International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

A Review of Protect the Integrity of Outsourced Data Using Third Party Auditing for Secure Cloud Storage

Yogesh Shinde[1], Omprakash Tembhurne[2]

[1]Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, University of Pune, India

[2]Professors, Department of Computer Engineering, Dr. D. Y. Patil School of Engineering & Technology, University of Pune, India

Abstract: ***The Cloud computing is a leading technology which provides various services to users such as allows users to store their data on a cloud without worrying about correctness & integrity of data, use on-demand high quality applications and services. But as data is stored at the remote place how users will get the confirmation about data stored on the cloud. Hence Cloud data storage must have some mechanism which will specify storage correctness and integrity of data stored on a cloud. Enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. In this paper, review on innovative idea for secure cloud storage system supporting privacy-preserving public auditing. The results are also extended to enable the TPA to perform audits for multiple users simultaneously and efficiently. It supports data dynamics where the user can perform different operations on data such as insert, update and delete as well as batch auditing where multiple user requests for storage correctness will be handled simultaneously which decrease communication and also computing cost.***

Keywords: Cloud Computing, Third Party Auditing (TPA), Privacy Preserving, Data storage, Batch Verification

1. Introduction

Cloud Computing uses hardware and software as computing resources to provide service through internet. Cloud computing provides various service models such as platform as a service (PaaS), Infrastructure as a service (Iaas), software as a service (SaaS), storage as a service (STaaS), security as a service (SEaaS), Data as a service (DaaS) etc. The "software as a service" (SaaS) computing architecture, is transforming data centers into pools of computing service on a high scale. This means that, user can now subscribe high quality services from data that reside on remote data centers only because of the increasing network bandwidth and reliable yet flexible network connections.

The increasing advantages of Cloud computing in IT (Information Technology), it has been envisioned as the next generation IT architecture for enterprises, The Advantages can be listed as: on-demand self-service, worldwide network access, location independent resource pooling, faster resource elasticity, data usage-based pricing and transference of risk [1]. One important approach of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From perspective, including users' like individuals and IT enterprises, data storing on the cloud in a flexible on-demand approach brings fascinating benefits such as relief of the burden for storage management, universal data access with location independence and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

In order to resolve the issue of data integrity checking, many techniques are proposed under various systems and security models. In all these works, much more efforts are made to design solutions that meet different requirements such as high methodology efficiency, stateless verification, unbounded use of queries and retrievability of data, etc. By considering the role of the verifier or user in the model, all the methods presented before, categories like private auditability and public auditability. Although methods with private auditability can achieve higher scheme efficiency, public auditability allows not only the client (data owner) but also to challenge the cloud server for security of data storage while without keeping personal information. Then, clients are able to represent the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. Firstly, in the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Hence, for practical use, it seems much more rational to equip the verification protocol with public auditability, which is expected to play a most important role in achieving economies of scale for Cloud Computing. Secondly, for efficiency analysis, the outsourced data themselves should not be essential by the verifier for the verification purpose.

Recently, increasing interest in cloud computing has been shown in ensuring remotely stored data integrity under various system and security models. Some of the work has already been promoting the development of public auditability for existing cloud data storage services [4], [5], [6], [7]. However, it is not feasible yet. On one hand, clients i.e. data owners are currently not enough knowledgeable to demand risk assessment; on the other hand, current commercial cloud vendors do not provide such a third party auditing interface to support a public auditing service. Our contribution can be summarized as the following three aspects:

1) The motivation is the public auditing system of cloud data storage security and also provides a privacy-preserving

auditing protocol. The mechanism stated enables an external auditor to perform audit on user's cloud data without having any knowledge about the content present in that data.

2) This mechanism is the used to support scalable and efficient privacy-preserving public storage auditing in cloud. Basically, the mechanism achieves batch auditing where multiple delegated auditing tasks from different users can be performed concurrently by the TPA in a privacy-preserving manner.

3) This proves the security and justifies the performance of proposed schemes through different experiments and comparisons with the state of the art.

