International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 18
December 2016

Confidentiality On Public Auditing For Secure Data Storage In Cloud

[1] R. Nethravathi,[2] S. Vahini

[1]PG Scholar, Dept.of S.E., SR Engineering college, Warangal, Telangana, India, nethravathi542@gmail.com
[2]Assistant professor, Dept.of CSE,SR Engineering college, Warangal, Telangana, India, vahini.siruvoru@gmail.com

Abstract: Currentlyclients no longer have physical presence of theoutsourced facts which makes the data security better.Additionally, clients should be in a position to only use the cloudstorage as if it is local, without traumatic concerning the itsintegrity. Consequently a few principal security challengesare arise and inspire the researchers for furtherinvestigations. Considering of this valuable problemsclients canresort to a third party auditor (TPA) to verify the integrityof outsourced data. To securely introduce an robustTPA, the auditing system must bring in no newvulnerabilities in the direction of consumer knowledge privateness, and introduceno extra on-line burden to person. In this paper, wepropose a comfort cloud storage procedure assistingprivacy-preserving public auditing. We additional lengthenour effect to permit the TPA to participate in audits fora couple of users concurrently and effectively. Largesafety and performance analysis exhibit the proposedschemes are provably comfortable and extremely effective.

Keywords-Data storage, preservingconfidentiality, public audit ability, cryptographicprotocols, cloud computing.

I. INTRODUCTION

In step with the NIST definition, “Cloud computing is a model for enabling ubiquitous, easy, on-demandcommunity entry to a shared pool of configurable computing resources (e.g. Networks, servers, storage, purposes,and offerings) that can be quickly provisioned and launched with minimal management effort or service provider interplay” [12]. Making use of the cloud saves both users time and money. In Cloud computing, the term cloud is a metaphor forthe internet, so the phrase Cloud computing is defined as a sort of internet based computing, the place dataservices are delivered to an group’s desktops and instruments by way of the internet [4]. Cloud computing is verypromising for the information technology (IT) purposes; nonetheless, there are still some issues to be solved forpersonal clients and agencies to retailer information and deploy functions within the Cloud computing atmosphere. Dataprotection is without doubt one of the most massive obstacles to its adoption and it's followed by way of problems together with compliance,privacy, believe, and legal concerns. Therefore, probably the most major targets is to preserve safety and integrity of dataprotected in the cloud considering the fact that of the critical nature of Cloud computing and big amounts of tricky data it contains.

The clients issues for security should be rectified first to make cloud environment reliable, so that it helps theusers and manufacturer to undertake it on massive scale [4].The predominant issues in cloud datasecurity comprise data privacy, data protection, data availability, information place, and secure transmission. Threats, data loss, provider disruption, external malicious attacks, and multi tenancy problemsare the security challenges integrated in the cloud. Data integrity within the cloud method means maintaining the integrity ofprotected understanding. The data should now not be lost or modified through unauthorized clients. Cloud computing providers aretrusted to maintain data integrity and accuracy of data. Data confidentiality can also be most important side from user's factorof view because they store their confidential or personal data within the cloud. Authentication and access control proceduresare used to make certain data confidentiality. The data confidentiality could be addressed by means of increasing the cloud reliabilityand trustworthiness in Cloud computing. As a consequence protection, integrity, privacyand confidentiality of the protecteddataon the cloud will have to be regarded

and are predominant standards from user's point of view [4]. To reap all ofthese standards, new methods or methods should be developed and carried out.

Data auditing is presented in Cloud computing to care for sensitive data storage. Auditing is a process ofverification of client data which can also be carried out both by way of the client himself (data owner) or by means of a TPA. It helps tomaintain the integrity of data stored on the cloud. The verifier's position are labeled into two: first one is privateauditability, wherein simplest consumer or data proprietor is allowed to check the integrity of the stored data. No different individualhas the authority to impeach the server concerning the info. Nevertheless it tends to increases verification overhead of the client.Second is public auditability, which permits any client, not simply the client, to challenge the server and performs dataverification assess with the aid of TPA. The TPA is an entity which is used so that it might probably act on behalf of the purchaser.It has all of the vital data, capabilities, skills and reputable data which might be required to manage thework of integrity verification and it additionally reduces the overhead of the user. It's indispensable that TPA shouldefficiently audit the cloud data storage without inquiring for for the local replica of data. It should have zero advantageabout the datastored in the cloud server. It should no longer introduce any extra on-line burden to the cloud user [6].

The three network entities viz. The client, cloud server and TPA are present in the cloud environment. The clientstores data on the storage server offered by means of the cloud service provider (CSP). TPA keeps a examine on client's datavia periodically verifying integrity of data on-demand and notifies client if any variant or fault is found in client'sdata. Fig.1 indicates the cloud data storage architecture.

