ISSN:0975-9646

Survey on Secure Public Auditing and Privacy Preserving in Cloud

Madhumati B.Shinde[1], S. B. Sonkamble [2]

[1] PG Scholar, [2] Professors, Department Of Computer Engineering, Savitribai Phule Pune University.
Rajarshi Shahu School of Engineering and Research Narhe, Pune-India.

***Abstract*— Cloud computing has become a popular buzzword; it has been widely used to refer to different technologies, services, and concepts. The most evident benefit from the use of cloud computing systems and technologies is the increased economical return due to the reduced maintenance costs and operational costs related to IT software and infrastructure. 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. This new paradigm of data hosting service also introduces new security challenges, which requires an independent auditing service to check the data integrity in the cloud. In this paper we are review an efficient auditing scheme to check the integrity of the outsourced data known as TPA.The TPA can perform audits for multiple users simultaneously & efficiently.**

***Keywords*— Data storage, privacy preserving, public auditability, cloud computing, cloud service provider (CSP)**

I. Introduction

Cloud computing can be defined as a new style of computing in which dynamically scalable and often virtualized resources are provided as a services over the Internet. Cloud computing has become a significant technology trend, and many experts expect that cloud computing will reshape information technology (IT) processes and the IT marketplace. Cloud computing can be viewed as a collection of services, which can be presented as a layered cloud computing architecture.services offered through cloud computing usually include IT services referred as

1.Software As a Service(SaaS)

A SaaS allows users to run pplications remotely from the cloud.

2. Platform-as-a-Service (PaaS)

In the PaaS model, cloud providers deliver a computing platform, typically including operating system, programming language execution environment, database, and web server. 3.Infrastructure-as-a-service (IaaS)

Refers to computing resources as a service. This includes virtualized computers with guaranteed processing power and reserved bandwidth for storage and Internet access.

Popularity of cloud computing comes with various advantages like on-demand self service provisioning. Even these advantages are more appealing to reduce the cost on IT

expenditure & relief the user online burden of data storage they brings new and challenging security threats toward users' outsourced data[1]. Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually relinquishing 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 [1]. Second, there do exist various motivations for CSP to behave unfaithfully toward the cloud users regarding their outsourced data status.

Public Auditing:

Public auditing is the service which is used to ensure integrity of the data stored on the cloud and save the cloud users' computation resources.To perform the auditing task the TPA known as third party auditor used to audit the stored data on cloud .TPA verify the correctness of the cloud data on demand without retrieving a copy of the whole data.The TPA, has expertise and capabilities that can periodically check the integrity of all the data stored which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud.

II. Literature Survey

Literature survey is the most important step in software development process. Use of privacy-preserving public auditing mechanism, and cryptographic scheme can increase the security level [2] for the data that are stored on the cloud servers Following is the literature survey of some existing technique for cloud security.

A. Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing[4].

Cloud Computing has been envisioned as the next-generation architecture of IT Enterprise. It moves the application software and databases to the centralized large data centers, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud is indeed intact, which can be important in achieving economies of scale for Cloud Computing. The support for data dynamics via the most general forms of data operation, such as block modification, insertion and deletion, is also a significant step toward practicality, since services in Cloud Computing are not limited to archive or backup data only. While prior works on ensuring remote data integrity often lacks the support of either public auditability or dynamic data operations, this paper achieves both. We first identify the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two salient features in our protocol design. In particular, to achieve efficient data dynamics, we can improve the existing proof of storage models by manipulating the classic (MHT) Merkle Hash Tree construction for block tag authentication. To support efficient handling of multiple auditing tasks, we can further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis show that the proposed schemes are highly efficient and provably secure.

B. Privacy-Preserving Public Auditing for Secure Cloud Storage [2][3].

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. In this paper, author propose a secure cloud storage system supporting privacy-preserving public auditing .We can further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently.