2. Literature Survey

C. Wang et al. [2] proposed a secure cloud data storage system supporting privacy-preserving public auditing. They further extended their result to enable the TPA to perform audits for multiple users simultaneously and efficiently. According to their proposed schemes they proved that the proposed schemes were provably secure and highly efficient. But the drawback of their scheme is, it is not used for multiple auditing tasks.

Sherman S. M. Chow proposed a secure cloud storage system which supporting privacy-preserving public auditing in [3]. They further extended the results to enable the third party (TPA) to performed audits for number of users simultaneously and efficiently.

Paper [4] introduced by Q. Wang et al. achieved the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two important features in their protocol design. To assist efficient handling of multiple auditing tasks, they further explored the technique of bilinear aggregate signature to extend their main result into a multi-user setting.

G. Ateniese [5] introduced a model for provable data possession (PDP) that allows a client (data owner) that has stored data at an untrusted server to verify that the server possesses the original data without extracting it.They addressed that the PDP model for remote data checking supports large data sets in widely-distributed storage systems. Besides, the overhead at the server is very low (or even constant), as completely opposed to linear in the size of the data.

In [6] H. Shacham and B. Waters gave the first proof of retrievability mechanisms with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. Their first scheme was built from BLS signatures and secure in the random oracle model.Their second scheme was building on pseudorandom functions (PRFs) and they stated that this scheme is secure in the standard model which allows only private verification.

A. Juels al, J. Burton. [7] defined and explored the proofs of irretrievability (PORs). According to their study, a POR scheme enables an archive or back-up service (provider) to produce a concise proof that a user (verifier) can retrieve a target file, means, that the archive retains and reliably transmits file data sufficient for the user to recover F in its entirety. In order to maintain the integrity of data in cloud B. Dhiyanesh [8] provided public audit ability to the network. This auditability can be done by third party auditor (TPA) on behalf of the cloud client to analyse the integrity of the dynamic stored cloud data. This removes the interference of users to check their intactness which could be important in achieving economies of scale for Cloud Computing.

S. Marium et al. [9] is containing to highlight cloud security and privacy problems. Their research was mainly focus on service provider's side security. S.Marium et al. purposed the implementation of Extensible Authentication Protocol through three way hand shake with RSA to ensure the security of client data in cloud.

Table 1: Summary of the Previous Techniques

Sr. No	Title of Paper	Previous Technique Used	Drawback of Existing System
1.	An Effective Privacy Protection Scheme for Cloud Computing [11]	Encryption Algorithm	Not Contain Dynamic data operation & server misbehavior
2.	Towards Secure and dependable Storage Services in Cloud Computing [12]	Distribution of file & Challenge token, File Retrieval and Error recovery	Large Memory Space Required
3.	Ensuring Data Storage Security in Cloud Computing [13]	Based on Token pre – computation	It does not support Insertion or Add operation
4.	Scalable and Efficient Provable Data Possession [14]	Symmetric key Cryptography	It also does not contain insertion operation.
5.	Auditing to Keep Online Storage Services Honest [15]	System support both internal and external auditing of online storage Services.	Cryptographic scheme is not Sufficient to maintain the privacy.
6.	On Data Replication and Storage Security over Cloud Computing: Are we getting what we are paying For? [16]	Stores multiple Copies of user data	Storage overhead at server side Increases.
7.	Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing[17]	RSA encryption Algorithm	File cannot be retrieved when server misbehavior detect.

3. Basic System Architecture

Representative Storage architecture for cloud data storage is illustrated in Fig. 1. Three different network components, Client, CSS and TPA can be identified as follows:

- **Client:** It is an entity, which can be individual consumers or organizations and has set of data files to be stored in the cloud and trust on the cloud for data maintenance and computation;
- **Cloud Storage Server (CSS):** It is an entity, which is managed maintained by Cloud Service Provider (CSP), has consequential storage space and computation resources to maintain the clients' data.
- **Third Party Auditor (TPA):** It is an entity, which has expertise and capabilities that clients' users do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

