© 2016 IJSRSET | Volume 2 | Issue 4 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Privacy Preserving and Dynamic Auditing for Outsourced Storages in Cloud

Satish Shelar*, Prof. S. Y. Raut
Computer Engineering, Pravara Rural Engineering College, Loni, Maharashtra, India

ABSTRACT

In cloud storage users can remotely store their data without the burden of local data storage and maintainance. Data security and data integrity for the outsourced data in the cloud becomes difficult and facing different types of problems. Fault tolerance is also necessary for security of the data in the cloud. Regenerating code is the concept which got the importance because of their lower bandwidth while providing fault tolerance. Last remote checking methods for regenerating coded data provides just private auditing which keeps data holders always online because of that auditing as well as repairing becomes difficult. In this paper we are going to develop a dynamic auditing system for the regenerating code based secure cloud storage. In order to develop the solution for the regeneration problem of failed authenticators when data holders are not present, we make a proxy, which is used to regenerate the authenticators, in the traditional public auditing scheme. Thus our system can almost release data holders from online load. Our system gives more efficiency and can be possibly combined with the regenerating secure cloud based storage.

Keywords: Cloud Storage, Regenerating Code, Public Auditing, Dynamic Auditing, Privacy Preserving, Proxy

I. INTRODUCTION

Cloud computing got importance because of various advantages like frees of burden from storage management, open access and avoidance of capital investment on hardware, software and personal maintenance etc. Some-times data holders lose their control on the destiny of their outsourced data; therefore the qualities of data like correctness and avail-ability becomes difficult to maintain. Most of the times the cloud service providers with the internal and external opponents , who would maliciously destroy users data and many times some cloud service providers acts as cheater and they tries to keep secretes about data loss and shows that the data is stored securely and correct for their reputation[1].

Therefore it is important for the users to evolve an effective protocol to perform regular confirmation about the accuracy of the outsourced data and also to ensure data integrity. Some implementations concerning with the correctness of outsourced data in the absence of a spatial copy have been presented under various methods and security methods up to this. The most important work from these inventions are the Provable Data Possession (PDP) model [1]and Proof Of Retrivability (POR), which was originaly presented for the single server scenario. Just imagine that files are spreaded and duplicatly stored on the multiple servers and multiple clouds[3], examine integrity confirmation techniques appropriate for such multiple servers and multiple cloud setting with many redundancy techniques[10], such as replication more recently, regenerating codes.

In this paper, we concentrate on integrity confirmation problem in regenerating cloud based storage systems, mainly with the functional repair strategy. In private auditing, only data holder is allowed to verify the integrity and regenerate the corrupted servers[10]. Suppose the large amount of outsourced data and the tasks of auditing and reparation in the cloud can be difficult and expensive for the users. The high burden of using cloud storage should be reduced as much as possible such that the number of operations done by the user should be less to their outsourced data[11].

Sometimes users may not want to go through the various problems in checking and reparation. In some auditing systems users need to always stay on-line, specially for the long term data storage[7][8]. To ensure data integrity and to save users online burden, we present public auditing scheme for the regenerating-code-based cloud storage, in which integrity verification and regeneration are obtained by third party auditors and a semi trusted proxy instead of the data owner. Instead of directly applying the last public auditing system to the multi-server setting, we propose a novel authenticator, which is more efficient for regenerating codes.

II. LITERATURE SURVEY

As the frequency for using internet increases, threats, attacks also increases. Therefore, number of researchers works on security issues in cloud.

M. Armbrust et al, Above the cloud: A Berkeley view of cloud computing discussed all the fundamental components of cloud computing and major aspects of cloud computing. This paper shows information about cloud computing definitions and its applications, cloud infrastructure, obstacles and openings in cloud computing, cloud storage and auditing capability etc. This paper gives a brief idea of basic cloud computing concept and current requirements but not gives any technical details.

N. K. Yang and X. Jia, An efficient and secure dynamic auditing protocol for data storage in cloud computing, proposed an efficient and inherently secure dynamic auditing protocol. It gives privacy to the data against the auditor by combining the cryptography method with the bilinearity property of bilinear paring, other than using the mask method.

