IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. VI (Nov – Dec. 2014), PP 24-28
www.iosrjournals.org

Efficient Audit Services for Data Outsourcing in Clouds

Anuraj C.K
(Department of Computer Science and Engineering, Sapthagiri College of Engineering, Dharmapuri/Anna University,Chennai)

Abstract: *This paper introduce a dynamic audit service for integrity verification of untrusted and outsourced storages. Our audit service is constructed based on the techniques, fragment structure, random sampling, and index-hash table, supporting provable updates to outsourced data and timely anomaly detection. Constructed on interactive proof system (IPS) with the zero knowledge property, our audit service can provide public auditability without downloading raw data and protect privacy of the data. Also, our audit system can support dynamic data operations and timely anomaly detection with the help of several effective techniques, such as fragment structure, random sampling, and index-hash table (IHT). We also propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof-of-concept prototype is also implemented to evaluate the feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show that our system does not create any significant computation cost and require less extra storage for integrity verification.*
Keywords: *Cloud storage, audit service, storage security*

I. Introduction

The cloud storage service (CSS) relieves the burden for storage management and maintenance. However, if such an important service is vulnerable to attacks or failures, it would bring irretrievable losses to the clients because their data or archives are stored in an uncertain storage pool outside the enterprises. These security risks come from the following reasons: First, the cloud infrastructures are much more powerful and reliable than personal computing devices, but they are still susceptible to internal threats (e.g., via virtual machine) and external threats (e.g., via system holes) that can damage data integrity; second, for the benefits of possession, there exist various motivations for cloud service providers (CSP) to behave unfaithfully toward the cloud users ; furthermore, disputes occasionally suffer from the lack of trust on CSP because the data change may not be timely known by the cloud users, even if these disputes may result from the users' own improper operations [1]. Therefore, it is necessary for CSP to offer an efficient audit service to check the integrity and availability of stored data [2]. Therefore, security and performance objectives such as Public auditability, dynamic operations, timely detection, effective forensic are the objectives should be addressed to achieve an efficient audit for outsourced storage in clouds.

Public auditability: To allow a third party auditor (TPA) or clients with the help of TPA to verify the correctness of cloud data on demand without retrieving a copy of the whole data or introducing additional online burden to cloud services.

Dynamic operations: To ensure there is no attack to compromise the security of verification protocol or cryptosystem by using dynamic data operations.

Timely detection: To detect data errors or losses in outsourced storage, as well as anomalous behaviors of data operations in a timely manner.

Effective forensic: To allow TPA to exercise strict audit and supervision for outsourced data, and offer efficient evidences for anomalies.

Lightweight: To allow TPA to perform audit tasks with the minimum storage, lower communication cost, and less computation overhead.

II. Related Works And Problem Definition

The traditional cryptographic technologies for data integrity and availability, based on Hash functions and signature schemes [3], [4], [5], cannot work on the outsourced data. it is not a practical solution for data validation by downloading them due to the expensive communications, especially for large size files. Moreover, the ability to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users. Therefore, it is crucial to realize public audit ability for CSS, so that data owners (Dos) may resort to a third party auditor (TPA) , who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and credibility in clouds. To implement public audit ability, the notions of proof of retrievability (POR) [6] and

provable data possession (PDP) [7] have been proposed by some researchers. Their approach was based on a probabilistic proof technique for a storage provider to prove that clients' data remain intact.

There exist some solutions for audit services on out-sourced data. For example, Xie et al. [8] proposed an efficient method on content comparability for outsourced database, but it was not suitable for irregular data. Wang et al. [9] also provided a similar architecture for public audit services. To support their architecture, a public audit scheme was proposed with privacy-preserving property. However, the lack of rigorous performance analysis for a constructed audit system greatly affects the practical application of their scheme. For instance, in this scheme an outsourced file is directly split into n blocks, and then each block generates a verification tag. To maintain security, the length of block must be equal to the size of cryptosystem, that is, 160 bits, which is 20 bytes. This means that 1M bytes file is split into 50,000 blocks and generates 50,000 tags [10], and the storage of tags is at least 1M bytes. Therefore, it is inefficient to build an audit system based on this scheme. To address such a problem, we introduce a fragment technique to improve the system performance and reduce the extra storage.