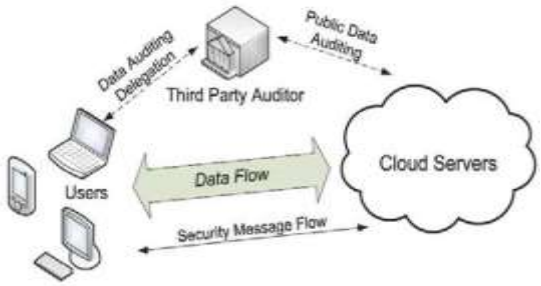

Fig. 1. Cloud Data Storage Architecture

II. RELATED WORKS

Cloud computing faces many problems on integrity and privacy of user's data stored in the cloud. Hence itrequires some secure and efficient methods which can ensure the integrity and privacy of data stored in the cloud.

Wang et al. [9] has proposed a privacy preserving public auditing protocol which makes use of an independent TPAto audit the data. It utilizes the public key based homomorphic linear authenticator (HLA) with random maskingtechniques. But this protocol is vulnerable to existential forgeries known as message attack from a malicious cloudserver and an outside attacker. To overcome this problem, Wang et al. [6] proposed a new improved scheme whichis more secure than the protocol proposed in [9]. It is a public auditing scheme with TPA, which performs dataauditing on behalf of users. It uses HLA which is constructed from Boneh-Lynn-Shacham short signature referred asBLS signatures. It also uses random masking for data hiding. For the sake of data binding, this new scheme involvescomputationally intensive pairing operation thus making it inefficient to use. This proposed scheme has beenimplemented practically on Amazon EC2 instance which demonstrates the fast performance of the design on boththe cloud and the auditor side. But the full-fledged implementation of this mechanism on commercial public cloudis not been tested. So it is difficult to expect it to robustly cope with very large scale data [7].

Wang et al. [10] proposed another protocol that supports both public auditing and data dynamics by using BLSbased HLA along with Merkle Hash Tree (MHT). It achieves the integrity of data but fails to provide confidentialityto the data stored on the cloud. Wang et al. [8] has also proposed a design to detect the modified blocks easily usinghomomorphic token pre-computation and later erasure coded technique is used to acquire the desired blocks fromdifferent servers. Solomon et al. [11] proposed protocol uses the same security level as Wang et al. [7] but withbetter efficiency. It generates a signature set which is an ordered collection of signatures on each file block, thusincurring computation and communication overhead. Meenakshi et al. [2] has proposed a protocol which uses TPAto audit the data of the users using Merkle Hash Tree algorithm. It supports data dynamics but fails to provideconfidentiality to the data stored in the cloud.

Tejaswani et al. [5] has achieved integrity of data using a Merkle hash tree by TPA and the confidentiality ofdata is achieved using RSA based cryptography algorithm whereas Jadhav et al. [3] have introduced an attackingmodule which continuously keeps track on data alteration in the cloud. The attacking module is a small code whichresides on cloud server. Confidentiality of stored data is achieved by encrypting the data using AES algorithm.

Arasu et al. [1] has proposed a method that uses the keyed Hash Message Authentication Code (HMAC) withhomomorphic tokens to enhance the security of TPA. It is a technique for verifying the integrity of a datatransmitted between two parties that agree on a shared secret key. HMAC's are based on a key that is sharedbetween the two parties, if either party's key is compromised, it will be possible for an attacker to create fraudmessages.

III. THE PROPOSED APPROACH

A confidentiality preserving scheme consists of fouralgorithms (KeyGen, SigGen, GenProof, VerifyProof).

- KeyGen: key generation algorithm that is run bythe user to setup the scheme
- **SigGen:**used by the user to generate verificationmetadata,which may consist of MAC, signatures or otherinformation used for auditing
- **GenProof:**run by the cloud server to generate aproof of data storage correctness
- VerifyProof:run by the TPA to audit the prooffrom the cloud server