O.C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, Toward secure and dependable storage ser-vices in cloud computing, demonstrates flexible distributed storage integrity auditing mechanism, using the homomorphic token and dis-tributed erasure-coded data. The presented de-sign permits users to audit the cloud storage with a little communication and computation cost. The auditing result not only gives strong cloud storage correctness guarantee, but also simultaneously takes fast data error localization, i.e., the identification of damaged servers.

C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for secure cloud storage introduced that a se-cure cloud storage system supporting privacy-preserving public auditing. They also provide their result to activate the TPA to do audits for many users at the same time and efficiently. Major security and achivement analysis show the proposed schemes are provably secure and highly efficient. Their analysis conducted on Amazon EC2 instance further explains the fast execution of the design.

H. C. H. Chen and P. P. C. Lee, Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage introduced simple assumption of thin-cloud storage and permits various parameters to be fine-tuned for the execution-security trade-off. They analyse and calculate the overhead of our DIP scheme in a real cloud storage test bed under different parameter choices. We implement and evaluate the hanging of their DIP scheme in a real cloud storage test bed under various parameter alternatives. They explains that remote integrity checking can be possibly combined into regenerating codes in practical deployment.

C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, provides privacy-preserving public auditing system for data storage security in Cloud Computing and gives an effective third party auditor(TPA) for various basic requirements.

B.Chen, R. Curtmola, G. Ateniese, and R. Burns, Remote data checking for network coding-based distributed storage systems, introduced RDC-NC, a novel secure and efficient RDC scheme for network coding-based distributed storage systems. RDC-NC mitigates new attacks that stem from the underlying principle of network coding. The scheme is able to maintain in an adversarial setting the mini-mal communication burden of the repair component achieved by network coding in a benign setting. They implement our scheme and experimentally show that it is computationally inexpensive for both clients and servers.

B.G. Worku, C. Xu, J. Zhao, and X. He, Secure and efficient privacy preserving public auditing scheme for cloud storage, provides a privacy preserving public auditing scheme that helps public auditing and identity

privacy on shared data stored in the cloud storage service for increasing its security and efficiency. This paper has mainly concentrated on improving the security mechanism of own Cloud storage service.

In this paper we are going to propose a public auditing scheme for the regenerating code based secure cloud storage. In order to propose the solution for the regeneration problem of damaged authenticators in the nonapperance of data holders, we are going to develop a proxy, which is privileged to regenerate the authenticators, in the traditional public auditing scheme. Thus this system can almost frees data holders from online load. Experimental evaluation model shows that this system is got more efficiency and can be possibly combined into the regenerating cloud based storage.

III. PROPOSED SYSTEM

We consider an auditing system model for dynamic auditing in the cloud storage, which involves four parts which involves four entities: the data owner, who owns large amounts of data files to be stored in the 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.

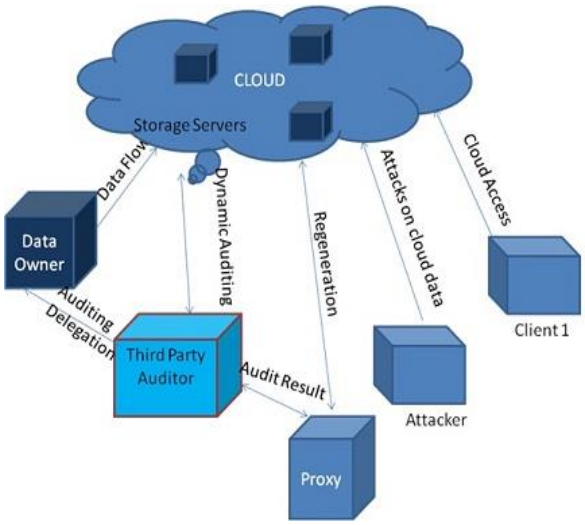

Figure 1. System Model

1. Data owner consists of huge amount of data which is stored on the cloud servers.
2. Cloud servers provides different cloud services and storage maintenance and have various beneficial resources
3. The third party auditor handles the public audit on the coded data on the cloud servers and audit results are same for data owner and the cloud servers.
4. Proxy agent is the trustworthy and may behave as a data owner to generate authenticators again and used to repair the data blocks on the failed servers during the repair procedure.

