AN EFFICIENT DYNAMIC AND PUBLIC AUDITING WITH SECURE SEARCHABLE DATA IN CLOUD STORAGE

[1] **Noor Unnisa Begum | [2]Amtul Shanaz | [3]Dr. Syed Raziuddin,**
[1]PG Scholar, [2]Assistant Professor, [3]Professor and Head of Dept, [1,2,3]Dept of CSE
[1]noorunnisa984@gmail.com, [2]amtulshanaz@deccancollege.ac.in, [3]hod_cse@deccancollege.ac.in
[1, 2, 3] DECCAN COLLEGE OF ENGINEETING & TECHNOLOGY Darussalam, Aghapura, Hyderabad, Telangana –India

Abstract

Data Outsourcing has become a rising trend with the advent of the cloud computing and hence promoting the remote data auditing schemes to be appeared in the research. Besides this the research considers the problem of data dynamics support, public verifiability and dispute arbitration simultaneously. This paper proposes an efficient dynamic and Public auditing scheme for checking and verifying the integrity of the file uploaded by Data Owner in the cloud provide data dynamic support. Moreover, this scheme provides fairness arbitration of potential disputes between the data owner and the Cloud Service provider by Third Party Arbitrator (TPAR). The system is extended by implementing the secure search operations on the files in cloud by any user. We assume a single-writer and many readers in our scheme.

Keywords:
Third Party Auditor (TPAU), CSP, Third Party Arbitrator (TPAR), integrity auditing, fairness arbitration, dynamic update, secure search operation

I. INTRODUCTION

Data auditing schemes allow the cloud users to check the integrity of their remotely stored data without downloading them locally, which is termed as blockless verification. It allow the data owners to periodically interact with the CSP through auditing protocols to check the correctness of their outsourced data by verifying the integrity proof computed by the CSP. It offers stronger confidence in data security because of user's own conclusion that data is intact is much more convincing than that from service providers. In general, there are several trends in the development of auditing schemes. Firstly, earlier auditing schemes usually require the CSP to generate a deterministic proof by accessing the whole data file to perform integrity check, e.g., schemes in [2], [3] use the entire file to

perform modular exponentiations. Such plain solutions incur expensive computation overhead at the server side, hence they lack efficiency and practicality when dealing with large-size data. Secondly, some auditing schemes provide private verifiability that require only the data owner who has the private key to perform the auditing task, which may potentially overburden the owner due to its limited computation capability. Thirdly, PDP[5] and PoR[4] techniques intend to audit static data that are seldom updated, so these schemes do not provide data dynamics support. Data update is a very common requirement for cloud applications. If auditing schemes could only deal with static data, their practicability and scalability will be limited.

Ateniese el al. [5] was the first to proposed public verifiability in data auditing schemes. In contrast, public auditing schemes in [6], [7] allow anyone who has the public key to perform the auditing, which makes it possible for the auditing task to be delegated to an external third party auditor (TPA). A TPA can perform the integrity check on behalf of the data owner and honestly report the auditing result to him [8].To my knowledge, only schemes in [7], [10], [11] provide built-in support for fully data dynamic operations (i.e., modification, insertion and

deletion of file blocks), but they are insufficient in providing data dynamics support, public verifiability and auditing efficiency simultaneously together in one scheme. From these trends, it can be seen that providing probabilistic proof, public verifiability and data dynamics support are three most crucial characteristics in auditing schemes. Among them, providing data dynamics support is the most challenging. Moreover, in a public auditing scenario, a data owner always delegates his auditing tasks to a TPA who is trusted by the owner but not necessarily by the cloud. Current research usually assumes an honest data owner in their security models, which has an inborn inclination toward cloud users. However,, not only the CSP, but also data owners, have the motive to engage in deceitful behaviors. For example, a malicious data owner may intentionally claim data corruption against an honest cloud for a money compensation, and a dishonest CSP may delete rarely accessed data to save storage or hides data loss to maintain reputation.