C. PORs: Proofs of Retrievability for Large Files[5].

In this paper, we define and explore proofs of retrievability (POR). A POR scheme enables an archive or back-up service (prover) to produce a concise proof that a user (verifier) can retrieve a target file F, that is, that the archive retains and reliably transmits file data sufficient for the user to recover F in its entirety. A POR may be viewed as a kind of cryptographic proof of knowledge (POK), but one specially designed to handle a large file (or bitstring) F. We explore POR protocols here in which the communication costs, number of memory accesses for the prover, and storage requirements of the user (verifier) are small parameters essentially independent of the length of F. In addition to proposing new, practical POR constructions, we explore implementation considerations and optimizations that bear on previously explored, related schemes. In a POR, unlike a POK, neither the prover nor the verifier need actually have knowledge of F. PORs give rise to a new and unusual security definition whose formulation is another contribution of our work. We view PORs as an important tool for semi-trusted online archives. Existing cryptographic techniques help users ensure the privacy and integrity of files they retrieve. It is also natural, however, for users to want to verify that archives do not delete or modify files prior to retrieval. The goal of a POR is to accomplish these checks without users having to download the files themselves. A POR can also provide quality-of-service guarantees, i.e., show that a file is retrievable within a certain time bound.

D. Scalable and Efficient Provable Data Possession[7].

In this paper author introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs. The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. To support the dynamic auditing, Ateniese et al. developed a dynamic provable data possession protocol based on cryptographic hash function and symmetric key encryption. Their idea is to precompute a certain number of metadata during the setup period, so that the number of updates and challenges is limited and fixed beforehand. The author construct a highly efficient and provably secure PDP technique based entirely on symmetric key cryptography, while not requiring any bulk encryption. Also, in contrast with its predecessors, this PDP techniqueallows outsourcing of dynamic data, i.e, it efficiently supports operations, such as block modification, deletion and append.

E. Towards Secure and Dependable Storage Services in Cloud Computing[8].

In this paper, author has propose an effective and flexible distributed storage verification scheme with explicit dynamic data support to ensure the correctness and availability of users' data in the cloud. They rely on erasure correcting code in the file distribution preparation to provide redundancies and guarantee the data dependability against Byzantine servers, where a storage server may fail in arbitrary ways. This construction drastically reduces the communication and storage overhead as compared to the traditional replication based file distri-bution techniques. By utilizing the homomorphic token with distributed verification of erasure coded data, their scheme achieves the storage correctness insurance as well as data error localization: whenever data corruption has been detected during the storage correctness verification, this scheme can almost guarantee the simultaneous localization of data errors, i.e., the identification of the misbehaving server(s). In order to strike a good balance between error resilience and data dynamics, their work further explore the algebraic property of our token computation and erasure coded data, and demonstrate how to efficiently support dynamic operation on data blocks, while maintaining the same level of storage correctness assurance. In order to save the time, computation re- sources, and even the related online burden of users, extension of the proposed main scheme to support third party auditing, where users can safely delegate the integrity checking tasks to third party auditors and be worry free to use the cloud storage services.

III. SYSTEM ARCHITECTURE

The system architecture of cloud data storage service involving three different entities, as illustrated in Fig. 2

1. Cloud user or client
2. Cloud service provider or cloud storage server
3. Third party auditor

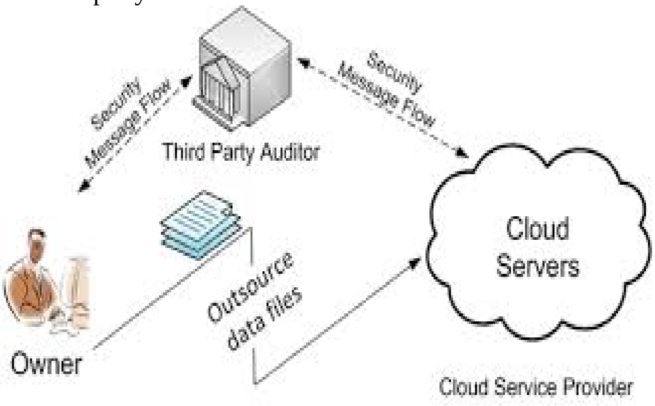

Fig 1.Cloud Storage server architecture

1. Cloud Client/user:
This is the entity which has large amount of data want store on the cloud storage server.

2. Cloud storage server or cloud server(CSS/CS):
The cloud storage server is the location where user store their data. The storage server in cloud maintained by the cloud service provider(CSP).

