International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Privacy in Cloud Storage Auditing with Random Masking Technique

Akavaram Swapna & Dr. M.Pandi M.E
[1]M.Tech (Computer Science & Engineering) Bharat Institute of Engg & Tech, Ibrahimpatnam(M) R.R Dist.
[2]Ph.D., Associate Professor, Dept of CSE Bharat Institute of Engg & Tech, Ibrahimpatnam(M) R.R Dist.

Abstract: *As cloud computing provides many relinquish characteristics to users like on demand self-service, storage, multi-tenancy, pay-as-you go and access data from shared pool of configurable computing resources without any burden.The Cloud server allowsconsumer to upload their data to a cloud. But a person's statistics are stored in the remote vicinity how users get the confirmationapproximately integrity of stored information. Sometimes Cloud provider vendors behave unfaithfully towards the cloud customers regardingthe status of their outsourced records. So we propose Public audit capacity that allows an external party, further to the userhimself, to confirm the integrity of outsourced records at the cloud. Indeed, they may doubtlessly display consumer data facts tothe auditors within the auditing technique ends in new vulnerabilities and additional online burden. However, maximum of theschemes do now not recall the privateness protection of users' data in opposition to outside auditors. So to securely introduce apowerful TPA, we suggest an aggregate homomorphic linear authenticator with a random protecting approach. In ourprotocol, the linear combination of sampled blocks in the server's reaction is masked with randomness generated by means of theserver using the pseudo-random feature (PRF). Also, we use the HLA that's based on the short signature scheme proposedby means of Boneh, Lynn, and Shacham (referred as BLS signature).*

Keywords-Cloud Computing, Data Integrity, Homomorphic Encryption, Homomorphic Linear Authentication (HLA),Zero Knowledge, Privacy Preserving, Public Auditing.

I. INTRODUCTION

Cloud computing has became a buzz word in today's era. It is amodel for enabling ubiquitous, convenient, on-demand networkaccess to a shared pool of configurable computing resources(e.g., networks, servers, storage, applications, and services) thatcan be rapidly provisioned and released with minimalmanagement effort or service provider interaction [2]. It hasbeen envisioned as the next-generation information technology(IT) architecture for enterprises, due to its long list ofunprecedented advantages in the IT history [1]. Users orenterprise store their data on cloud and it will be stored incentralized manner. They can get their outsourced data fromanywhere and cloud service providers (CSP) will charged thempay-as-you go. Users can upload huge amount of data on cloudwithout any burden of capacity and maintenance. As adisruptive technology with profound implications, CloudComputing is transforming the very nature of how businessesuse information technology. One fundamental aspect of thisparadigm shifting is that data is being centralized or outsourcedto the Cloud [1].

From users' perspective, including both individuals and ITenterprises, storing data remotely to the cloud in a flexible ondemand manner brings appealing benefits: relief of the burdenfor storage management, universal data access withindependent geographical locations, and avoidance of capitalexpenditure on hardware, software, and personnelmaintenances, etc [5]. As cloud computing provides manyadvantages but it also brings security threads towards user'soutsourced data. As users no longer physically possess thestorage of their data, traditional cryptographic primitives forthe purpose of data security protection cannot be directlyadopted [6]. Hence due these many attacks on outsourced datais possible. As a result, the correctness of the data in the cloudis being put at risk due to the following reasons. First of all,although the infrastructures under the cloud are much morepowerful and reliable than personal computing devices, theyare still facing the broad range of both internal and externalthreats for data integrity. Even though, there do exist various

motivations for CSP to behave unfaithfully towards the cloudusers regarding the status of their outsourced data. Forexamples, CSP might reclaim storage for monetary reasons bydiscarding data that has not been or is rarely accessed, or evenhide data loss incidents so as to maintain a reputation willeliminate any data.To avoid this problem, we introduce an effective third partyauditor (TPA) to audit the user's outsourced data when needed[1]. TPA is the third party auditor who will audit the data ofdata owner or client so that it will let off the burden ofmanagement of data of data owner. TPA eliminates theinvolvement of the client through the auditing of whether hisdata stored in the cloud are indeed intact, which can beimportant in achieving economies of scale for CloudComputing. The released audit report would not only helpowners to evaluate the risk of their subscribed cloud dataservices, but also be useful for the cloud service provider toimprove their cloud based service platform. This public auditorwill help the data owner that his data are safe on cloud [3].Public auditability allows anyone, not just the client (dataowner), to challenge the cloud server for the correctness of datastorage while keeping no private information. Hence TPA willhelp data owner to make sure that his data are safe in the cloudand management of data will be easy and less burdening to dataowner.