Therefore, it is of critical importance for a data auditing scheme to provide fairness guarantee to settle potential disputes between the two parties. Zheng et al. [11] proposed a fair PoR scheme to prevent a dishonest client from accusing an honest CSP, but their scheme only realizes private auditing. Kupccu [12] proposed general arbitration protocols with automated payments using fair signature exchange protocols.Thus, we are combining efficient data dynamics support , fair dispute arbitration and secure search operation into a single auditing scheme. To solve the fairness problem i.e, potential disputes in auditing, we introduce an entity called third-party arbitrator (TPAR), which is a professional institute for conflicts arbitration and is trusted by both data owners and the CSP. Since a TPAU can be viewed as a delegator of the data owner and is not necessarily trusted by the CSP, we differentiate between the roles of auditor and arbitrator. Hence, this paper proposes a new auditing scheme to address the problems of data dynamics support, public verifiability ,dispute arbitration and secure search operation simultaneously.

Our contributions mainly lie in:

- We are solving the data dynamics problem in auditing by introducing an index switcher to keep a mapping between block indices and tag indices.
- We provide dispute arbitration between the data owner and the CSP, which is of great significance and practicality for cloud data auditing, since most existing schemes generally assume an honest data owner in their threat models. Thus, we will provide fairness guarantee and dispute arbitration in our scheme, which ensures that both the data owner and the CSP cannot misbehave in the auditing process otherwise the TPAR finds out the cheating party.
- We provide secure search operation that allow the users to access and download multiple files from the cloud that are being activated by the TPAR in a secure manner.

The rest of the paper is organized as follows. Section 2 consists of surveys the related work. In Section 3 we introduce the scheme description, system model, and our design goals. In Section 4, we elaborate on the implementation of our dynamic auditing scheme and arbitration protocols. Further, we present the Experiment Results in Section 5. Finally, Section 6 concludes the paper.

II. RELATED WORK

To provide the data Integrity auditing different schemes were provided some of them are:

C.Erway,A.Kupcu, and R.Tamassiaand Illinois [10] For maintaining the integrity for static files they proposed the provable data possession technique. In this technique the client preprocess the data and then sends it to an untrusted server for storage, while keeping small amount of meta data. Client later asks the server to prove that the stored data has not been tampered or deleted. When the dynamic files are considered the dynamic provable data possession (DPDP) was proposed where the data integrity is maintained by the rank information which is used to organize the dictionaries information. By using this scheme it is helpful for practical cloud computing systems for file storage, database services, and peer-to-peer storage. The rank-based authenticated dictionary is constructed using the RSA tree with improved error detection probability but higher server computation.

C.Wang, Q.Wang,K.Ren, and W.Lou [14] They presented public auditing scheme which provides a complete outsourcing solution of data and also provides its integrity checking. 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, especially for users with constrained computing resources. 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.

J.Yuan and S.Yu [16] They stated a proof of retrievability (POR) is a compact proof by a file system (prover) to a client (verifier) that a target file F is intact, in the sense that the client can fully recover it. As PORs incur lower communication complexity than transmission of itself, they are an attractive building block for high-assurance remote storage systems. This technique enables individuals and organizations to verify the integrity of their outsourced data on an untrusted server (e.g., public cloud storage platform). While existing POR schemes have focused on various practical issues, they still have limitations either the communication cost is linear to the number of elements in a data block, or the public verifiability is not supported. Such limitations cause these POR schemes to suffer from a severe scalability issue in terms of data file size or user number for practical use.

Metadata key Generation: Let the verifier V needs to the store the file F. Let this file F contains n file blocks. We tend to at the start preprocess the file and make metadata to be appended to the file. Let every data of the n data blocks have m bits in them. A typical file F that has the user needs to store within the cloud. Each of the Meta data from {the data, the info , the information} blocks mi is encrypted by using a appropriate algorithm to provide a new changed Meta data Mi while not loss of generality. This concatenated Meta data should be appended to the file F before storing it at the cloud server. Then file F together with the appended Meta data with the cloud.

