International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2013): 4.438

Privacy Preserving Auditing For Cloud Storage

Nandini P. Wasnik[1], Mahip M.Bartere[2]

[1] M.E. final year CSE, GHRCEM, Amravati, India

[2] Assistant Professor, Department of Computer Science and Engineering, GHRCEM, Amravati, India

Abstract: ***Cloud storage provides users to easily store their data and enjoy the good quality of cloud applications which is need not install in any local hardware and software system. such a service is also gives users control of their outsourced data, which also provides control to the security problems regarding the correctness of the data storage in the cloud. The main goal of cloud computing the data protection, secure and the process data stored under the property of users. As the data which is stored at the remote server how the cloud users will get the confirmation about data which are stored. That's why cloud storage should have some technique and mechanism which will specify correctness of data storage and integrity of data stored on cloud. For that users can resort to a third-party auditor (TPA) which is to check the integrity of outsourced data ,TPA should be able to efficiently audit the data storage on cloud . To introduce an effective and secure TPA, the auditing process should bring in no new vulnerabilities toward user data privacy, and no online additional burden to user. In this paper, we propose system for a cloud storage which is the secure and supporting privacy-preserving public auditing. The proposed system perform for multiple users auditing process simultaneously and efficiently.***

Keywords: :. *Data storage, privacy preserving, public audit ability, cloud computing, delegation, batch verification.*

1. Introduction

In the history of IT, cloud computing has brought unprecedented benefits to the computing world. It has made it possible to have a different computing model that does not suffer with scarcity of resources. Cloud computing enables to share computing resources without the need for investment in pay as you use fashion. Cloud service providers such as Microsoft, Oracle, Amazon, Google etc. are able to provide huge clouds which are nothing but computing resources that are provided on demand through Internet(1).The way on that IT infrastructure has been used; is changing with the emergence of cloud computing. One important part of cloud computing is that data which is stored in a centralized server is linked to data centre of cloud . The storage and other services provided by cloud can be utilized by individuals and organizations alike without the need for capital investment. For organizations and individuals cloud provides very useful advantages as they are relieved from storage management, investment, and maintenance. (2).

Along with the advantages, it also has challenges in terms of security threats. This is because the users' data is stored in a remote server which is considered "untrusted". Users are losing control over their data and the storage facilities are under control of cloud service providers. Thus the correctness or integrity of the data is questioned. The cloud data storage might be subjected to internal and external threats.(3) Security problems surfaced in cloud computing were known to the (4). On the other hand CSPs might have intentions to be unfair towards cloud users and their outsourced data besides hiding security flaws in their storage infrastructure (7)To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may employ to an independent third-party auditor (TPA) to audit the outsourced data when needed. The TPA, who has expertise capabilities that users do not have, it is periodically check the integrity of all data which are stored in the cloud instead 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 it help users to evaluate the risk of their subscribed services of cloud data, the audit result from TPA would also be important for the cloud service providers to improve their cloud-based service platform, and even serve for independent arbitration purposes (5). In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established; where users will need ways to assess risk and gain trust in the cloud. Recently, the notion of public audit ability has been proposed in the context of ensuring remotely stored data integrity under different system and security models . Public auditability allows an external party, in addition to the user himself, to verify the correctness of stored data. However, most of these schemes do not consider the privacy protection of users' data against external auditors. Indeed, they may potentially leak user's data to external auditors, this drawback greatly affects the security in cloud computing. For the purpose of protecting data privacy, the users, who own the data , rely on TPA just for the storage security of their data, toward their data security(6).The first ones to support privacy-preserving public auditing in cloud computing, with a focus on data storage. As the individual auditing of these growing tasks can be tedious, a natural demand is then how to enable the TPA to efficiently perform multiple auditing tasks in a batch manner, i.e., simultaneously.To address these problems, utilizes the technique of public key-based homomorphic linear authenticator , which enables TPA to perform the auditing without demanding the local copy of data and thus drastically reduces the communication and computation overhead as compared to the straightforward data auditing approaches. By integrating the HLA with random masking, our protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server (CS) during the efficient auditing process. The aggregation and algebraic properties of the authenticator further benefit our design for the batch auditing.

