ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

Enabling Data Security in Cloud Computing Using Third Party Auditing and Encryption Services

Amal Jose, M.Sambath, S.Ravi

PG Scholar, Department of Computer Science & Engineering , Hindustan University, Chennai, India

Assistant Professor, Department of Computer Science & Engineering , Hindustan University, Chennai, India

Assistant Professor, Department of Computer Science & Engineering , Hindustan University, Chennai, India

ABSTRACT: Cloud Computing is the next-generation architecture of computing. It moves the software and databases to the large data centers, where the management of the data and services can face a number of challenges. By outsourcing data, users are free from the burden of local data storage and maintenance. However, since the users does not have physical possession of large size of outsourced data makes the data integrity protection in cloud computing a very challenging task for users. So public auditability for cloud data storage security is important where users can entrust an external audit party to check the integrity of outsources data when needed. To securely introduce an effective third party auditor (TPA), the following requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without the local copy of data, and should not introduce any additional on-line burden to the cloud user; 2) The third party auditing process should preserve user data privacy**.**

KEYWORDS*:* public auditing, cloud service provider, thirdpartyauditng

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Because of number of advantages it offers cloud computing is looked upon as the architecture for next generation enterprises. Some of the advantages are on demand self service, usage based pricing, rapid resource elasticity, location independent resource pooling etc.Users have a number of appealing benefits such as universal data access, relief of burden of storage management, avoidance of capital expenditure on hardware ,software etc.Although cloud computing has a lot of advantages it also brings security threats towards user's outsourced data. Many times correctness of data is put under risk since cloud service providers are separate administrative entities. The main threats to data are mainly due to the reasons described below. First of all there are internal and external threats even though cloud infrastructures are powerful and reliable. Secondly there are chances that cloud service provider behave unfaithfully towards outsourced data to cloud users. Since the users no longer have the possession of outsourced data it is necessary that the data is audited to ensure data integrity.Inorder to ensure data integrity and save cloud users computation resources it is of critical importance to enable public auditing service for cloud data storage so that users can resort to a third party auditor to audit outsourced data. Third party auditor provide easier and affordable way for users to ensure storage correctness and the audit result from third party auditor will also be beneficial for cloud service provider to improve cloud based service platform. By using public auditing services users can avoid risk and gain trust in cloud.To ensure remotely stored data integrity public auditability has been proposed which allow external party to audit data but most of the schemes do not consider privacy protection of user's

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

data. Here a privacy preserving public auditing protocol is proposed which enable an external auditor to audit data without learning the content. Batch auditing and data dynamics are also allowed. Public key based homomorphic linear authenticator which enables third party auditor to perform auditing without demanding local copy of data .By integrating homomorphic linear authenticator with random masking our protocol guarantees that third party auditor could not learn any knowledge about data content stored in cloud server during auditing processes.

II RELATED WORK

Public auditability in provable data possession are first considered by Ateniese for possession of data files on untrusted storages. They utilize the RSA-based homomorphic linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file. However, among their two proposed schemes, the one with public auditability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the external auditor. Juels et al. [11] describe a "proof of retrievability"(PoR) model, where spot-checking and error-correcting codes are used to ensure both "possession" and "retrievability"of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Later, Bowers et al. [18] proposean improved framework for POR protocols that generalizes Juels' work. Shacham andWaters [13] design an improved PoR scheme built from BLS signatures [19] with proofs of security in the security model defined in [11]. Similar to the construction in [9], they use publicly verifiable homomorphic linear authenticators that are built from provably secure BLS signatures. Based on Comparison on auditing time between batch and individual auditing, when _-fraction of 256 responses are invalid: Per task auditing time denotes the total auditing time divided by the number of tasks. the elegant BLS construction, a compact and public verifiable scheme is obtained. Again, their approach is not privacy preserving due to the same reason as [9]. Shah et al. [15], [10]propose introducing a TPA to keep online storage honest by first encrypting the data then sending a number of precomputed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies the integrity of the data file and the server's possession of a previously committed decryption key. This scheme only works for encrypted files, requires the auditor to maintain state, and suffers from bounded usage, which potentially brings in online burden to users when the keyed hashes are used up. Dynamic data have also attracted attentions in the recent literature on efficiently providing the integrity guarantee of remotely stored data

III PROBLEM STATEMENT

There are mainly four different entities involved that are called as cloud user, cloud service provider, cloud server and third party auditor. Cloud user have huge amount of data that has to be stored in the cloud. Cloud server is managed by cloud service provider to provide data storage service and has significant storage space and computational resources. Third party auditor is used to assess cloud storage service reliability on behalf of user upon request. User depend on cloud service provider to store data since user no longer possess data locally user need to ensure that data are being correctly stored and maintained. User's data may face both internal and external attack at cloud server.Inorder to save computation resource as well as online burden of periodic storage correctness verification cloud users resort to a third party auditor to ensure storage integrity of outsourced data. Public auditability, storage correctness, privacy preserving, batch auditing and lightweight processing are the design goals to be achieved.