III.SCHEME DESCRIPTION

In existing public auditing schemes [4], [5], [6], [14] mainly focus on the delegation of auditing tasks to a third party auditor (TPA) so that the overhead on clients can be offloaded as much as possible. However, such models have not seriously considered the fairness problem as they usually assume an honest owner against an untrusted CSP. Since the TPA acts on behalf of the owner, then how could the CSP trust the auditing result? What if the owner and TPA collude together against an honest CSP for a financial compensation? In this sense, such models reduce the practicality and applicability of auditing schemes. In the cloud scenario, both the data owners and the CSP have the motive to cheat. The CSP makes profit by selling its storage capacity to cloud users, so he has the motive to reclaim sold storage by deleting rarely or never accessed data, or may even hides the data loss accidents to maintain the reputation. Here, we assume the CSP as semi-trusted, namely, the CSP behaves properly as prescribed contract most of the time, but he may also try to pass the integrity check without possessing correct data. On the other hand, the data owner also has the motive to cheat or falsely accuse an honest CSP, e.g., a malicious owner intentionally claims data corruption despite the fact to the contrary so that he can get a compensation from the CSP. Therefore, disputes between the two parties are unavoidable to a certain degree. So an arbitrator for dispute settlement is required for the fair and dynamic auditing scheme. We extend the threat model in existing public schemes by differentiating between the auditor (TPAU) and the arbitrator (TPAR) and putting different trust assumptions on them. Since the TPAU is mainly a delegated party to check client's data integrity, and the potential dispute may occur between the TPAU and the CSP, so the arbitrator should be an unbiased third party who is different to the TPAU. As for the TPAR, we consider it honest-but-curious. It behave honestly most of the time but it is also curious about the content of the auditing data.

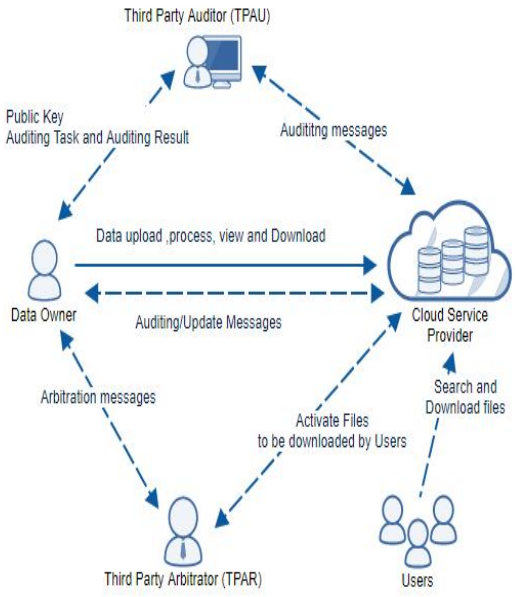

Fig 1. Proposed System Architecture

As illustrated in Fig. 1, the system model involves five different entities:

1. The data owner, who has a large amount of data to be stored in the cloud, and can dynamically update his data (e.g., insert, delete or modify a data block) in the future.

1.The cloud service provider (CSP), who has massive storage space and computing power that users do not possess, stores and manages user's data and related metadata.

2.The third party auditor (TPAU) is a public verifier with expertise and capabilities for auditing, and is trusted and payed by the data owner (but not necessarily trusted by the CSP) to verify the integrity of the owner's remotely stored data.

3.The third party arbitrator (TPAR), is an entity for potential conflict arbitration and trusted by both the owner and the CSP, and is different to the role of TPAU.

4.Users, who can search and download multiple files at a time from the cloud with the owner's permission in secure fashion .Only the files activated by the TPAR can be available to download.

Data Owner rely on the CSP for data storage and maintenance, and they may access and update their data. To alleviate their burden, cloud users can delegate auditing tasks to the TPAU, who periodically performs the auditing and honestly reports the result to users. For potential disputes between the data owner, auditor and the CSP, the TPAR can fairlysettle the disputes on proof verification or data update.

IV.EXPERIMENTAL RESULTS

This project is developed using C# language on a Windows system equipped with processor as Intel(R) Core(TM) i3-3120 CPU running at 2.5GHz and 4GB. The size of the blocks of the data file are equal. For example, if the size of the test data is 9 KB, then it is divided into 3 block size of fragmentation each of size 3 KB.. I measure the performance of the auditing scheme from three aspects: tag/token generation time, proof generation time and proof verification time. For data dynamic update and dispute arbitration, we test the update overhead by inserting, deleting and modifying some blocks.