2. Proposed Method

The proposed system contain following three entities, as show in Fig. 1: cloud user (U), which contain the amount of data files which are stored in the cloud; cloud server (CS), managed by the cloud service provider (CSP) for providing data storage service and has significant storage space as well as computation resources; third party auditor (TPA), who has expertise and capabilities that cloud users does not have and TPA trustfull for assessing the reliability of cloud storage upon request of the user . Users can rely on the CS for cloud data storage and maintenance, also dynamically interact with the CS for accessing and update the data stored for purpose of various application . To save the computation resource as well as the online limitations ,the users of cloud may resort to TPA for ensuring their outsourced data storage integrity, which hoping to keep their data private from TPA. It is most importance to enable public auditing service for cloud data storage, so that users resort to an third party auditor (TPA) which is independent to audit the outsourced data when ever needed. The TPA, which make it a much more easier and efficient way for the users to ensure their storage correctness in the cloud. Moreover, for evaluate the risk of the cloud user the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud based service platform, and even serve for independent negotiation purposes.

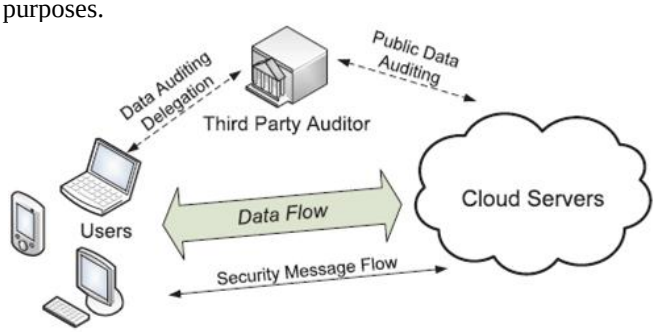

Figure : System architecture

3. System Modules

1. System Module
2. Privacy-Preserving Public Auditing Module
3. Batch Auditing Module
4. Data Dynamics Module

3.1 System Module

User: users, who have data to be put in the cloud and also for cloud data computation, which is both individual consumers and organizations. Cloud Service Provider (CSP): CSP, who has resources capabilities and expertise in building organised distributed cloud storage servers, and operates Cloud Computing systems. Third Party Auditor (TPA): is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

3.2 Privacy-Preserving Public Auditing Module

Overview to achieve privacy-preserving public auditing, the propose system has to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

The proposed system consist of two phases:

- Setup Phase
- Audit Phase

3.3 Batch Auditing Module

With the implementation of privacy-preserving public auditing in Cloud Computing, TPA may handle multiple auditing delegations upon different users' requests. Batch auditing not only allows TPA to perform the multiple auditing tasks of different user simultaneously, but also it greatly decreases the computation cost on the TPA side.

3.4 Data Dynamics Module

Support data dynamics, including block level operations of modification, deletion and insertion. We can take this technique in our proposed system design to achieve privacy-preserving public risk auditing with support of data dynamics.

4. Proposed System Framework

A public auditing scheme consists of four algorithms Key Gen is a key generation algorithm which is run by the user. Sig Gen is used by the cloud user to generate verification metadata, and also other related information that will be used for auditing purpose.

Gen Proof is run by the cloud server to generate a proof of data storage. Verify Proof is run by the TPA to audit the proof from the cloud server. The public auditing system consists of two phases, Setup and Audit:

- **Setup:** The user first initializes the public and secret parameters of the proposed system by executing KeyGen, and then pre-processes the data file F by using Sig Gen which generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server.
- **Audit:** The TPA issues an audit message to the cloud server which make confirm that the cloud server has retained the data file F properly at the time of the audit By executing GenProof ,the cloud server will derive a response message from a function of the data stored file F and its verification metadata. Via Verify Proof the TPA verify verification proof .The proposed system assumes the TPA is stateless, which is a desirable property achieved by proposed system.

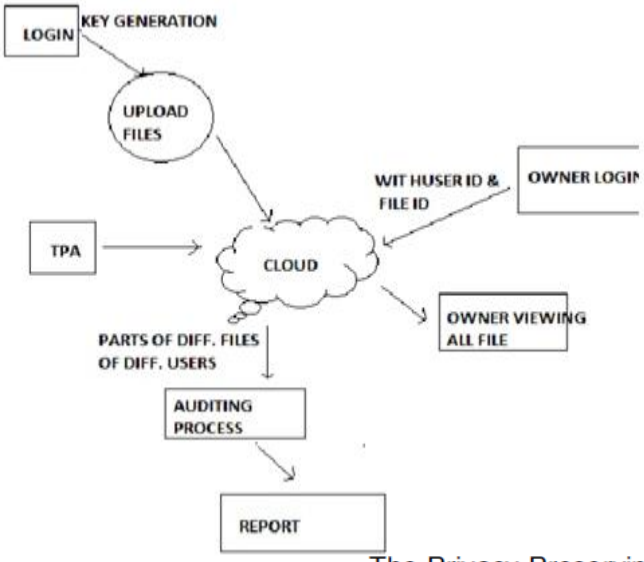

Figure: Flow diagram

5. Privacy-Preserving Public Auditing Scheme

Here we propose to uniquely integrate the homomorphic linear authenticator with random masking technique. In our protocol, the linear combination of data file of sampled blocks in the server's response is masked with randomness generated by the server. With random masking, the TPA 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, no matter how many linear combinations of the same set of file blocks can be collected.