IV PROPOSED SCHEME

Public auditing scheme is discussed here. Two straight forward scheme and their demerits are also discussed. Then we present the main scheme which support batch auditing and data dynamics. Public auditing scheme provide complete outsourcing solution of data. There are mainly four algorithms in public auditing scheme. There are mainly four algorithm for public auditing keygen,siggen,genproof,verifyproof.Keygen is a keygeneration algorithm,sigen is used to generate

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

verification metadata,genproof is used to generate proof of data storage correctness while verifyproof is run by third party auditor to audit the proof. Setup and audit are the two phases of running a public auditing system. In set up phase user initializes public and secret parameters of the system by executing keygen and preprocess the data file F by using siggen to generate the verification metadata. User then stores the data file F and the verification metadata at the cloud server and deletes it's local copy. In audit phase an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of audit.

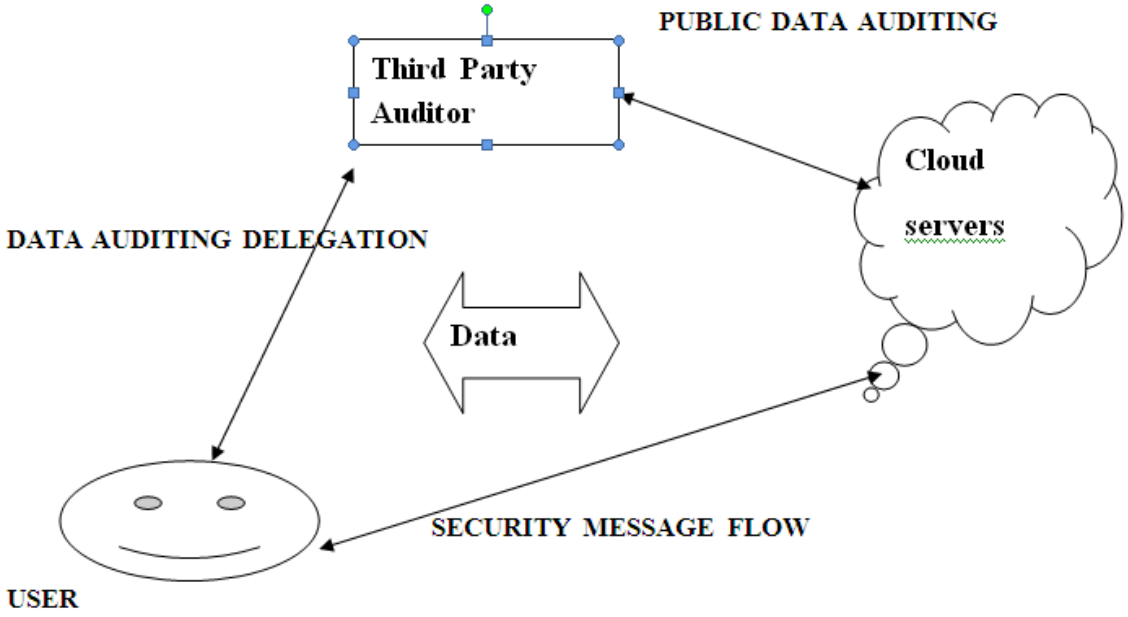

Fig 1.1: The basic system architecture is given here.

A. PRIVACY PRESERVING PUBLIC AUDUTING SCHEME

Homomorphic linear authenticator with random masking technique is used to achieve privacy preserving public auditing. The linear combination of sampled blocks in the server's response is masked with randomness generated by the server. Even though many linear combinations of the same set of file blocks can be collected by using random masking, the third party auditor no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content. The design makes use of public key based homomorphic linear authenticator to equip auditing protocol with public auditability.

Let G_1, G_2 and G_t are multiplicative cyclic groups of prime order p and e: $G1_x G_2 \rightarrow G_T$ be a bilinear map and let g be a generator of G_2. H(.) is a secure map-to-point hash function:$\{0,1\}\rightarrow G_1$, which maps strings uniformly to G_1. Another hash function h(.) : $G_t \rightarrow Z_P$ maps group element of GT uniformly to Zp.

