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

Secrecy Preserving Public Ascertaining for Cloud Storage Using Digital Signature

Rekha A[1], Padmashree G[2]

[1]M.Tech, Department of Computer Science & Engineering, MITE College, Moodabidri,-574225, mangalore, VTU University
[2]Sr. Assistant Professor , Departmentbof Computer Science & Engineering, Moodabidri,-574225, mangalore, VTU University

Abstract: ***Cloud is employed not just for storing data, however the stored data will be shared by multiple users. Due to this the integrity of cloud data is subject to doubt. Manymechanisms are designed to support public auditing of shared data stored within the cloud. Throughout auditing, the shared data is kept private from Third party auditor(TPA), who are able to verify shared data integrity using digital signature without downloading or retrieving the whole file. Digital signature is used to assess the verification metadata required to audit the correctness of shared data.With this, the identity of the signer on each block of a file is kept private from auditor. In this paper, we tend to propose the traceability and data freshness in the cloud using digital signatures.***

Keywords: Public auditing, secrecy preserving, shared data, traceability, datafreshness, cloud computing

1. Introduction

With cloud computing and storage, users are able to access and to share resources offered by the cloud service provider at a lower marginal cost. It is routine for users to leverage cloud storage services to share data with others in a group, as data sharing becomesa standard feature in most cloud storage offerings, as well as Drop box, iCloud and Google Drive . The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, asdata stored within the cloud will simply be lost or corrupted due to the inevitable hardware/software failures and human errors, the traditional approach for checking data correctness is to retrieve the whole data from the cloud, then verify data integrity by checking the correctness of themessage digest by using MD5 algorithm of the whole data.Certainly, this traditional approach is able to check the correctness of cloud data.However, the efficiency of using this approach on cloud knowledge is in doubt.

The most reason is that the dimensions of cloud data are large normally. Downloading the whole cloud data to verify the data integrity can price or waste the users amounts of computation and communication resources,particularly when the data arecorrupted within the cloud. Recently, several mechanisms are proposed to permit not only a data owner itself, however the auditor can also be to efficiently perform integrity checking without downloading the whole data from the cloud, that is referred as public auditing. With these mechanisms, data are split into several number of blocks,wherever every block is independently signed by the owner; and a random combination of all the blocksrather than the total data is retrieved throughout integrity checking.The auditor can give the several data integrity checking services. Existing public auditing mechanisms will truly be extended to verify shared data integrity and data freshness.

However, a brand new significant privacy issue introduced within the case of shared data with the utilization of existing mechanisms is that the leak of identity privacy to the auditor.To protect the confidential information, it is essential and demanding to preserve identity of signer from the auditor or public verifierthroughout public auditing. To solve the on top of privacy issue on shared data, we tend to propose a secrecy preserving mechanism, is completely unique privacy preserving public auditing mechanism. A lot ofspecifically, we tend to utilize digital signature and hash values of MD5 algorithm, in order verify the integrity of shared data without retrieving the whole data and it also helps to identify the signer on each block of a file which is stored in the cloud.

2. Literature Servey

G. Ateniese, et.al [2] proposed a Provable Data Possession (PDP) model in 2007. This model allows a client that has storeddata at an untrusted server to verify that the server possesses the original data without retrievingit. The model generates probabilistic proofs of possession by sampling random sets of blocksfrom the server, which drastically reduces I/O costs. The client maintains a constant amountof metadata to verify the proof. The challenge/response protocol transmits a small, constantamount of data, which minimizes network communication. Thus, the PDP model for remotedata checking supports large data sets in widely-distributed storage systems. They presented two provably-secure PDP schemes that are more efficient than previous solutions,even when compared with schemes that achieve weaker guarantees. In particular, the overheadat the server is low (or even constant), as opposed to linear in the size of the data. Experimentsusing our implementation verify the practicality of PDP and reveal that the performance ofPDP is bounded by disk I/O and not by cryptographic computation.

C. Wang, et.al [3] proposed a Privacy-Preserving Public Auditing system in 2010. Using Cloud Storage, users will remotely store their data and enjoy the on-demand prime quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the very fact that users now not have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, particularly for users

with constrained computing resources. Moreover, users should be in a position to just use the cloud storage as if it is local, without concern regarding the need to verify its integrity. Thus, enabling public auditability for cloud storage is of crucial importance so that users will resort to a third party auditor (TPA) to ascertain the integrity of outsourced data and be worry-free. To securely introduce a good TPA, the auditing method should bring in no new vulnerabilities towards user data privacy, and introduce no further on-line burden to user. During this paper, they proposed a secure cloud storage system supporting privacy-preserving public auditing. They have a tendency to more extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. In depth security and performance analysis show the plannedschemes areprovably secure and extremely efficient.