The Privacy-Preserving Public Auditing Protocol

TPA		Cloud Server
1. Retrieve file tag t, verify its signature, and quit if fail;		
2. Generate a random challenge $chal = \{(i, \nu_i)\}_{i \in I}$;	$\xrightarrow[\text{challenge request } chal]{\{(i,\nu_i)\}_{i\in I}}$	3. Compute $\mu' = \sum_{i \in I} \nu_i m_i$, and $\sigma = \prod_{i \in I} \sigma_i^{\nu_i}$; 4. Randomly pick $r \leftarrow \mathbb{Z}_p$, and $R = e(u, v)^r$ and $\gamma = h(R)$;
	$\xleftarrow[\text{storage correctness proof}]{\{\mu,\sigma,R\}}$	5. Compute $\mu = r + \gamma\mu' \mod p$;
6. Compute $\gamma = h(R)$, and then verify $\{\mu, \sigma, R\}$ via Equation 1.		

The client's public key and private key are generated by invoking KeyGen(·). By running SigGen(·), the data file F is pre-processed, and the homomorphic authenticators together with metadata are produced. KeyGen(1k). The client generates a random signing key pair (spk, ssk). Choose a random α ← Zp and compute v ← gα. The secret key is sk = (α, ssk) and the public key is pk = (v, spk).
SigGen(sk, F). Given F = (m1,m2 . . . ,mn), the client chooses a random element u ← G. Let t = name‖n‖u‖SSigssk(name‖n‖u) be the file tag for F.

Then the client computes signature σi for each block mi (i = 1, 2, . . . , n) as σi ← (H(mi) · umi)α. Denote the set of signatures by _ = {σi}, 1 ≤ i ≤ n. The client then generates a root R based on the construction (pk, sk) ← KeyGen(1k). *This probabilistic algorithm is run by the client. It takes as input security parameter* 1k, *and returns public key* pk *and private key* sk.(_, sigsk(H(R))) ← SigGen(sk, F). *This algorithm is run by the client. It takes as input private key* sk *and a file* F *which is an ordered collection of blocks* {mi}, *and outputs the signature set* _, *which is an ordered collection of signatures* {σi} *on* {mi}. *It also outputs metadata-the signature* sigsk(H(R)) *of the root* R *of a Merkle hash tree. In our construction, the leaf nodes of the hashes of* H(mi). (P) ← GenProof(F,_, chal). *This algorithm is run by the server. It takes as input a file* F, *its signatures* _, *and a challenge* chal. *It outputs a data integrity proof* P *for the blocks specified by* chal.

6. Conclusions

Proposed system introduced a privacy-preserving public auditing for data storage security in cloud computing. Proposed system 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 reduces the burden of cloud user from the tedious and possibly expensive auditing task. The process as data user can check the integrity of their data stored in cloud server using TPA which can be done in efficient manner. If any changes find out in data by the TPA, TPA will immediately intimate to the owner of the file and so security and data integrity is secured properly. The system further extend our privacy-preserving public auditing protocol into a many user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Third party auditor can be a trusted third party to resolve the conflicts between the cloud service provider and the client.

References

[1] P. Mell and T. Grance, "Draft NIST working definition of cloud computing," Referenced on June. 3rd, 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," University of California, Berkeley, Tech. Rep. UCBEECS-2009-28, Feb 2009.

[3] A. Juels and B.S. Kaliski Jr., "Pors: Proofs of Retrievability forLarge Files,"Proc. 14th ACM Conf. Computer and Comm. Security(CCS '07),pp. 584-597, 2007.
[4] M. Arrington, "Gmail disaster: Reports of mass emaildeletions," 2006
[5] J. Kincaid, "MediaMax/TheLinkup closes its doors,"July 2008,
[6] Amazon.com, "Amazon s3 availability event: July 20, 2008,"
[7] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling publicauditability and data dynamics for storage security in cloudcomputing," *IEEE Transactions on Parallel and Distributed Systems*,vol. 22, no. 5, pp. 847–859, 2011.
[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] 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.
[13] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 213-222, 2009.
[14] F. Sebe, J. Domingo-Ferrer, A. Martı´nez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient Remote Data Possession Checking in Critical Information Infrastructures," IEEE Trans. Knowledge and Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.
[15] T. Schwarz and E.L. Miller, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '06), 2006.
[16] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '08), pp. 411-420, 2008.
[17] K.D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198, 2009.