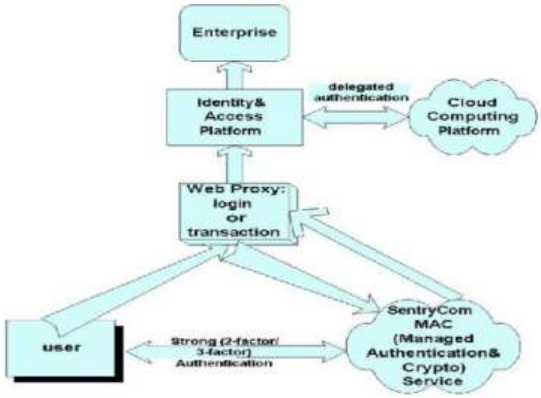

Fig. 2 Flow chart f proposed system

A. To achieve confidentiality preserving:

Homomorphic authenticators are unforgivableverification meta data generated from individual datablocks, which can be securely aggregated in such a wayto assure an auditor that a linear combination of datablocks is correctly computed by verifying only theaggregated authenticator. Overview to achieve privacypreserving public auditing, we propose to uniquelyintegrate the homomorphic authenticator with randommask technique. In our protocol, the linear combinationof sampled blocks in the server's response is maskedwith randomness generated by a pseudo random function(PRF) [8].

B. Support for Batch Auditing

With the establishment of privacy preserving publicauditing, the TPA may concurrently handle multipleauditing upon different users' delegation. The individualauditing of these tasks for the TPA can be tedious andvery inefficient. Given K auditing

delegations on Kdistinct data files from K different users, it is moreadvantageous for the TPA to batch these multiple taskstogether and audit at one time [9].

C. Data Dynamics

Hence, supporting data dynamics for privacypreserving public risk auditing is also of paramountimportance. Now we show how our main scheme can beadapted to build upon the existing work to support datadynamics, including block level operations ofmodification, deletion and insertion. We can adopt thistechnique in our design to achieve privacy-preservingpublic risk auditing with support of data dynamics [10].

To enable preserving confidentiality through publicauditing for Cloud data storage under the aforementionedmodel, our protocol design should achieve the followingsecurity and performance guarantees

 Public audit ability: To allow TPA to verifythe correctness of the cloud data on demand withoutretrieving a copy of the whole data or introducingadditional online burden to the cloud users.

 Storage correctness: to ensure that there existsno cheating cloud server that can pass the TPA'sauditwithout indeed storing users' data intact.

 Privacy-preserving: to ensure that the TPAcannot derive users' data content from the informationcollected during the auditing nprocess.

 Batch auditing: to enable TPA with secure andefficient auditing capability to cope with multipleauditing delegations from possibly large number ofdifferent users simultaneously.

 Lightweight: to allow TPA to perform auditingwith minimum communication and computationoverhead

IV. CONCLUSION

We advocate a confidentiality preserving through publicauditing approach for data storage security in CloudComputing. We utilize the homomorphic linearauthenticator and random overlaying to guarantee that theTPA would now not be taught any skills concerning the datacontent material stored on the cloud server in the course of the efficientauditing process, which no longer most effective eliminates the burden ofcloud user from the tedious and probably costlyauditing mission, but additionally alleviates the users' worry of theiroutsourced data leakage. Since TPA couldsimultaneously control more than one audit sessions fromspecial users for their outsourced data records, we furtherlengthen our privateness-maintaining public auditing protocolinto a multi-user environment, the place the TPA can participate inmore than one auditing duties in a batch method for highereffectivity. Vast analysis suggests that our schemes areprovably relaxed and highly efficient.

REFERENCES

[1] S Ezhil Arasu, B Gowri, and S Ananthi. Privacy-Preserving Public Auditing in cloud using HMAC Algorithm. International Journalof Recent Technology and Engineering (IJRTE) ISSN: 2277, 3878, 2013.

[2] IK Meenakshi and Sudha George. Cloud Server Storage Security using TPA. International Journal of Advanced Research in Computer Science & Technology (IJARCST) ISSN: 2347-9817, 2014.

[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 berkeleyview of cloud computing," University of California,Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.

[4] M. Arrington, "Gmail disaster: Reports of mass emaildeletions," Online athttp://www.techcrunch.com/2006/12/28/gmaildisasterreports-of-mass-email-deletions/, December2006.

[5] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors,"Online at http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closes-its-doors/, July 2008.

[6] Amazon.com, "Amazon s3 availability event: July 20,2008," Online at http://status.aws.amazon.com/s3-20080720.html, 2008.

[7] S. Wilson, "Appengine outage," Online athttp://www. cio-weblog.com/50226711/appengineoutage.php, June 2008.

[8] B. Krebs, "Payment Processor Breach May BeLargest Ever," Online athttp:/voices.washingtonpost.com/securityfix/2009/01/payment processor breach may b.html, Jan.2009.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L.Kissner, Z. Peterson, and D. Song, "Provable datapossession at untrusted stores," in Proc. of CCS'07,Alexandria, VA, October 2007, pp. 598–609.

[10] M. A. Shah, R. Swaminathan, and M. Baker,"Privacypreserving audit and extraction of digitalcontents," Cryptology ePrint Archive, Report 2008/186,2008.