Another major concern is the security issue of dynamic data operations for public audit services. In clouds, one of the core design principles is to provide dynamic scalability for various applications. This means that remotely stored data might be not only accessed by the clients but also dynamically updated by them, for instance, through block operations such as modification, deletion and insertion. However, these operations may raise security issues in most of existing schemes, e.g., the forgery of the verification metadata (called as tags) generated by DOs and the leakage of the user's secret key. Hence, it is crucial to develop a more efficient and secure mechanism for dynamic audit services, in which a potential adversary's advantage through dynamic data operations should be prohibited.

III. Proposed Scheme

This paper introduce a dynamic audit service for integrity verification of untrusted and outsourced storages [6]. Our audit system, based on novel audit system architecture, can support dynamic data operations and timely abnormal detection with the help of several effective techniques, such as fragment structure, random sampling, and index-hash table. Furthermore, we propose an efficient approach based on probabilistic query and periodic verification for improving the performance of audit services. A proof of- concept prototype is also implemented to evaluate the 2 feasibility and viability of our proposed approaches. Our experimental results not only validate the effectiveness of our approaches, but also show our system has a lower computation cost, as well as a shorter extra storage for integrity verification

IV. Architecture

This paper introduce an audit system architecture for outsourced data in clouds as shown in Fig. 1. In this architecture, we consider that a data storage service involves four entities: DO, who has a large amount of data to be stored in the cloud; CSP, who provides data storage service and has enough storage space and computation resources; TPA, who has capabilities to manage or monitor the outsourced data under the delegation of DO; and authorized applications (AAs) , who have the right to access and manipulate the stored data. Finally, application users can enjoy various cloud application services via these AAs.

Here assume the TPA is reliable and independent through the following audit functions: TPA should be able to make regular checks on the integrity and availability of the delegated data at appropriate intervals; TPA should be able to organize, manage, and maintain the outsourced data instead of Dos, and support dynamic data operations for AAs; and TPA should be able to take the evidences for disputes about the inconsistency of data in terms of authentic records for all data operations.

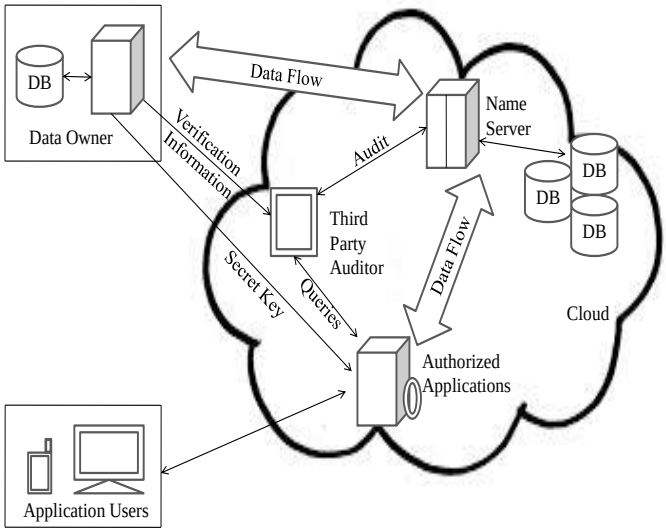

Fig. 1. Audit System Architecture

V. Techniques

To realize these functions, our audit service is comprised of three processes:

V. 1. Tag Generation

The client (DO) uses a secret key to preprocess a file, which consists of a collection of n blocks, generates a set of public verification parameters (PVPs) and index hash table (IHT) that are stored in TPA, transmits the file and some verification tags to CSP, and may delete its local copy (See Fig. 2.1).