Setup Phase: The cloud user runs KeyGen to generate the public and secret parameters. Specifically, the user chooses a random signing key pair (spk,ssk), a random x ←Zp, a random element u GG1, and computes v gx.The secret parameter is

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

sk=(x,ssk) and the public parameters are pk=(spk,v,g,u,e(u,v)).Given a data file F ={Mi}, the user runs SigGen to compute authenticator GG1 for each i.Here, Wi = name || i and name is chosen by the user uniformly at random from Zp as the identifier of file F.The last part of SigGen is for ensuring the integrity of the unique file identifier name.
Audit Phase: The TPA first retrieves the file tag t. With respect to the mechanism we describe in the Setup phase, the TPA verifies the signature SSigssk(name) via spk, and quits by emitting FALSE if the verification fails. Otherwise, the TPA recovers name. Now it comes to the "core" part of the auditing process. To generate the challenge message for the audit "chal," the TPA picks a random c-element subset I = $\{s_1,\ldots.s_c\}$ of set[1,n]. For each element i€I, the TPA also chooses a random value v_i (of bit length that can be shorter than |p|, as explained in [13]). The message "chal" specifies the positions of the blocks required to be checked. The TPA sends chal = $\{(i,v_i)\}$ to the server. Upon receiving challenge chal= $\{(i,V_i)\}$,the server runs GenProof to generate a response proof of data storage correctness. Specifically, the server chooses a random element r ←Zp, and calculates R = $e(u,v)^r$ G€T . Finally the third party auditor runs the verify proof to validate it by checking verification equation.

B.PROPERTIES OF PROTOCOL

Public auditability is achieved in the protocol and it does not pose any potential online burden on users. It supports privacy of user data by employing a random masking and linear combination of data blocks. Underlying protocol ensures storage correctness and HLA helps to achieve the constant communication overhead for server's response during audit.O (1) is the probability to detect server misbehavior if the server is missing a fraction of data. Given the huge volume of data outsourced in the cloud, checking a portion of the data file is more affordable and practical for both the TPA and the cloud server than checking all the data, as long as the sampling strategies provides high-probability assurance.

C.SUPPORT FOR BATCH AUDUTING

Third party auditor can concurrently handle multiple auditing from different users delegation and thus supports batch auditing. If TPA audit the tasks individually it will be tedious and inefficient.
It is always advantageous for the TPA to batch multiple batches together and audit at one time. By aggregating K verification equations into single one a secure batch auditing protocol for simultaneous auditing of multiple tasks is obtained. There are two phase setup phase and audit phase. In setup phase basically; the users just perform Setup independently. Suppose there are K users in the system, and each user k has a data file Fk =(mk,1,……..,mk,n) to be outsourced to the cloud server, where k € (1; . . .;K). For simplicity, we assume each file Fk has the same number of n blocks. For a particular user k, denote his/her secret key as (xk; sskk), and the corresponding public parameter (spkk,vk,g,uk,e(uk,vk)) where vk = gxk . Similar to the single user case, each user k has already randomly chosen a different name k € Zp for his/her file Fk, and has correctly generated the corresponding file tag tk .Finally, each user k sends file Fk, set of authenticators φk, and tag tk to the server and deletes them from local storage. In audit phase TPA retrieves and verifies file tag tk first for each user k.If verification fails TPA quits by emitting false otherwise TPA recovers $name_k$ and sends the audit challenge to the server for auditing data files of all K users.Effiecency improvement is the main advantage of batch auditing. It allows TPA to perform multiple tasks simultaneously but also greatly reduces computation cost on TPA side.Aggreagating K verification equations into one saves a considerable amount of auditing time.

D.SUPPORT FOR DATA DYNAMICS

Supporting data dynamics for privacy preserving public auditing is very important, outsourced data not only be accessed but also updated frequently by users for various application purposes. Data dynamics is achieved by replacing index information i with mi in computation of block authenticators and using merkle hash tree. As a result, the authenticator for each block is changed. We can adopt this technique in our design to achieve privacy-preserving public auditing with support of data dynamics. Specifically, in the Setup phase, the user has to generate and send the tree root TPA as additional

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

metadata. In the Audit phase, the server's response should also include corresponding auxiliary authentication information aux in the MHT. Upon receiving the response, TPA should first use TRMHT and aux to authenticate computed by the server. The Batch Auditing Protocol these changes does not interfere with the proposed random masking technique, so data privacy is still preserved. To support data dynamics, each data update would require the user to generate a new tree root TRMHT, which is later sent to TPA as the new metadata for storage auditing task. The details of handling dynamic operations are similar and thus omitted.

