www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 5 Issue 1 Jan 2016, Page No. 15411-15414

A Review On Efficient Privacy Preserving And Secure Data Integrity Protection In Regenerating Coding Based Multi-Cloud Storage

Supriya Sahare[1], Prof. Fazeel I. Z. Qureshi[2]

[1] Department of Computer Science and Engineering,RTMNU University , W.C.E., Nagpur, Maharashtra, India.
supriya.sahare7@gmail.com
[2] Department of Computer Science and Engineering,RTMNU University , W.C.E, Nagpur, Maharashtra, India.
Fazeel.zama20@gmail.com

Abstract:
Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, 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, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits in multi-cloud storage efficiently**.**
Keywords: Cloud Storage, Privacy Preserving, Public Auditing, Data integrity

1. Introduction

Cloud computing is one of the hottest buzzwords in technologies. It provides access to its users to various services that it provides. The emergence of this new technology allows users to access their files, software and computing power over the web. Many small scale businesses and organization can establish its infrastructure without the need for implementing actual hardware and software that are needed to build entire structure as it can entirely rely on the cloud services and use its resources on pay per use basis. But as every coin has two sides so, with this advent of technology where data is easily stored and available on cloud; there are various threats challenging the data security and integrity.

Popularity of cloud computing comes with various advantages like on-demand self service provisioning. Even these advantages are more appealing to reduce the cost on IT expenditure & relief the user online burden of data storage they brings new and challenging security threats toward users' outsourced data[1]. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity [1]. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.

The data stored on cloud is in shared form which invites the threats like loss or corruption of data due to software, hardware or human errors [2]. Moreover, the cloud service providers (CSP) may be reluctant to inform the data owner about the

data theft or corruption due to fear of losing their reputation and business profit. So, to deal with this issues, Public Verifiers are used. A public verifier could be data user who would like to utilize the owner's data via cloud or third party auditor (TPA) who can provide expert integrity checking services.

There are several approaches [3] [4] to check the correctness of the data stored on the cloud, like the traditional approach is to retrieve the entire data from the cloud to check its correctness. But, this approach wastes users' amount of computation and communication resources and of course the time and cost.

1.1 Public Auditing

Public auditing is the service which is used to ensure integrity of the data stored on the cloud storage and save the cloud users' computation resources. To perform the auditing task the TPA known as third party auditor used to audit the stored data on cloud on the behalf of data owner. TPA verify the correctness of the cloud data on demand without retrieving a copy of the whole data. The TPA, has expertise and capabilities that can periodically check the integrity of all the data stored which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud.

2. Review Of Literature:

Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian[5] proposed two scheme. First for auditing scheme and second for privacy preserving. Although previous paper introduced private remote data checking schemes for regenerating-code-based cloud storage, there are still some other challenges for us to design a public auditable version. Hence they proposed public auditing scheme which allows the public verifier to audit the correctness of data even if the data owner is offline. First, this scheme construct a BLS-based authenticator, which consists of two parts for each segment of coded blocks. Utilizing its homomorphic property and the linearity relation amongst the coded blocks, the data owner is able to generate those authenticators in a new method, which is more efficient compared to the straightforward approach.

Henry C.H. Chen and Patrick P.C. Lee introduced a scheme to protect outsourced data in cloud storage against corruptions, adding fault tolerance to cloud storage, along with efficient data integrity checking and recovery procedures, becomes critical. They design and implement a practical data integrity protection (DIP) scheme for a specific regenerating code, while preserving its intrinsic properties of fault tolerance and repair-traffic saving. DIP scheme is designed under a mobile Byzantine adversarial model, and enables a client to feasibly verify the integrity of random subsets of outsourced data against general or malicious corruptions. It works under the simple assumption of thin-cloud storage and allows different parameters to be fine-tuned for a performance-security trade-off[6].

Henry C.H. Chen, Yuchong Hu, Patrick P.C. Lee, and Yang Tang designed a proxy-based storage system for fault-tolerant multiple-cloud storage called NCCloud, which achieves cost-effective repair for a permanent single-cloud failure. NCCloud is built on top of a network-coding-based storage scheme called the functional minimum storage regenerating (FMSR) codes, which maintain the same fault tolerance and data redundancy as in traditional erasure codes[7].

Kan Yang, and Xiaohua Jia[8] proposed an auditing framework for cloud storage systems and proposed an efficient and privacy-preserving auditing protocol, further extended auditing protocol to support the data dynamic operation. Also further extend auditing protocol to support batch auditing for both multiple owners and multiple clouds, without using any trusted organizer.

Yan Zhu, Hongxin Hu, Gail-Joon Ahn and Mengyang Yu introduced a Cooperative Provable Data Possession (CPDP) scheme based on homomorphic verifiable response and hash index hierarchy whose security is based on multiprover zero-knowledge proof system[9]. Also it focus on performance optimization mechanisms for the given scheme.

Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou designed a scheme which is combination the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system. To support efficient handling of multiple auditing tasks, they further explore the technique of bilinear aggregate signature to extend result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously [10].