II. RELATED WORK

Portions of the work presented in this paper have previously appeared in [10]. TPA is stateless i.e. no need to maintain or updatethe state information of audit phase. Public key based homomorphic linear authentication with random masking technique is usedto achieve privacy preserving public auditing. TPA checks the integrity of the outsourced data stored on a cloud without accessingactual contents. Existing research work of proof of retrievability (PoR) or Proofs of Data Possession (PDP) technique doesn'tconsider data privacy problem. PDP scheme first proposed by Ateniese et al. used to detect large amount corruption in outsourceddata [6].

It uses RSA based Homomorphic authentication for auditing the cloud data and randomly sampling a few blocks of files. ASecond technique proposed by Juels as Proofs of retrievability (PoR) allows user to retrieve files without any data loss orcorruptions [15]. It uses spot checking & error correcting codes are used to ensure both "Possession" and "Retrievability". Toachieve Zero knowledge privacy, researcher proposed Aggregatable Signature Based Broadcast (ASBB). It providescompleteness, privacy and soundness. It uses 3 algorithms as Keygen, Gentag and Audit.

III. PROPOSED WORK

Random masking: Public audit ability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data.However, most of these schemes [6], [7], [8] do not consider the privacy protection of users' data against external To fully ensurethe data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enablepublic auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to audit the outsourced data when needed public key based homomorphic linear authenticator (or HLA for short) [6], [7], [8], which enables TPA to perform the auditingwithout demanding the local copy of data and thus drastically reduces the communication and computation overhead as comparedto the straightforward data auditing approaches. By integrating the HLA with random masking, our protocol guarantees that theTPA could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process. Theaggregation and algebraic properties of the authenticator further benefit our design for the batch auditing.

Privacy-Preserving Public Auditing Scheme:

To achieve privacy-preserving public auditing, we propose uniquely integrate the homomorphic linear authenticator with randommasking technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomnessgenerated by the server based on pseudo random function (PRF).With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations andtherefore cannot derive the user's data content, no matter how many linear combinations of the same set of file blocks can becollected. On the other hand, the correctness validation of the block authenticator pairs can still be carried out in a new way.Our design makes use of a public key based HLA, to equip the auditing protocol with public audit

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

ability. Specifically, we use theHLA proposed in [1], which is based on the short signature scheme proposed by Boneh, Lynn and Shacham (referred as BLSsignature).

Though HLA with random masking solves the problem of privacy-preserving, it increases the burden of maintenance andcalculation of masking information on user as well as on TPA.

Algorithm 1: generates an asymmetric key pair (x, v) ∈ Zn * Gn with private key x and public key v	**KeyGen** Data: generator g2 for G2, prime number p Result: private key x ∈ Zn, public key v ∈ G2 Choose random x ∈ Zn V ← $g2^x$ Return (x, v)
Algorithm 2: This is used when signing a message M with the private key x. This algorithm requires a hash function H that can hash the message to an element h ∈ G1. we will assume that H is random hash function	**SigGen** Data: private key x ∈ Zn, message M ∈ {0,1}* Result: signature σ ∈ G1 h ← H(M) ∈ G1 σ ← h^x Return σ
Algorithm 3: verify the signature with public key	Data: public key v ∈ G2,message M ∈ {0,1}*, signature σ ∈ G1 Result: boolean value h ← H(M) ∈ G1 Return Test ((g2, v, h, σ)

Fig 1. Implementation of BLS signature

The System and Threat Model [10]

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server / cloud serviceprovider.

Cloud user (CU): is a person who stores large amount of data or files on a cloud server.Cloud server (CS) & Cloud service provider: is a place where we are storing cloud data and that data will be managed by thecloud service provider.

Third party auditors (TPA): TPA will do the auditing on users request for storage correctness and integrity of data.

Zero knowledge: TPA will audit the users' data without seeing the contents. It uses public key based homomorphic linearauthentication (HLA) [6], [7] which allows TPA to perform auditing without requesting for user data.

Design Goals

1) Public audit ability: Allows third party auditor to check data correctness without accessing local data.

2) Storage Correctness: The data stored on a cloud is as it. No data modification is done.

3) Privacy preserving: TPA can't read the users' data during the auditing phase.

4) Batch Auditing: Multiple users auditing request is handled simultaneously.

5)Light Weight: Less communication and computation overhead during the auditing phase.

fig.2cloud data storage architecture

Algorithms involved: There are two phases, setup and audit.

Setup

KeyGen: is a key generation algorithm that is run by the user to setup the scheme.

SigGen: is used by the user to generate verification metadata, which may consist of MAC, signatures, or other relatedinformation that will be used for auditing.

