International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

Secure Public Auditing With Dynamic Structure for Cloud Data

Aswathy K A[1]

[1]*Department of Computer science and engineering, Thejus Engineering College, Vellarakkad, Thrissur, Kerala, India*

Abstract– *With cloud computing, data owners can outsource their data to the cloud servers and retrieve the data files when necessary. There are several security challenges introduced on the outsourced data if it not kept securely. It May destroy confidentiality, integrity, and availability of data. Hence data owners need to verify the correctness of data on cloud storage. Here proposing a secure and efficient public auditing method for outsourced data on cloud. It performs global and sampling verification along with batch auditing. It also supports the dynamic behavior of cloud data efficiently. The dynamic structure introduced in this method consist a doubly linked info table and location array. This dynamic structure helps to reduce the communication and computational overhead.*

Key Words: **auditing protocol, batch auditing, cloud storage.**

1. INTRODUCTION

One of the important service of cloud computing is cloud storage. It helps data owners to store their data to the cloud and retrieve them from cloud when necessary. However, this hosting service introduces new security challenges. The outsourced data may suffer several internal and external attacks. Sometimes illegal behaviour of cloud service provider breaches the security of cloud data. Therefor owners need to verify the correctness of their data on cloud to ensure that their data is secure. Hence, to check the integrity of data in the cloud some auditing protocols are designed. It helps the data owners to verify whether their data are stored securely on cloud. For an efficient verification of cloud data a trustworthy third party called Third Party Auditor (TPA) was introduced, which receives the auditing request from the data owner and executes it.

Once the data is outsourced to the cloud, it may change during the whole period of cloud. Due to this dynamic nature of cloud data, auditing protocol need to support data dynamics of cloud data. Several auditing protocols with dynamic support are researched, but some existing protocols are too expensive and some of them have low efficiency in supporting data dynamics. There for design of an efficient protocol is necessary. Here introduce a public auditing with dynamic structure composed of doubly linked info table and location array; it makes the verification process more effective.

1.1 Contribution of this protocol

Introduce an efficient and secure public auditing protocol with doubly linked info table and location array for outsourced data in the cloud. The main contribution of this protocol is as follows.

1) Global and sampling verification: provide mutual trust between data owner and cloud service provider.
2) Data dynamic support with dynamic structure : consist doubly linked info table and location array. It maintain mapping between blocks and their specific location.
3) Various auditing properties: Public auditing, Batch auditing.

The above contributions provide better performance with effective communication overhead.

1.2 Related Works

Many protocols have been designed for data auditing in cloud and can be divided into private and public protocols. Only the DO and CSP participate in the private protocol [1],[2],[3]. Here the entire auditing is performed by the owner hence it increase the burden on DO. To overcome this problem a trustworthy third party TPA is introduced. First public auditing is proposed by Ateniese et al. in 2007 [4].after that More Public Auditing Protocols Was Designed. Wang et al. [5] discover that the auditing in [4] leak data information. Hence in 2013 auditing protocol [5] was designed.it introduce holomorphic linear authenticator (HLA) and random masking technique. Later, Worku et al. [6] suggested that the auditing in [5] could not preserve privacy of signers. Therefor Worku et al. introduce ring signature for verify data integrity. It preserves privacy of signers.

To support the dynamics of cloud data Atenies et al. [7] in 2008 propose PDP (Partially dynamic Provable Data Possession) based auditing protocol. Later Erway et al. [8] extend [7] to support fully dynamic storage by employing a skip list. And Wang et al. [9] use a Merkle Hash Tree to support full data dynamics. Due to both of this schemes have

large communication cost, in 2003 Zhu et al. [10] design a protocol with an index-hash table, which require lower communication and computation cost. In this method insertion and deletion are inefficient. To overcome this problem Tian et al. [11] propose an auditing protocol with DHT (Dynamic Hash Table) and Jian et al. [12] designed a protocol with index switcher, both of which were cause significant extra cost. Inspired by [11], this paper design an efficient public auditing protocol with dynamic structure composed of doubly linked info table and location array.

2. METHODOLOGY

2.1 System Model

As shown in Fig 1, the system model consist three entities: DO,CSP and TPA.

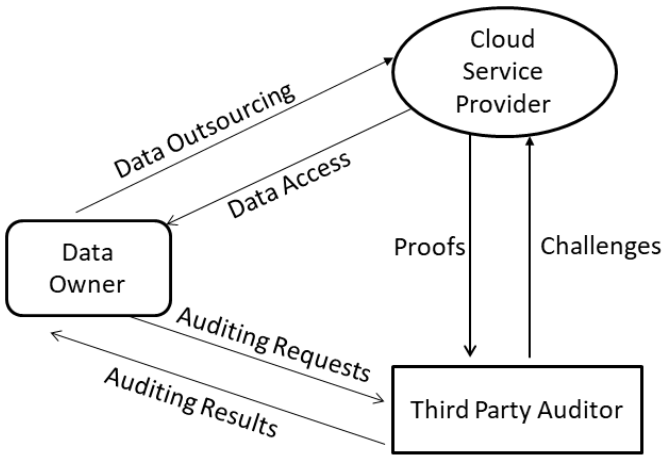

Fig 1: System Model

The data owners encrypt their data and outsource to the cloud. The cloud service provider stores owner's data and provides the data access to users when they required. TPA is a trustworthy third party. It provides convincing auditing results for both the owners and servers.

2.1 The Proposed System

The proposed dynamic structure is composed of doubly linked info table and location array.