3. Proposed Scheme:

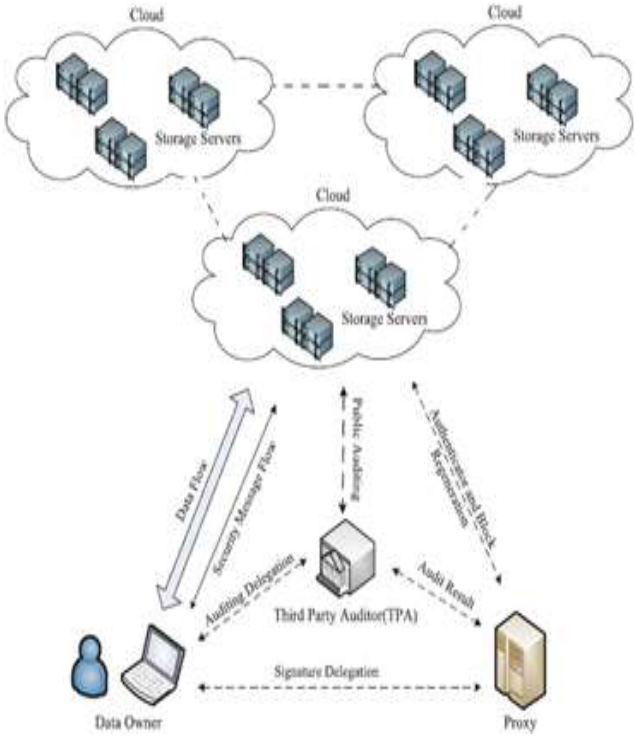

Fig. 1. System model

We consider the auditing system model for regenerating Code-based for multi-cloud storage as Fig.1, which involves four entities: the data owner, who owns large amounts of data files to be stored in the multi-cloud; the cloud, which are managed by the cloud service provider, provide storage service and have significant computational resources; the third party auditor (TPA), who has expertise and capabilities to conduct public audits on the coded data in the cloud, the TPA is trusted and its audit result is unbiased for both data owners and cloud servers; and a proxy agent, who is semi-trusted and acts on behalf of the data owner to regenerate authenticators and data blocks on the failed servers during the repair procedure. Notice that the data owner is restricted in computational and storage resources compared to other entities and may become off-line even after the data upload procedure. The proxy, who would always be online, is supposed to be much more powerful than the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources as well as the online burden potentially brought by the periodic auditing and accidental repairing, the data owners resort to the TPA for integrity verification and delegate the reparation to the proxy.

4. Conclusion:

We present, multi-cloud, a proxy-based, and multiple cloud storage system that practically addresses reliability of today's cloud backup storage. In this paper, we proposed public auditing scheme for the regenerating code based multi-cloud storage, where data owner are privileged to make data validity checking. To protect original data privacy, we have provided efficient technique during auditing process. Assuming that data owner is not always able to stay online in practice, in order to keep storage available and verifiable after malicious corruption, we introduce semi-trusted proxy into the system model and provide a privilege for proxy to handle the reparation of coded block and authenticators. Thus, this authenticator can be efficiently generated by the data owner simultaneously with encoding procedure.

References

1. Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010.
2. D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses,"Computer, vol. 45, no. 1, pp. 39-45, 2012.
3. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession,"Proc. 16th ACM Conf. Com-puter and Comm. Security (CCS'09), pp. 213-222, 2009.

4. Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing,"Proc. 14th European Conf. Research in Computer Security (ESORICS'09), pp. 355-370, 2009.
5. Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "Privacy Preserving Public Auditing for Regenerating-Code-Based Cloud Storage", 2015.
6. Henry C.H. Chen and Patrick P.C. Lee, "Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation", 2014.
7. Henry C.H. Chen, Yuchong Hu, Patrick P.C. Lee, and Yang Tang, "NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds", 2014.
8. Kan Yang, Xiaohua Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", 2013.
9. Yan Zhu, Hongxin Hu, Gail-Joon Ahn, and Mengyang Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", 2012.
10. Cong Wang, Qian Wang, and Kui Ren, Wenjing Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", 2010.
11. C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," Apr./Jun. 2012.
12. A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," Sep. 2010.
13. A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Mar. 2011.
14. [14] Pooja Kapadne," Survey on Privacy Preserving Public Auditing for Shared Data in Cloud", July-August, 2015.
15. S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage", 2013.
16. M. Armbrust et al., "Above the clouds: A Berkeley view of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.
17. G. Ateniese et al., "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.
18. A. Juels and B. S. Kaliski, Jr., "PORs: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Comput. Commun. Secur., 2007, pp. 584–597.
19. R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-replica provable data possession," in Proc. 28th Int. Conf. Distrib. Comput. Syst. (ICDCS), Jun. 2008, pp. 411–420.
20. K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A high-availability and integrity layer for cloud storage," in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 187–198.
21. J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," J. Comput. Syst. Sci., vol. 78, no. 5, pp. 1345–1358, 2012.