Audit

GenProof: is run by the cloud server to generate a proof of data storage correctness.

VerifyProof: is run by the TPA to audit the proof from the cloud server.

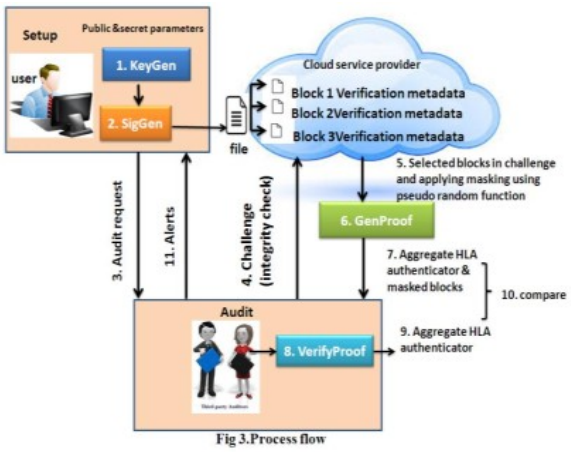

fig.3 process flow

Batch Auditing: It also supports batch auditing through which efficiency is improved. It allows TPA to perform multiple auditing tasksimultaneously and it reduces communication and computation cost. Through this scheme, we can identify invalid response. Ituses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will befaster.

Data Dynamics: It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation ofinsertion, deletion and modification. Author of [6] proposed scheme which support simultaneous public audability and datadynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data for block tag authentication.

IV. CONCLUSION

In this paper, we studied all techniques used for a privateness-maintaining public auditing machine for records garage security inCloud Computing. As TPA will tell approximately data integrity andnot offering a genuine idea of how information is misplaced.In this paper, we suggest a privacy-keeping public auditing for the outsourced statistics integrity in safety in Cloud Computing.We make use of the homomorphic linear authenticator and random overlaying to guarantee that the TPA might not analyze any knowledgeapproximately the data content material stored at the cloud server at some stage in the efficient auditing system, which not only eliminates the load ofcloud user from the tedious and likely costly auditing mission, however also alleviates the customers' fear of their outsourced recordsleakage.

REFERENCES

[1] Cong Wang, Sherman S.-M, Qian Wang, KuiRen, WenjingLou, "Privacy-Preserving Public Auditing for Secure CloudStorage", IEEE Trans. on Cloud Computing, March-2013

[2] P. Mell and T. Grance, "Draft NIST working definition ofcloud computing," Referenced on Nov. 22rd, 2014 Online athttp://csrc.nist.gov/groups/SNS/cloud-computing/index. html,2014.

[3] P. Selvigrija, D. Sumithra," Public Auditing & AutomaticProtocol Blocking with 3-D Password Authentication forSecure Cloud Storage", D. Sumithra et al, International Journalof Computer Science and Mobile Applications,Vol.2 Issue. 1,January- 2014, pg. 1-8

[4] Cong Wang, Qian Wang, and KuiRen "Ensuring DataStorage Security in Cloud Computing" Email: {cwang, qwang,kren}@ece.iit.edu.-pg:2,3

[5] 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 cloudcomputing," University of California, Berkeley, Tech. Rep

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

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloudcomputing," in Proc. of ESORICS'09, volume 5789 of LNCS. Springer-Verlag, Sep. 2009, pp. 355–370.

[8] H. Shacham and B. Waters, "Compact proofs of retrievability," in Proc. of Asiacrypt 2008, vol. 5350, Dec 2008, pp. 90–107.

[9] 104th United States Congress, "Health Insurance Portability and Accountability Act of 1996 (HIPPA)," Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.

[10] Cong Wang, Student Member, IEEE, Sherman S.-M. Chow, Qian Wang, Student Member, IEEE, KuiRen, Member, IEEE,and Wenjing Lou, Member, IEEE" Privacy-Preserving Public Auditing for Secure Cloud Storage".

[11] Rana M Pir, Lecturer, Leading university, Sylhet Bangladesh © 2014 IJEDR | Volume 2, Issue 4 | ISSN: 2321-9939,"Cloud Storage Security Using Encryption and Third-Party Storage Auditing Service".

[12] Maha TEBAA, Saïd EL HAJJI, Abdellatif EL GHAZI, Proceedings of the World Congress on

Engineering 2012 Vol IWCE 2012, July 4 - 6, 2012, London, U.K," Homomorphic Encryption Applied to the Cloud Computing Security".

[13] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11thUSENIXWorkshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.

[14]CMerkle, "Protocols for public key cryptosystems," in Proc.of IEEE Symposium on Security and Privacy, Los Alamitos, CA,USA, 1980.

[15] A. Juels and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October2007, pp. 584–597.