The data owner is forced in computational and storage resources matched to other entities and may goes off-line even after the data uploaded on the cloud servers. The proxy is the most powerful than the data owner but less than the cloud servers in terms of computation and storage capacity, who would be always online. The cyclic auditing and coincidental repairing is used to save resources and online load. The data owners centre to the TPA for integrity checking and alternate the reparation to the proxy. As compare to the last public auditing system architecture, our system model includes an one more block that is proxy agent.

The auditing scheme consist of three procedures: Setup, Audit, Repair

1. Setup

Data owner used setup procedure to initialize the auditing scheme.

2. Audit:

Audit procedure contains the interaction between TPA and cloud servers in which random sample is taken and on the blocks to check correctness of data.

3. Repair:

When data owner is not present, the proxy interacts with the cloud servers during the repair procedure to repair the damaged servers found by auditing process.

Design Goals

1. **Dynamic Auditing**: To permit TPA to check the correctness of the data in the cloud on demand without introducing additional online load to the data owner.

2. **Storage Soundness:** To make sure that the cloud server can never pass the auditing procedure apart from when it indeed man-age the owners data intact.

3. **Privacy Preserving:** To ensure that neither the auditor nor the proxy can obtain users data content within auditing and reparation processes.

4. **Data Regeneration:** The authenticator of the repaired blocks can be correctly generated again in the absence of the data owner.

IV. RESULTS AND DISCUSSION

In our system there is privacy-preserving public audit scheme during the Setup, Audit and Repair procedure. During the Setup phase, the authenticators are generated in a novel method instead of computing an authenticator for each segment of every coded block independently meaning that the file is first encoded and then authenticator is directly computed for each segment and then fragmentation is done.

Considering that the cloud servers are usually powerful in computing capacity, we focus on analyzing the computational overhead on the auditor side and omit those on the cloud side. The regeneration of the corrupted files is delegated to a proxy in our dynamic auditing scheme. The result graphs are as followes

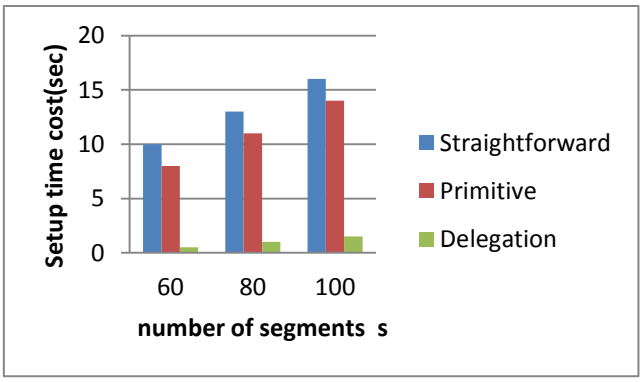

Figure 2. Time for System Setup

.