3. Third party auditor(TPA):
On the behalf of the client TPA is responsible to check the integrity of the user outsourced data in cloud. This is trusted party by the client.

IV. METHODOLOGY

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, and VerifyProof). KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification metadata, which may consist of digital signatures. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof.

Running a public auditing system consists of two phases, Setup and Audit:

1. Setup Phase

The user initializes the public and secret parameters of the system by executing KeyGen, and preprocesses the data file F by using SigGen to generate the verification metadata. The user then stores the data file F and the verification metadata at the cloud server. The user may alter the data file F by performing updates on the stored data in cloud.

2. Audit Phase

The TPA issues an audit message or challenge to the cloud server to make sure that the cloud server has retained the data file F properly at the time of the audit. The cloud server will create a response message by executing GenProof using F and its verification metadata as inputs. The TPA then verifies the response by cloud server via VerifyProof.

V.CONCLUSION

For ensuring security of cloud data storage, it is difficult for enabling a TPA for evaluating the quality of service from an objective and independent point of view. Public audit ability is able to allow clients for delegating the tasks of integrity verification to TPA while they are independently not reliable or cannot commit required resources of computation performing verifications in a continuous manner. One more important concern is the procedure for construction of verification protocols which can be able to accommodate data files that are dynamic. In this paper, the problem of employing simultaneous public audit ability and data dynamics for remote data integrity check in Cloud Computing is explored. The construction is designed for meeting these two main goals but efficiency is set as the main goal. For achieving data dynamics that are effective, the existing proof of storage models is enhanced through manipulation of the construction of classic Merkle Hash Tree for authentication of block tag. For supporting good handling of multiple numbers of auditing tasks, the method of bilinear aggregate signature is further explored for extending the main result into a multiuser setting, where TPA is able to perform multiple auditing tasks in a simultaneous manner. Huge security as well as performance analysis proves that the proposed scheme is efficient and secure to a greater extent.

ACKNOWLEDGEMENT

I sincerely thanks to prof. S. B. Sonkamble for her continuous and constructive support for the work. I would also like to thanks to my friends for their valuable comments.

REFERENCES

1. Cloud Security Alliance, “Top Threats to Cloud Computing,” http://www.cloudsecurityalliance.org, 2010.
2. C. Wang, Q. Wang, K.Ren, and W.Lou, “Privacy Preserving Public Auditing for Storage Security in Cloud Computing”, IEEE INFOCOM’10, March 2010.
3. Cong Wang, Sherman S.M.Chow, Qian Wang, Kui Ren, and Wenjing Lou, “Privacy Preserving Public Auditing for Secure Cloud Storage”, IEEE , Vol.62 , No. 2,February 2013.
4. Qian Wang and Cong Wang and Kui Ren, Wenjing Lou, Jin Li “Enabling Public Auditability And Data Dynamics For Storage Security in Cloud Computing” in IEEE transactions on parallel and distributed systems, 2011, vol. 22, no. 5.
5. A.Juels and J.Burton, S.Kaliski, “PORs: Proof Of Retrieviability for Large Files”, Proc. ACM Conf. Computer and Comm.

Security(CCS'07), pp.584-597, October 2007.

6. H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc. Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (Asiacrypt), vol. 5350, pp. 90-107, Dec. 2008.
7. G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Int'l Conf. Security and Privacy in Comm. Networks (SecureComm '08), pp. 1-10, 2008.
8. C. Wang, Q. Wang, K. Ren, and W. Lou, "Towards Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Service Computing, vol. 5, no. 2, 220-232, Apr.-June 2012.