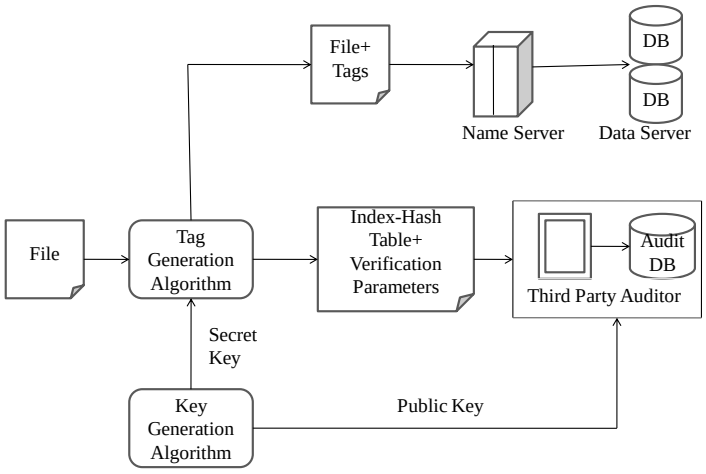

Fig. 2.1. Tag generation for outsourcing file

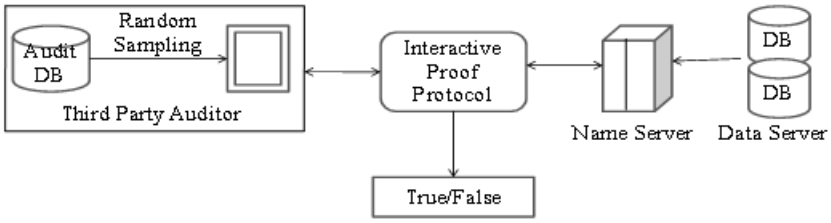

Fig. 2.2. Periodic Sampling Audit

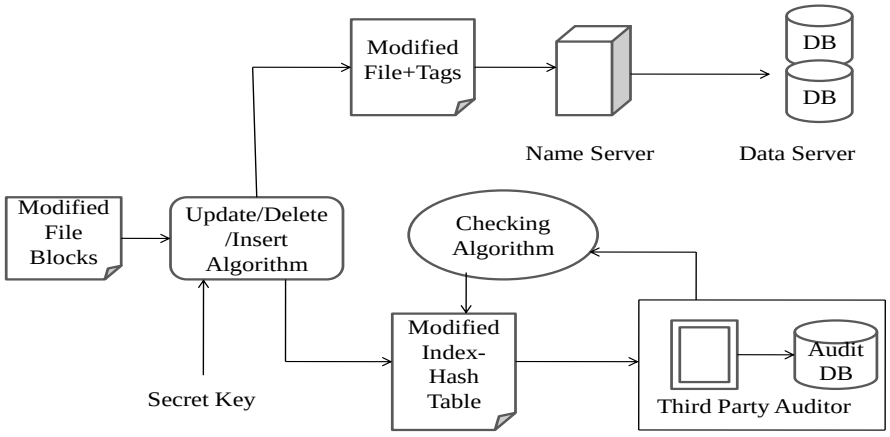

Fig. 2.3. Dynamic data operations and audit
Fig. 2. Three processes of audit system

V. 2. Periodic Sampling Audit

In contrast with "whole" checking, random "sampling" checking greatly reduces the workload of audit services, while still achieves an effective detection of misbehaviors. Thus, a probabilistic audit on sampling checking is preferable to realize the anomaly detection in a timely manner, as well as to rationally allocate resources. Generally, this algorithm relies on homomorphic properties to aggregate data and tags into a constant-size response, which minimizes network communication costs. Since the single sampling checking may overlook a small number of data abnormalities, we propose a periodic sampling approach to audit outsourced data, which is named as Periodic Sampling Audit. With this approach, the audit activities are efficiently scheduled in an audit period, and a TPA merely needs to access small portions of files to perform audit in each activity. Therefore, this method can detect exceptions periodically, and reduce the sampling numbers in each audit (Fig.2.2).

V. 3. Audit For Dynamic Operations

To ensure the security, dynamic data operations are available only to DOs or AAs, who hold the secret key . Here, all operations are based on data blocks. Moreover, to implement audit services, applications need to update the IHTs. It is necessary for TPA and CSP to check the validity of updated data. First, an AA obtains the public verification information from TPA. Second, the application invokes the Update, Delete, and Insert algorithms, and then sends to TPA and CSP, respectively. Next, the CSP makes use of an algorithm check to verify the validity of updated data. Note that the Check algorithm is important to ensure the effectiveness of the audit. Finally, TPA modifies audit records after the confirmation message from CSP is received and the completeness of records is checked (Fig 2.3).