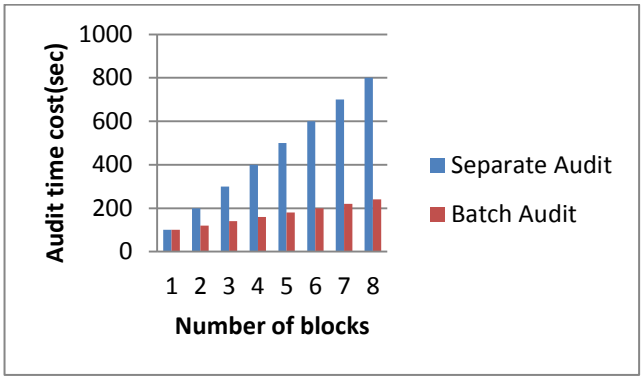

Figure 3. Time for Audit

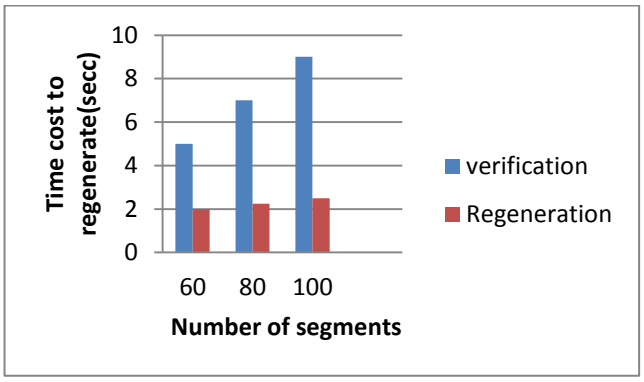

Figure 4. Time for Repair

I. CONCLUSION

In this paper, we are going present a public au-diting scheme for the regenerating-code-based cloud storage system, where the data owners are right to delegate TPA for their data validity confirmation. Data owner cannot always stay online , in order to keep the storage available and verifiable after a malicious corruption, we present a semi-trusted proxy into the system model and give a privilege for the proxy to maintain the regeneration of the data.

II. REFERENCES

[1] 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.

[2] 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. 598609.

[3] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, Distributed data possession checking for securing multiple replicas in geographically dispersed

clouds, J. Comput. Syst. Sci., vol. 78, no. 5, pp. 13451358, 2012.

[4] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, Re-mote data checking for network coding-based distributed storage systems, in Proc. ACM Workshop Cloud Comput. Secur. Workshop, 2010, pp. 3142. .

[5] H. C. H. Chen and P. P. C. Lee, Enabling data integrity pro-tection in regenerating-coding-based cloud storage: Theory and implementation, IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 407416, Feb. 2014.

[6] K. Yang and X. Jia, An efficient and secure dynamic au-diting protocol for data storage in cloud computing, IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 17171726, Sep. 2013.

[7] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, Cooperative provable data possession for integrity verification in multicloud storage, IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 22312244, Dec. 2012.

[8] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, A survey on network codes for distributed storage, Proc. IEEE, vol. 99, no. 3, pp. 476489, Mar. 2011.

[9] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, NCCloud: Applying network coding for the storage repair in a cloud-of-clouds, in Proc. USENIX FAST, 2012, p. 21.

[10] C. Wang, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for data storage security in cloud computing, in Proc. IEEE INFOCOM, Mar. 2010, pp. 19

[11] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, Privacy-preserving public auditing for secure cloud storage, IEEE Trans. Comput., vol. 62, no. 2, pp. 362375, Feb. 2013J. Misic and V. B. Misic, Implementation of security policy for clinical information systems over wireless sensor networks, Ad Hoc Networks,vol.5, no.1, pp.134-144, Jan 2007.

[12] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, Toward secure and dependable storage services in cloud comput-ing, IEEE Trans. Service Comput., vol. 5, no. 2, pp. 220232, Apr./Jun. 2012.

[13] Y. Deswarte, J.-J. Quisquater, and A. Sadane, Remote integrity checking, in Integrity and Internal Control in Information Systems VI. Berlin, Germany: Springer-Verlag, 2004, pp. 111.

[14] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, Scalable and efficient provable data possession, in Proc. 4th Int. Conf. Secur. Privacy Commun. Netw., 2008, Art. ID 9.

[15] C. Erway, A. Kp, C. Papamanthou, and R. Tamassia, Dynamic provable data possession, in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 213222.

[16] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, Enabling public verifiability and data dynamics for storage security in cloud computing, in Computer Security. Berlin, Ger-many: Springer-Verlag, 2009, pp. 355370.

[17] S. G. Worku, C. Xu, J. Zhao, and X. He, Secure and efficient privacy preserving public auditing scheme for cloud storage, Comput. Elect. Eng., vol. 40, no. 5, pp. 17031713, 2013.

[18]] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage, in IEEE Trans. on information forensics and security , vol.. 10,no. 7, July 2015.