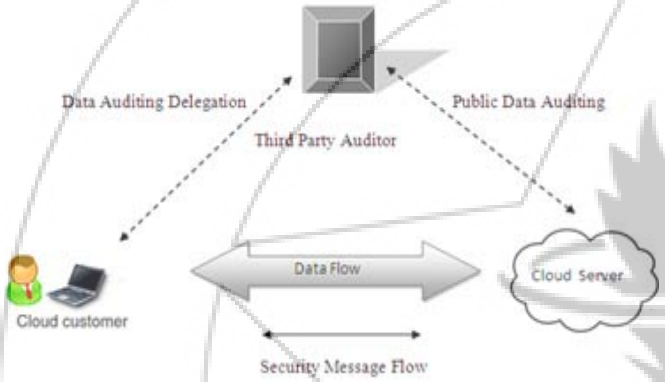

Figure 1: The Architecture of cloud data storage

4. Applications

Third Party Auditor (TPA) to check the integrity of outsourced data has been studied widely for having many real world applications. Followings are the application areas:

1) Fraud detection
2) Misbehaving of servers detection

5. Conclusion

In this way we surveyed many techniques which are meant for integrity checking of outsourced data. Third Party Auditor (TPA) can be used to maintain the security and integrity of outsourced data. TPA would not learn any information about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the load of cloud user from the tedious and possibly expensive auditing task, but also relives the users' fear of their outsourced data leakage or data loss. This paper contains an abstract view of various technique proposed in recent past year for cloud data security and integrity using third party auditor.

References

[1] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, June 2009.
[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-PreservingPublic Auditing for Storage Security in Cloud Computing," Proc.IEEE INFOCOM '10, Mar. 2010.
[3] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud storage",IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.
[4] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling PublicAuditability and Data Dynamics for Storage Security in CloudComputing," IEEE Trans. Parallel and Distributed Systems, vol. 22,no. 5, pp. 847-859, May 2011.
[5] 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. Security(CCS '07), pp. 598-609, 2007.
[6] 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.
[7] 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.
[8] Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" , International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 6602 3127,2011
[9] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177- 183, 2012
[10] Bharti Dhote , A.M. Kanthe "Secure Approach for Data in Cloud Computing" International Journal of Computer Applications, Volume 64– No.22, February 2013 ISSN: 0975 – 8887
[11] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo, "An Effective Privacy Protection Scheme for Cloud Computing", ICACT-2011, Pages 260-265
[12] Cong Wang,Qian Wang,Kui Ren, Ning Cao , and Wenjing Lou "Toward Secure and Dependable Storage Services in Cloud Computing" IEEE Transaction On Service Computing Vol. 5,No.2,April-June 2012
[13] Cong Wang, Qian Wang, Kui Ren, Wenjing Lou "Ensuring Data Storage Security in Cloud Computing," Proc.IWQoS '09, July 2009, Pages 1–9.
[14] Giuseppe Ateniese, Roberto Di Pietro, Luigi V. Mancini, and Gene Tsudik., "Scalable and Efficient Provable Data Possession," Proc.SecureComm '08, Sept. 2008.

[15] Mehul A. Shah, Mary Baker, Jeffrey C. Mogul, Ram Swaminathan., "Auditing to keep Online Storage Services Honest," Proc.USENIX HotOS '07, May 2007.
[16] Ayad F.Barsoum and M.Anwar Hasan, "On Data Replication and Storage Security over Cloud Computing: Are we getting what we are paying for?" in digital library citeseerx.ist.psu.edu/viewdoc/ pg. 1-36
[17] Uma Somani,Kanika Lakhani,Manish Mundra, "Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing" , 2010 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010) Pages 211-216

Author Profile

Yogesh N. Shinde Research Scholar Dr. D.Y.Patil School of Engineering & Technology, Pune, University of Pune. He received B.E. in Information Technology from Information Technology Department of Tatyasaheb Kore Institute of Engineering & Technology, Warananagar, Kolhapur from Shivaji University. Currently He is pursuing M.E. in computer engineering from Dr. D.Y. Patil School of Engineering & Technology, Pune, University of Pune, India

Prof. Omprakash Tembhurne received the B.E. and MTech degrees in Computer Science Engineering. Currently he is working as Assistant Professor of Computer Engineering Department in Dr. D. Y. Patil School of Engineering & Technology, Pune, India