about the data stored in the cloud network during auditing.

II. Problem Statement

Those are 1) TPA should be able to efficiently does auditing job in the cloud data base with no need of additional local copy of data. This gives advantages that makes user comfortable. Mostly, our addition in this work is:

1. Creating interest public auditing system of data storage securing nature in Cloud Computing and providing a privacy-storing, auditing protocol.
2. This method is the premier one that gives flexibility of scalable and efficient public auditing in the Cloud Computing. In particular, our scheme achieves batch auditing where multiple assigned auditing actions from different users can be performed concurrently by using TPA.
3. We prove the security and advocate the efficiency of our methodology through concrete experiments and comparisons with the state-of-the-art.

a) Security and Privacy Challenges

It's is not that easy to create a data-protection solution for the threats in the cloud, cause of cloud network itself includes so many various elements. Result of work done will be stored in particular domain accordingly; main spot will be on widely used apps such as e-mail, personal financial management, social networks, and business tools such as word processors and spread sheets. The following are the class of applications used.

- Provide services to a huge quantity of various end users, as against to huge data workflow management for a single entity.
- Use a data model consisting mostly of sharable units, where all data objects have access control lists (ACLs) with one or more users.
- Developers are capable of performing the operations of apps in another computing platform those are the physical infrastructure, job scheduling, user authentication, and the base software environment, which makes easy to perform but not for in the same platform.

Overly rigid security is as detrimental to cloud service value as inadequate security. A primary challenge in designing a platform-layer solution useful to many applications is ensuring that it enables rapid development and maintenance. To ensure a practical solution, we considered the following goals relating to data protection as well as ease of development and maintenance.

- Integrity. The user's stored data won't be corrupted.
- Privacy. Private data won't be leaked to any unauthorized entity.
- Access transparency. Logs will clearly indicate who or what accessed any data.
- Ease of verification. Users will be able to easily verify what platform or application code is running, as well as whether the cloud has strictly enforced their data's privacy policies.
- Rich computation. The platform will allow efficient, rich computations on sensitive user data.
- Development and maintenance support. Because they face a long list of challenges bugs to find and

fix, frequent software upgrades, continuous usage pattern changes, and user demand for high performance developers will receive both development and maintenance support.

Any credible data protection approach must grapple with these issues, several of which are often overlooked in the literature.

III. System Development

a) *Privacy-Preserving Public Auditing*

Homomorphism based authenticators are outstanding metadata outlet from each data block individually, which can be protected in the way to assure an auditor that a linear clubbed of data blocks is correctly calculated by verifying only the aggregated authenticator. Complete view to achieve privacy-preserving public auditing, we prefers to uniquely integrate the Homomorphic authenticator with the help of technique random mask. In our study, the linear combination of sampled blocks in the server's response is masked with randomness produced by a pseudo random function (PRF).

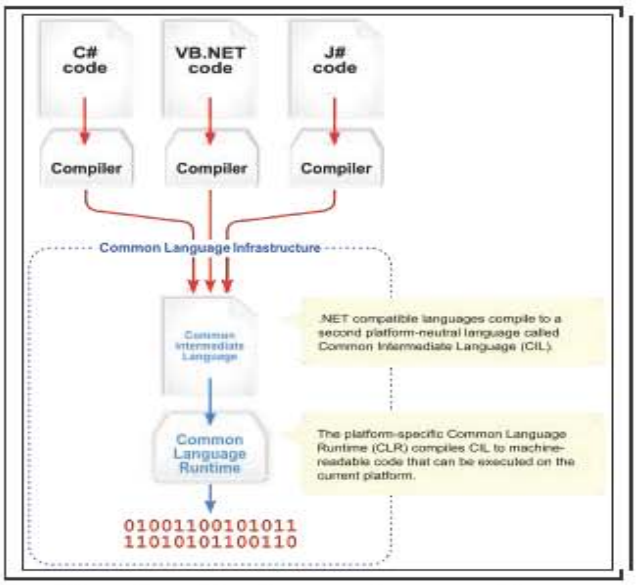
The proposed scheme is as follows:

- Setup level
- Audit level

i. *Batch Auditing*

By using privacy-preserving public auditing in Cloud Computing, TPA may concurrently manages a lot auditing delegations according to various users' requests. The each auditing of these operations for TPA can be clumsy and not efficient. Batch auditing not only allows TPA to perform the various auditing tasks parallel, but also efficiently reduces the computation cost on the TPA side.

Architecture



Visual Overview of the Common Language Infrastructure

ii. *Data Dynamics*

At last, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Here we explored how our scheme can be adapted to do operations on already existing work to support data dynamics, including block level operations of alterations, deletion and insertion. We are capable of using this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

IV. Related Work

The defined "provable data possession" (PDP) model for ensuring possession of data files on harmful storages. Their scheme uses the RSA based Homomorphic linear authenticators for auditing already stored data and prefers randomly sampling a few blocks of the file. Moreover, the general audit ability in their scheme requires the linear combination of sampled blocks shown to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. In "proof of retrieve ability' (PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrieve ability" of data files on re- mote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public audit ability is not supported in their main scheme. Although they describe a straight forward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Dodis et al. give a study on different variants of PoR with private auditability.

