A Survey Paper On Privacy Preservation In Clone Cloud Computing

C.S.KULKARNI
Ckulkarni47@gmail.com

SUNIL KENGAR
sunilkengar@gmail.com

TANAJI TORE
tanajitore@gmail.com

VIJAY MASAL
vijay.v.masal@gmail.com

SWAPNIT UBALE
swa23ubale@gmail.com

Abstract--The cloud data service is commonplace for data to be not only stored in the cloud, but also shared across multiple users. In Cloud Computing large computer net- work and number of server data are stored in centralized manner. Several mechanisms have been designed to allow both data owners and public verifiers to audit efficiently cloud data integrity without retrieving the entire data from the cloud server. Public auditing on the integrity of shared data with these existing mecha- nisms will inevitably reveal condential information like identity privacy to public verifiers. We propose a novel privacy-preserving mechanism that supports public auditing on shared data stored in the cloud. We exploit ring signatures to compute verica- tion metadata needed to audit the correctness of shared data. With our mechanism, the identity of the signer on each block in shared data is kept private from public verifiers, who are able to verify efficiently shared data integrity without retrieving the entire file.

Keywords-- Public auditing, privacy-preserving, shared data, cloud computing, cryptographic protocol

I. INTRODUCTION

Cloud Computing, which provides Internet- based service and use of computer technology. This is cheaper and more strong processors, together with the software as a service (SaaS) computing architecture, are transforming data into data centers on huge scale. The increasing network and flexible network connections make it even possible that users can now use high quality services from data and provides remote on data centers. Storing data into the cloud offers great help to users since they don't have to care about the problems of hardware problems. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is avoids the responsibility of local machines for data maintenance at the same time. As a result, users are at the interest of their cloud service providers for the availability and integrity of their data the one hand; although the cloud services are much more powerful and reliable than personal computing devices and broad range of both internal and external threats for data integrity still exist. Examples of outages and data loss incidents of noteworthy cloud storage services appear from time to time. On the other hand, since users may not keep a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Our work is among the first few ones in this field to consider distributed data storage security in Cloud Computing.

II. RELATED WORK

The public auditability in their defined provable data possession model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA based homomorphic non-linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file. However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. Jules teal describe a proof of irretrievability|| model, where spot-checking and error-correcting codes are used to ensure both possession|| and irretrievability|| of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Dodisetal.give a study on different variants of PoR with private auditability. Shachamet al.design an improved PoR scheme built with full proofs of security in the security model defined. Similar to the construction, they use publicly verifiable homomorphism non-linear authenticators that are built from provably secure BLS signatures. Construction, a compact and public verifiable scheme is obtained. Again, their approach does not support privacy preserving auditing for the same reason. The propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. This scheme only works for encrypted files, and it suffers from the auditor state fullness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up.

III. PROBLEM STATEMENT

Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. To securely introduce an effective third party auditor (TPA) the following two fundamental requirements have to be met:

1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user.

2) The third party auditing process should bring in no new vulnerabilities towards user data privacy.

IV. MOTIVATION

1) We motivate the public auditing system of datastorage security in Cloud Computing and provide a privacy-preserving auditing protocol, i.e., our scheme enables an external auditor to audit user's outsourced data in the cloud without learning the data content.

2) To the best of our knowledge, our scheme is the first to support scalable and efficient public auditing in the Cloud Computing. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA.

3) We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

V. OBJECTIVE

1. Storing of user data in the cloud despite its advantages has many interesting Security concerns which needs to be extensively investigated for making it reliable solution to the problems in local storage of data.

2. The main problem with cloud storage is securities of information as the cloud server we use are the third party. So we need to use the encryption algorithm which will give security to our data. We also need to keep some auditor who will take care of data integrity by monitoring the data.

3. We are compressing the data using algorithm for Data optimization. Algorithm works by manipulate bits of data to reduce the size and optimize input.

VI. PROPOSED SYSTEM

In this paper, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We are encrypt the data using RSA algorithm cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key that cannot be restored. Only the user knows the key, the clouds do not know the key. Also, because the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage.

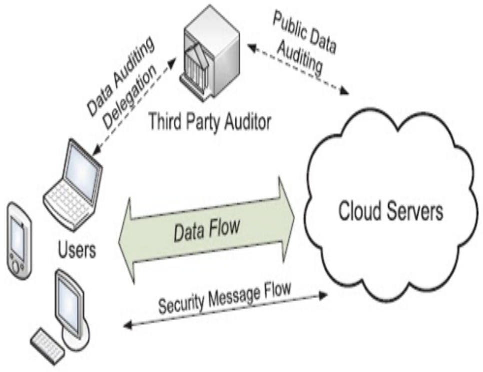

Fig. 1. The architecture of cloud data storage service.

VII. FUTURE SCOPE

With the establishment of privacy-preserving public auditing in cloud computing, TPA may concurrently handle multiple auditing delegations upon different user's requests. The individual auditing of these tasks for TPA can be tedious and inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also reduces the computation cost on TPA side.

VIII. CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in guarantee that the TPA would not learn any knowledge about the data.

VIII. References

[1] P.mell and T.Grance, “” Draft NIST working definition of cloud computing,” Referenced on june 3rd 2009 Online at http://csrc.nist.gov/ groups/SNS/cloud computing/index html 2009.

[2]Q.wang,C.wang.j.li,K.Ren,and W.lou,”Enable public verifiability and data dynamics for storage security in cloud computing”.

[3]B.wang.B.LI and H.Li,” Oruta : Privacy Preserving Public Auditing for Shared Data in the Cloud”, IEE transactions on cloud computing,vol.2,no. 1,janurary-march 2014

[4]S.Archana,Anathi J,”Privacy –Preservation and public auditing for cloud Data – A Survey”,International Journal of Science and Research(IJSR), Vol.3,No.10,October 2014,pp-1989-1992

[5] K. Ren , C. Wang, and Q. Wang “Security Challenges for the Public Cloud,” IEEE Internet Computing, vol.16,no.1,pp.69-73,2012.