International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Privacy-Preserving Public Auditing for Secure Cloud Storage

Maragoni Mahendar[1], Malipatel Anusha[2]
[1]Assistanr Professor, Department of CSE, AVANTHI'S scientific of technological & research academy, Hyderabad, Telangana, India
[2]M.Tech Student, Department of CSE, AVANTHI'S scientific of technological & research academy, Hyderabad, Telangana, India

ABSTRACT

Cloud computing is internet based computing which enables sharing of services. Many users place their data in the cloud. However, the fact that users no longer have physical possession of the possibly large size of outsourced data makes the data integrity protection in cloud computing a very challenging and potentially formidable task, especially for users with constrained computing resources and capabilities. So correctness of data and security is a prime concern. This article studies the problem of ensuring the integrity and security of data storage in Cloud Computing. Security in cloud is achieved by signing the data block before sending to the cloud. 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. Thus, 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. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Keyword : Cloud Computing, TPA, Cloud Storage, NIST, PoR scheme, RAM technique, HARS, CSS, Cloud Service Provider

I. INTRODUCTION

CLOUD computing has been envisioned as the next-generation information technology (IT) architecture for enterprises. Cloud computing is extensively developed technology used in business, IT industries which provide services like network access, resources, infrastructure, platform, and rapid resource elasticity as per user require. The user can gain access of services anytime, anywhere on-demand. In cloud computing the data of user is centralized to the cloud storage. Cloud storage is a prototype of networked online storage in which the data is stored in virtualized pools of storage that are generally given by the TPA. NIST definition of cloud computing as: "Cloud computing is a model for enabling convenient, on- demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction".

Many users from remote location use services continuously so there may arise some issues like data security, data integrity, dynamic updates. Every time it is not possible for user to check the data is being

consistent which is stored on cloud storage. So user always wants that cloud server must have to maintain data integrity and privacy. Cloud service providers are the separate entities that store data and provide services to the user. The security and data integrity issues arise due to following reasons:

1. The types of attackers like internal and external and their capability of attacking the cloud.
2. The security risks associated with the cloud, and where relevant considerations of attacks and Countermeasures.
3. Emerging cloud security risks.

Some other issues like lack of training and expertise, unauthorized secondary usage, complexity of regulatory compliance, lack of user control, addressing transborder data flow restrictions, legal uncertainty, compelled disclosure to the government, data accessibility, location of data, transfer and retention, data security and disclosure of breaches. The cloud server stores large amount of data which does not offer guarantee on data integrity and consistency. This problem is addressed and solve by giving public auditing for secure cloud.

II. LITERATURE SURVEY

Ateniese et al. are the first to consider public auditability in their defined "provable data possession" (PDP) model for ensuring possession of files on untrusted storages. In their scheme, utilize RSA based homomorphic tags for auditing outsourced data, thus public auditability is achieved. However, Ateniese et al. do not consider the case of dynamic data storage, and the direct extension of their scheme from static data storage to dynamic case may suffer design and security problems. In their subsequent work, Ateniese et al. propose a dynamic version of the prior PDP scheme. However, the system imposes a priori bound on the number of queries and does not support fully dynamic data operations, i.e., it only allows very basic block operations with limited functionality, and block insertions cannot be supported. In, Wang et al. consider dynamic data storage in a distributed scenario, and the proposed challenge-response protocol can both determine the data correctness and locate possible errors. Similar to, they only consider partial support for dynamic data operation. Juels et al. describe a "proof of retrievability" (PoR) model, where spot-checking and errorcorrecting codes are used to ensure both "possession" and "retrievability" of data files on archive service systems. Specifically, some special blocks called "sentinels" are randomly embedded into the data file F for detection purpose, and F is further encrypted to protect the positions of these special blocks. However, like, the number of queries a client can perform is also a fixed priori, and the introduction of precomputed "sentinels" prevents the development of realizing dynamic data updates.

Shacham et al. design an improved PoR scheme with full proofs of security in the security model defined in. They use publicly verifiable homomorphic authenticators built from BLS signatures, based on which the proofs can be aggregated into a small authenticator value, and public retrievability is achieved. Still, the authors only consider static data files. Erway et al. was the first to explore constructions for dynamic provable data possession.

They extend the PDP model in to support provable updates to stored data files using rank-based authenticated skip lists. The scheme is essentially a fully dynamic version of the PDP solution. To support updates, especially for block insertion, they eliminate the index information in the "tag" computation in Ateniese"s PDP model [6] and employ authenticated skip list data structure to authenticate the tag information of challenged or updated blocks first before the verification procedure.