Design an improved PoR scheme built from BLS signatures with full proofs of security in the security model defined in. Similar to the construction in, they use publicly verifiable homomorphic linear authenticators that are built from provably secure BLS signatures. Based on the elegant BLS construction, a compact and public verifiable scheme is obtained. Again, their approach does not support privacy-preserving auditing for the same reason as. Shah et al. propose allowing a TPA to keep online storage honest by first encrypting the data then sending 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 possession of a previously committed decryption key. This scheme only works for encrypted files and it suffers from the auditor statefulness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up. In other related work, Ateniese et al. Propose a partially dynamic version of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits. In, Wang et al. consider a similar support for partial dynamic data storage in a distributed scenario with additional feature

of data error localization. In a subsequent work, Wang et al. propose to combine BLS-based HLA with MHT to support both public audit ability and full data dynamics. Almost simultaneously, Erway et al. Developed a skip lists based scheme to enable provable data possession with full dynamics support. However, the verification in these two protocols requires the linear combination of sampled blocks just as, and thus does not support privacy- preserving auditing. While all the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving public auditing in cloud computing. More importantly, none of these schemes consider batch auditing, which can greatly reduce the computation cost on the TPA when coping with a large number of audit delegations.

a) Virtual Administration

The advent of cloud has changed the role of System Administrator to a "Virtual System Administrator". This simply means that daily tasks performed by these administrators have now become even more interesting as they learn more about applications and decide what's best for the business as a whole. The System Administrator no longer has a need to provision servers and install software and wire up network devices since all of that grunt work is replaced by few clicks and command line calls. The cloud encourages automation because the infrastructure is programmable. System administrators need to move up the technology stack and learn how to manage abstract cloud resources using scripts.

Likewise, the role of Database Administrator is changed into a "Virtual Database Administrator" in which he/she manages resources through a web-based console, executes scripts that add new capacity programmatically in case the database hardware runs out of capacity and automates the day-to-day processes. The virtual DBA has to now learn new deployment methods (virtual machine images), embrace new models (query parallelization, geo-redundancy and asynchronous replication, rethink the architectural approach for data and leverage different storage options available in the cloud for different types of datasets. In the traditional enterprise company, application developers may not work closely with the network administrators and network administrators may not have a clue about the application. As a result, several possible optimizations in the network layer and application architecture layer are overlooked. With the cloud, the two roles have merged into one to some extent. When architecting future applications, companies need to encourage more cross-pollination of knowledge between the two roles and understand that they are merging.

V. Conclusion

In this paper, we explore a Cloud Computing new entity privacy-preserving public auditing system for the purpose of data storage security, where TPA works on auditing details without need of data which was stored locally. Here we uses the authenticator with feature of homomorphism and also using technique random mask to create trust on cloud that used TPA will not get or bother about the information which was stored by the user while auditing process, it also reduces the workflow to cloud user from the annoying and cost efficient auditing task, but also take the edge off the users to decrease the fear of their uploaded data privacy. Under taking TPA may concurrently handle different audit levels from various users for their updated data files, in addition we extend our privacy-preserving public auditing protocol from single user to multi-user, here TPA workouts on various number of auditing tasks parallel. Efficient security and performance analysis gives reports that the proposed techniques are secure and highly efficient. The mighty features of the proposed schemes reduce the burden of economies in future for Cloud Computing.

References Références Referencias

1. 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," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
2. N. Gohring, "Amazon's s3 down for several hours," Online.http://www.pcworld.com/businesscenter/article/142549/amazons s3 down for several hours.html, 2008.
3. Amazon.com, "Amazon s3 availability event: July 20, 2008," Online at http://status.aws.amazon.Com/s3-20080720.html, July 2008.
4. S. Wilson, "Appengine outage," Online at http://www.cio-weblog.com/50226711/appengineou tage.Php, June 2008.
5. B. Krebs, "Payment Processor Breach May Be Largest Ever," Online at http://voices.Washingonpost.Com/securityfix/2009/01/payment processor breach may b.html, Jan. 2009.
6. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," Cryptology ePrint Archive, Report 2007/202, 2007, http://eprint.iacr.org/.
7. M. A. Shah, R. Swaminathan and M. Baker, "Privacy-preserving audit and extraction of digital contents," Cryptology ePrint Archive, Report 2008/186, 2008, http://eprint.iacr.org/.
8. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for

storage security in cloud computing," in Proc. of ESORICS'09, Saint Malo, France, Sep. 2009.
9. Cloud Security Alliance, "Security guidance for critical areas of focus in cloud computing," 2009, http://www.cloudsecurityalliance.org.
10. H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.
11. A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.
12. M. A. Shah, M. Baker, J. C. Mogul, and R. Swaminathan, "Auditing to keep online storage services honest," in Proc. of HotOS'07. Berkeley, CA, USA: USENIX Association, 2007, pp. 1–6.
13. 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996, last access: July 16, 2009.
14. D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and verifiably encrypted signatures from bilinear maps," in Proc. of Eurocrypt 2003, volume 2656 of LNCS. Springer-Verlag, 2003, pp. 416–432.

This page is intentionally left blank