International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 3 | ISSN : 2456-3307

Review : Dynamic and Public Auditing with Fair Arbitration for Cloud Data

Amit Kumar Pandey, Prof. Nitin Choudhary

Department of Computer Science and Engineering, Kopal Institute of Science & Technology, Bhopal, Madhya Pradesh, India

ABSTRACT

Now a day's Storage outsourcing became a refresh trend with the arrival of the cloud computing encouraging the secure remote data auditing to be appeared in the research work. Besides, danger models in these plans more often than not manage a fair information holder and centralize on identifying an dishonest cloud specialist organization in spite of the way that customers may likewise make tough..Review paper based on Cloud environment Storage, client can remotely store their information and like the on-demand high standard applications and services from a shared pool of configurable computing resources, without the load of local data storage and maintenance.

Keywords : Third Party Auditor (TPA), Dynamic Auditing; Data integrity; Fairness Protocol

I. INTRODUCTION

Cloud storage inspect is used to verify the integrity of the data stored in public cloud, which is one of the important security techniques in cloud storage. In recent years, auditing protocols for cloud storage have attracted much attention and have been study greatly. These protocols focus on many different sides of auditing, and how to achieve high bandwidth and computation efficiency is one of the essential concerns. Data auditing schemes can enable cloud users to check the integrity of their remotely stored data without downloading them locally, which is named as block less verification. With auditing schemes, users can periodically interact with the CSP through auditing protocols to check the correctness of their outsourced data by showing the integrity proof computed by the CSP, which offers stronger confidence in data security because user's own conclusion that data is whole is much more convincing than that from service providers. Many cloud storage auditing protocols like have been proposed based on this technique. The privacy protection of data is also an important feature of cloud storage auditing. In order to decreases the computational burden of the client, a third-party auditor (TPA) is introduced to help the client to periodically check the integrity of the data in cloud. However, it is possible for the TPA to get the client's data after it executes the auditing protocol multiple times. Auditing protocols are designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how

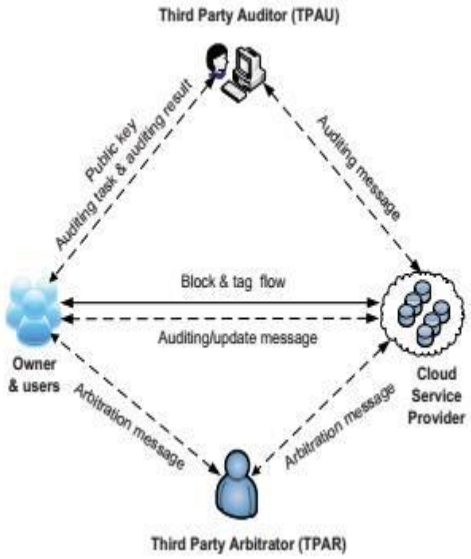

Figure 1. Third party auditor

Enabling public audit ability 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. To securely

introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user.

II. LITERATURE SURVEY

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

Ayad F. Barsoum and M. Anwar Hasan PDP schemes have been presented for multiple copies of static data, by this work it implemented PDP scheme directly dealing with multiple copies of dynamic data. When verifying multiple data copies, the overall system integrity check fails if there is one or more corrupted copies. To address this issue and recognize which copies have been corrupted, a map-based provable multi-copy dynamic data possession (MB-PMDDP) scheme is proposed. This scheme provides an adequate guarantee that the CSP stores all copies that are agreed upon in the service contract. Moreover, the scheme supports outsourcing of dynamic data, i.e., it supports block-level operations such as block modification, insertion, deletion, and append.

J.Yuan and S.Yu 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. Framework for the design of PORs is designed in this scheme. This technique enables individuals and organizations to verify the integrity of their outsourced data on auntrusted 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.

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"Cloud Computing is defined as an environment in which users can share their resources with others in pay per use model. The resources are stored centrally and can access from anywhere. Despite these advantages, there still exist significant issues that need to be considered before shifting into cloud. Security stands as major obstacle in cloud computing. This paper gives an overview of the security issues on data storage along with its possible solutions. It also gives a brief description about the encryption techniques and auditing mechanisms. The National Institute of Standard and Technology's (NIST) defined cloud computing as a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. The NIST has listed five main characteristics of cloud computing.

III. DESCRIPTION

Cloud service providers (CSP) are separate administrative entities; data outsourcing is actually renounce 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.
It has some disadvantaged although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture.

Some Algorithm use in this is: A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof).

IV. CONCLUSION

In this review paper we study the need of a fair and dynamic auditing scheme to prevent a dishonest client accusing an honest CSP. Though many research works about cloud storage auditing have been done in recent years, a critical security problem exposure problem for cloud storage auditing, has remained unexplored in previous researches. While all existing protocols focus on the faults or dishonesty of the cloud, they have overlooked the possible weak sense of security and/or low security settings at the client.

Therefore, how to deal with the client's secret key exposure for cloud storage auditing is a very important problem. Unfortunately, previous auditing protocols did not consider this critical issue, and any exposure of the client's secret auditing key would make most of the existing auditing protocols unable to work correctly. We can propose a system on how to reduce the damage of the clients' key exposure in cloud storage auditing.

V. REFERENCES

[1]. "Provable Multicopy Dynamic Data Possession in Cloud Computing Systems",Ayad F. Barsoum and M. Anwar Hasan, IEEE Transactions On Information Forensics And Security, march 2015.

[2]. "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 .

[3]. 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 Trans. Services Comput. , vol. 6 , no. 2 , pp.227 -238 , 2013

[4]. B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditing for shared data in the cloud," IEEE Trans. Cloud Computing, vol. 2, no. 1, pp. 43–56, 2014

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

[6]. A. K¨upc¸ ¨ u, "Official arbitration with secure cloud storage application," The Computer Journal, pp. 138–169, 2013

[7]. 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 Trans. Services Comput. , vol. 6 , no. 2 , pp.227 -238 , 2013

[8]. 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

[9]. 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

[10]. 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.