Doubly Linked Info Table: It is a two-dimensional data structure used by the TPA to store the data information. This data information is divided into file information and block information. In the Fig 2 the left part represents the file information, include the user ID and file ID (ID_u,ID_f). The right part represents the block information, include the version number and time stamp (V_{un},$T_{u,f,n}$) of each data block In DLIT, file information and block information are doubly linked. This DLIT helps to locate a certain block more quickly. Therefor it reduce the cost for searching a certain element.

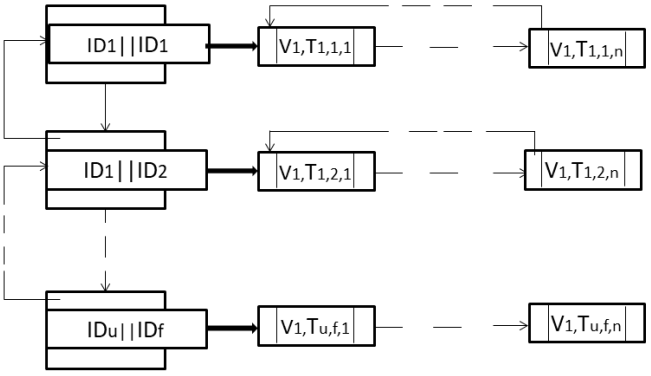

Fig 2: The doubly linked info table

Location Array: The location array maintain the relation between blocks and their specific location. it looks like a common array.

$$\begin{matrix} A_{1,1} & A_{1,2} & A_{1,3} & A_{1,4} & \dots \\ A_{2,1} & A_{2,2} & A_{2,3} & A_{2,4} & \dots \\ A_{3,1} & A_{3,2} & A_{3,3} & A_{3,4} & \dots \\ \dots & \dots & & & \end{matrix}$$

Fig 3: Location Array

Here the index $A_{x,y}$ indicate the y-th block of the x-th file.

2.1 The proposed Protocol

The proposed auditing protocol divided into setup phase and auditing phase. The following are the details of these two phases:

1) *Setup phase:*-In this phase the DO made some preparations for system setup by using three algorithms: KeyGen, Filepro2C and the Filepro2T.

a) KeyGen: Generate public and secret key.

b) Filepro2C: pre-processing the files that are outsourced to the cloud.

c) Filepro2T: It preprocess the information to be stored in the TPA.

2) *Verify Phase*: This phase performs data verification with the help of three algorithms:

a) ChalGen: TPA runs chalgen algorithm to launch the challenge to the CSP.

b) ProofGen: This algorithm is run by the CSP to generate the proof for the received challenges, from the TPA. After the execution of ProfGen, the result is sent back to TPA.

c) VerifyProof: It checks the correctness of proof returned from the CSP.

Global and Sampling Verification: The verify phase includes global and sampling verification. The common verification process in the existing technology represents the sampling verification. Auditor irregularly conducts the sampling verification to check the correctness and completeness of cloud data. In global verification the verification process is performed at the moment that the data file is uploaded or updated in the cloud.

Batch Auditing: Batch Auditing allows the TPA to handle multiple auditing delegations from the various data owners simultaneously.

3. CONCLUSIONS

This paper proposes a public auditing protocol with a dynamic structure composed of doubly linked info table and location array. This protocol provide better performance in terms of efficient dynamic support and reduced overhead with the help of doubly linked info table and location array. Moreover, some auditing properties such as public auditing and batch auditing are supported by this protocol. Extensive numerical analysis, experimental comparison results are used to validate the performance of our protocol by making it more effective and convincing.

REFERENCES

[1] A. Juels and B. S. Kaliski, "Pors: proofs of retrievability for large files,"in ACM Conference on Computer and Communications Security, 2007, pp. 584–597.

[2] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy-preserving audit and extraction of digital contents." Pasos Revista De Turismo Y Patrimonio Cultural, vol. 2008, pp. 477–494, 2008.

[3] F. Seb, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J. J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," IEEE Transactions on Knowledge and Data Engineering, vol. 20, no. 8, pp. 1034–1038, 2007.

[4] G.Ateniese, R.Burns,R. Curtmola,J. Herring, L.Kissner, Z.Peterson, and D. Song, "Provable data possession at untrusted stores," in ACM Conference on Computer and Communications Security, 2007, pp. 598–609.

[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacypreserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 2009, no. 2, pp. 362–375, 2013.

[6] S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy-preserving public auditing scheme for cloud storage," Computers and Electrical Engineering, vol. 40, no. 5, pp. 1703–1713, 2014.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and efficient provable data possession." in Proceedings of the 4th international conference on Security and privacy in communication networks, 2008, pp. 1–10.

[8] C. C. Erway, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," Acm Transactions on Information and System Security, vol. 17, no. 4, pp. 213–222, 2009.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, 2011.

[10] Y. Zhu, G. J. Ahn, H. Hu, S. S. Yau, H. G. An, and C. J. Hu, "Dynamic audit services for outsourced storages in clouds," IEEE Transactions on Services Computing, vol. 6, no. 99, pp. 227–238, 2013.

[11] H. Tian, Y. Chen, C. C. Chang, H. Jiang, Y. Huang, Y. Chen, and J. Liu," Dynamic-hash-table based public auditing for secure cloud storage," IEEE Transactions on Services Computing, pp. 1–1, 2016.

[12] H. Jin, H. Jiang, and K. Zhou, "Dynamic and public auditing with fair arbitration for cloud data," IEEE Transactions on Cloud Computing, pp. 1–1, 2016.