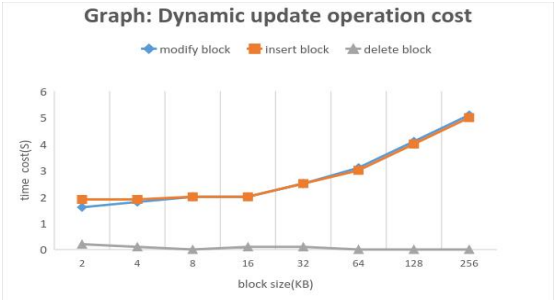

Fig 2: Cost of blocks update Graph

For data dynamics, I test the overhead of inserting, deleting and modifying 1 block and corresponding tag, as illustrated in Fig 2.

The graph in Fig 3 shows how the proposed scheme search algorithm searches multiple files in the same time when compared to Existing schemes where one file can be searched at a time. Since it takes less time to search and hence its performance is better.

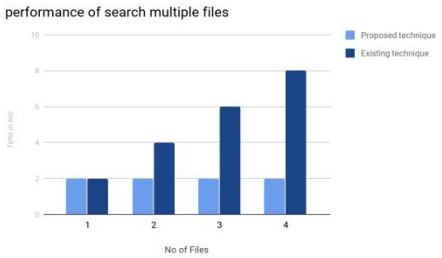

Fig 3: Search File Performance Graph

V.CONCLUSION

In this paper we study the need of a fair and dynamic auditing scheme to prevent a dishonest client accusing an honest CSP. Compared to these schemes, our work is the first to combine public verifiability, data dynamics support and dispute arbitration simultaneously. We also provide secure Search operation to the users to access the files in the cloud. The system can extended by implementing the data dynamics and fair arbitration on groups and on big data in future.

VI.REFERENCES

[1] HaoJin, Hong Jiang, "Dynamic and Public Auditing with Fair Arbitration for Cloud Data" in IEEE TRANSACTIONS ON CLOUD COMPUTING, Vol. 13, No. 9, September 2014.

[2] Y. Deswarte, J.-J.Quisquater, and A. Sa¨ıdane, "Remote integrity checking," in Proc. 5th Working Conf. Integrity and Intl Control in Information Systems, 2004

[3] D.L. GazzoniFilho and P.S.L. M. Barreto, "Demonstrating data possession and uncheatable data transfer." IACR Cryptology ePrint Archive, Report 2006/150, 2006.

[4] A. Juels and B. S. KaliskiJr, "Pors: Proofs of retrievability for large files," in Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), 2007, pp. 584–597.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Computer and Comm. Security (CCS07), 2007.

[6] H.Shacham and B. Waters, "Compact proofs of retrievability," in Proc. 14th Intl Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT 08), 2008, pp. 90–107.

[7] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling public verifiability and data dynamics for storage security in cloud computing," in Proc. 14th European Conf. Research in Computer Security (ESORICS 08), 2009, pp. 355–370.

[7] M. A. Shah, R. Swaminathan, and M. Baker, "Privacy- preserving audit and extraction of digital contents." IACR Cryptology, Report 2008/186, 2008.

[8] C. Wang, K. Ren, W. Lou, and J. Li, "Toward publicly auditable secure cloud data storage services," Network, IEEE, vol. 24, no. 4, pp. 19–24, 2010.

[9] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), 2009, pp. 213–222.

[10] Y. Zhu, H.Wang, Z. Hu, G.-J.Ahn, H. Hu, and S. S. Yau,"Dynamic audit services for integrity verification of outsourced storages in clouds," in Proc. ACM Symp. Applied Computing (SAC 11), 2011, pp. 1550–1557.

[11] Q. Zheng and S. Xu, "Fair and dynamic proofs of retrievability," in Proc. 1st ACM Conf. Data and Application Security and Privacy (CODASPY 11), 2011, pp. 237–248. [12] A. K¨upc¸ ¨u, "Official arbitration with secure cloud storage application," The Computer Journal, pp. 138–169, 2013.

[13] N. Asokan, V. Shoup, and M. Waidner, "Optimistic fair exchange of digital signatures," in Proc. 17th Intl Conf. Theory and Applications of Cryptographic Techniques: Advances in Cryptology(EUROCRYPT98),1998.

[14] C.Wang, Q.Wang, K. Ren, andW. Lou, "Privacy- preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[15] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," IEEE Trans. Computers, vol. 62, no. 2.

[16] "Proofs of retrievability with public verifiability and constant communication cost in cloud", J.Yuan and S.Yu, International workshop on security in cloud computing, may 2013.