H. Shacham, et.al [4] proposed proof-of-retrievability system in 2008. A data storage center must prove to a verifier that he isactually storing all of a client's data. The central challenge is to build systems that are bothefficient and provably secure that is, it should be possible to extract the client's data fromany prover that passes a verification check. In this paper, they give the first proof-of-retrievabilityschemes with full proofs of security against arbitrary adversaries in the strongest model, that ofJuels and Kaliski. The first scheme, built from BLS signatures and secure in the random oraclemodel, has the shortest query and response of any proof-of-retrievability with public verifiability.Our second scheme, which builds elegantly on pseudorandom functions (PRFs) and is secure inthe standard model, has the shortest response of any proof-of-retrievability scheme with privateverifiability. Both schemes rely on homomorphic properties to aggregate aproof into one small authenticator value.

3. System Architecture

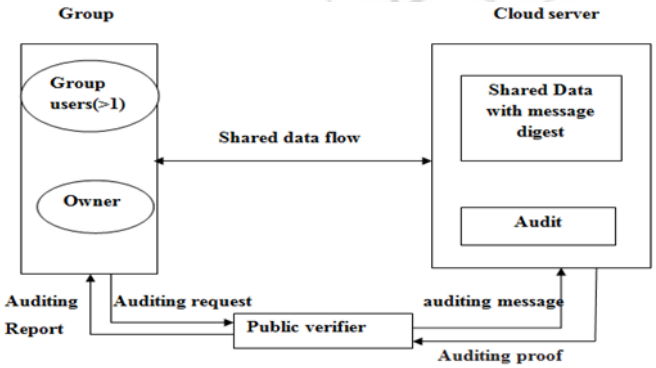

Figure 1: Proposed System

As explained in Figure 1, the system design includes 3 entities: the cloud server, a group of users and auditor/public verifier. A group of users includes admin/owner and cloud users [1].The owner contains a huge amount of knowledge to cache within the cloud. Cloud server has necessary data storage and computation power that is ruled by the cloud service supplier. The auditor has wonderful data auditing services to verify the correctness of shared data stored within the cloud server. The owner should have toregister into the cloud. The cloud sends the private key and public key by using the Digital Signature Algorithm[7] to all users who have registered into the cloud. The owner is going to browse the file and divide the file into three blocks. Each block should be encrypted using ECC algorithm[6] and then generate message digest for each block using MD5 algorithm[5]. Finally, those blocks with the message digest will be uploaded into the cloud. The users can able to modify the files, which are uploaded by the owner and upload to the cloud. The auditor requests to the cloud server to send the main points of the changed file block. The cloud server sends the file block details to the auditor. Then, the auditor will simply check the correctness of the complete data by examination the changed message digest of the file block with the main points provided by the cloud server.The the auditor is send the details of the user who has modified the file.

4. Conclusion

The proposed system known the signer on every block of a file that is hold on within the cloud. The auditor wouldn't learn any information regarding the info content stored on the cloud server. The proposed system eliminates the burden of cloud user from the tedious and probably valuable auditing task, however additionally reduces the users worry of their outsourced data leakage.

As future work the owner will refresh those changed data within the original format for various users. Additionally TPA at the same time handles multiple audit sessions from completely different users for his or her outsourced knowledge files, we have a tendency to more extend the proposed system in a very multi-user setting, wherever the TPA will perform multiple auditing tasks in a batch manner for higher efficiency additionally greatly reduces the computation price of the TPA.

Acknowledgement

I would like to thank Sr.Assistant Professor Padmashree G. I am so grateful for her help, professionalism and valuable guidance throughout this paper. This accomplishment would not hav been possible without her support. Thank you.

References

[1] B. Wang, B. Li, and H. Li, "Oruta: Privacy-Preserving PublicAuditing for Shared Data in the Cloud," Proc. IEEE Fifth Int'l Conf.Cloud Computing, pp. 295-302, 2012.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner,Z. Peterson, and D. Song, "Provable Data Possession atUntrusted Stores," Proc. 14th ACM Conf. Computer and Comm.Security (CCS '07), pp. 598-610, 2007.
[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Data Storage Security in Cloud Computing,"Proc. IEEE INFOCOM, pp. 525-533, 2010.

[4] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and InformationSecurity: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008
[5] The MD5 Message-Digest Algorithm: http://en.wikipedia.org/wiki/MD5.
[6] http://en.wikipedia.org/wiki/Elliptic_curve_cryptography for Elliptic curve cryptography.
[7] http://en.wikipedia.org/wiki/Digital_Signature_Algorithm for Digital signature algorithm