V. 4. Anomaly Detection

For every available tag generation and a random challenge, the protocol always passes the verification test and to protect the confidentiality of the checked data, we are more concerned about the leakage of private information in public verification process. It is obvious that enormous audit activities would increase the computation and communication overheads of our audit service. However, the less frequent activities may not detect anomalies in a timely manner. Hence, the scheduling of audit activities is significant for improving the quality of audit services. To detect anomalies in a low-overhead and timely manner, we attempt to optimize the audit performance from two aspects: Performance evaluation of probabilistic queries and scheduling of periodic verification. Our basic idea is to maintain a tradeoff between overhead and accuracy, which helps us improve the performance of audit systems.

In general, the AAs should be cloud application services inside clouds for various application purposes, but they must be specifically authorized by DOs for manipulating outsourced data. Since the acceptable operations require that the AAs must present authentication information for TPA, any unauthorized modifications for data will be detected in audit processes or verification processes. Based on this kind of strong

authorization-verification mechanism, we assume neither CSP is trusted to guarantee the security of stored data, nor a DO has the capability to collect the evidence of CSP's faults after errors have been found.

The ultimate goal of this audit infrastructure is to enhance the credibility of CSSs, but not to increase DO's burden. Therefore, TPA should be constructed in clouds and maintained by a CSP. To ensure the trust and security, TPA must be secure enough to resist malicious attacks, and it should be strictly controlled to prevent unauthorized accesses even for internal members in clouds. A more practical way is that TPA in clouds should be mandated by a trusted third party (TTP) . This mechanism not only improves the performance of an audit service, but also provides the DO with a maximum access transparency. This means that DOs are entitled to utilize the audit service without additional costs.

VI. Conclusion

In this paper, I presented a construction of dynamic audit services for untrusted and outsourced storages. We also presented an efficient method for periodic sampling audit to enhance the performance of TPAs and storage service providers. Our experiments showed that our solution has a small, constant amount of overhead, which minimizes computation and communication costs.

Acknowledgements

I would like to take this opportunity for expressing our profound gratitude and deep regards to Mr. P. Senthil Kumar (Head of the Department, Computer Science and Engineering, Sapthagiri College of Engineering), Mr. P.V Sankar Ganesh(PG Coordinator, Computer Science and Engineering, Sapthagiri College of Engineering) and all teaching and non-teaching staffs of the department of Computer Science and Engineering, Sapthagiri College of Engineering, Dharmapuri, Tamil Nadu, for their guidance, monitoring and constant encouragement throughout the preparation of this paper.

References

[1]. M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009..
[2]. A.A. Yavuz and P. Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proc. Ann.Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009.
[3]. H.-C. Hsiao, Y.-H. Lin, A. Studer, C. Studer, K.-H. Wang, H.Kikuchi, A. Perrig, H.-M. Sun, and B.-Y. Yang, "A Study of User-Friendly Hash Comparison Schemes," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 105-114, 2009.
[4]. A.R. Yumerefendi and J.S. Chase, "Strong Accountability for Network Storage," Proc. Sixth USENIX Conf. File and Storage Technologies (FAST), pp. 77-92, 2007.
[5]. Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S.S. Yau, "Efficient Provable Data Possession for Hybrid Clouds," Proc. 17th ACM Conf. Computer and Comm. Security, pp. 756-758, 2010.
[6]. A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Communications Security (CCS '07), pp. 584-597, 2007.
[7]. G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untruste Stores," Proc. 14th ACM Conf. Computer and Comm.Security, pp. 598-609, 2007.
[8]. M. Xie, H. Wang, J. Yin, and X. Meng, "Integrity Auditing of Outsourced Data," Proc. 33rd Int'l Conf. Very Large Databases (VLDB), pp. 782-793, 2007.
[9]. C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 1-9, 2010.

Author Details

Anuraj C.K received his B-Tech Degree in Computer Science and Engineering in 2011 from Adi Shankara Institute of Engineering and Technology, Kalady affiliated to Mahatma Gandhi University, Kottayam. He completed his M.E research in the area of Cloud Storage Security in the Department of Computer Science and Engineering, Sapthagiri College of Engineering, Dharmapuri, affiliated to Anna University, Chennai. His area of interests include Cloud Computing, Storage Security, Network Security, Internet Computing Computer Graphics, Operating Systems and Neural Network.