V EVALUATION

The evaluation includes security analysis and performance analysis. Security of the proposed scheme is done by analyzing storage correctness and privacy preserving property.Seurity analysis include storage correctness gurantee,privacy preserving gurantee,batch auditing gurantee,sorting out invalid responses. Storage correctness guarantee ensures that if cloud server passes the audit phase it must indeed possess the specified data intact as it is. The TPA cannot derive user's data from information during auditing; this is called as privacy preserving guarantee. The efficiency analysis on the batch auditing, is done by considering only the total number of pairing operations. However, on the practical side, there are additional less expensive operations required for batching, such as modular exponentiations and multiplications. Thus, whether the benefits of removing pairings significantly outweighs these additional operations remains to be verified. To get a complete view of batching efficiency, we conduct a timed batch auditing test, where the number of auditing tasks is increased from 1 to approximately 200 with intervals of 8.The performance of the corresponding non batched (individual) auditing is provided as a baseline for the measurement. It can be shown that compared to individual auditing, batch auditing indeed helps reducing the TPA's computation cost, as more than 15 percent of per task auditing time is saved.

.

VI CONCLUSION

In this paper secure cloud storage privacy preserving public auditing system is proposed. Homomorphic linear authenticator and random masking is used 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 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. The future extension is full fledged implementation of mechanism on commercial public cloud which can handle large amount of data and thus enable users to outsource the data more confidently.

REFERENCES

[1]P.MellandT.Grance,"DraftNISTWorkingDefinitionofCloudComputing,"http://csrc.nist.gov/groups/SNS/cloudcomputing/index.html, June 2009.
[2] 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.WANG ET AL.: PRIVACY-PRESERVING PUBLIC AUDITING FOR SECURE CLOUD STORAGE 373
[3]CloudSecurityAlliance,"TopThreatstoCloudComputing,"http://www.cloudsecurityalliance.org, 2010.
[4]M.Arrington,"GmailDisaster:ReportsofMassEmailDeletions,"http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.
[5]J.Kincaid,"MediaMax/TheLinkupClosesItsDoors,"http://www.techcrunch.com/2008/07/10/mediamaxthelinkup-closesits-doors/, July 2008.
[6] Amazon.com, "Amazon s3 AvailabilityEvent:July20,2008,"http://status.aws.amazon.com/s3-20080720.html, July 2008.
[7] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at UntrustedStores," Proc. 14th ACM Conf. Computer and Comm. Se
curity(CCS '07), pp. 598-609, 2007.
[8] M.A. Shah, R. Swaminathan, and M. Baker, "Privacy-PreservingAudit and Extraction of Digital Contents," Cryptology ePrintArchive, Report 2008/186, 2008.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 2, February 2014

[9] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievabilityfor Large Files," Proc. ACM Conf. Computer and Comm. Security(CCS '07), pp. 584-597, Oct. 2007.
[10] Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in CloudComputing," http://www.cloudsecurityalliance.org, 2009.
[11] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. Int'l Conf. Theory and Application of Cryptology and InformationSecurity: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107,Dec. 2008.
[12] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly AuditableSecure Cloud Data Storage Services," IEEE Network Magazine,vol. 24, no. 4, pp. 19-24, July/Aug. 2010.
[13] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditingto Keep Online Storage Services Honest," Proc. 11th USENIXWorkshop 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.
[14] R. Curtmola, O. Khan, and R. Burns, "Robust Remote DataChecking," Proc. Fourth ACM Int'l Workshop Storage Security andSurvivability (StorageSS '08), pp. 63-68, 2008.
[15] K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability:TheoryandImplementation," Proc. ACM Workshop Cloud ComputingSecurity (CCSW '09), pp. 43-54, 2009.
[16] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from theWeil Pairing," J. Cryptology, vol. 17, no. 4, pp. 297-319, 2004.
[17] A.L. Ferrara, M. Green, S. Hohenberger, and M. Pedersen,"Practical Short Signature Batch Verification," Proc. Cryptographers'Track at the RSA Conf. 2009 on Topics in Cryptology (CT-RSA),pp. 309-324, 2009.
[18] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. ACM Conf. Computerand Comm. Security (CCS '09), pp. 213-222, 2009.