However, the efficiency of their scheme remains unclear. Shan et al. introduce TPA concept to maintain data integrity and preserve privacy. It reduces online burden and keeps the privacy preserve. Chen et al. gives mechanism for auditing

the correctness of data with multiple server. Frenz et al.introduce a new strategy ,an Oblivious out-sourced storage which is based on Oblivious RAM technique. This idea used to conceal user access pattern and preserve the identity.

III. EXISTING SYSTEM

Although the existing schemes aim at providing integrity verification for different data storage systems, the problem of supporting both public auditability and data dynamics has not been fully addressed. How to achieve a secure and efficient design to seamlessly integrate these two important components for data storage service remains an open challenging task in Cloud Computing.

Proposed System

1. **Client:** an entity, which has large data files to be stored in the cloud and relies on the cloud for data maintenance and computation, can be either individual consumers or organizations.
2. **Cloud Storage Server (CSS):** an entity, which is managed by Cloud Service Provider (CSP), has significant storage space and computation resource to maintain the clients' data.
3. **Third Party Auditor (TPA):** an entity, which has expertise and capabilities that clients do not have, is trusted to assess and expose risk of cloud storage services on behalf of the clients upon request.

Problem Statement

As data integrity and the security is main important thing in cloud, to provide full security and data integrity we are giving public auditing process. Our scheme performs both public auditing and data dynamic operation. For public auditing process we are using here Hashing technique in which hash function is applied on the user's data. The data dynamic performs operation like insert, update, and delete in block wise manner. TPA does the auditing process. Again we extend our concept in which multiple user access cloud storage simultaneously through batch auditing. TPA batch multiple auditing task together and audit at one time. So it reduces the time for auditing process. In our proposed wok we are giving multiple TPA for auditing process. As there are problems like users load ,system crash , system failure at this situation multiple TPA do the auditing process in which if there is failure of one TPA another TPA do the auditing process by taking backup of first TPA. Again we are giving here ring signature concept in which we are using HARS (Homomorphic Authenticable Ring Signature) scheme. In this scheme a group of users can access the CS and they share data in group. Any user in group does the update, delete operations. The system model for our scheme is given below.

A. The System Model:

The system model consist three different entities: the cloud user, the cloud server (CS) and the thirdparty auditor (TPA). As shown in fig. 1.The cloud user is the one who has large amount of data files that are stored in the cloud; the cloud server is the one who provides the data storage service like resources, software to the user. The cloud server is managed by cloud service provider; the third- party auditor is the one who has belief to access the cloud storage service for the benefit of user whenever user request for data access. The TPA has capabilities and competence that the user does not have. They can also interact with cloud server to access the stored data for different purpose in different style. Every time it is not possible for user to check the data which is stored on cloud server that arrives online burden to the user .so that's why to reduce online burden and maintain that integrity cloud

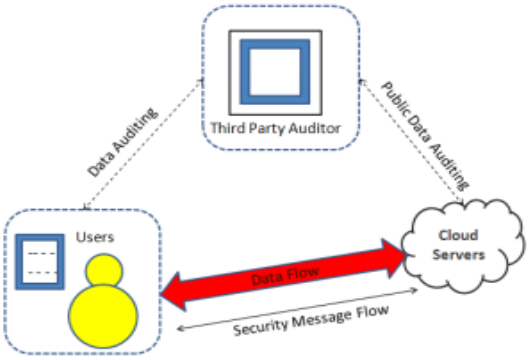

Figure 1. The architecture of cloud data storage.

User may resort to TPA. The data stored on cloud server is come from internal and external attacks, which is having data integrity threads like hardware failure, software bug, hackers, and management errors. The Cloud Server can maintain reputation for its self-serving. The CS might even decide to hide these data correction incidents to user. So that's why here we are giving third-party auditing service for users to gain belief on cloud.

B. Design Goals:

The data integrity and security can be achieved by enabling privacy public auditing for cloud data storage as given below:

1. **Privacy-preserving:** TPA can't see the users data content during the auditing process.
2. **Public Auditability:** To allow TPA to verify the correctness of cloud data without demanding the copy of whole data.
3. **Batch Auditing:** TPA handles multiple users for multiple tasks during auditing process.
4. TPA performs auditing process with minimum communication.
5. **Identity privacy:** The TPA cannot identify the identity of the signer of each block when auditing process going on.

IV. CONCLUSION

Here in this paper, we are given the privacy – preserving public auditing scheme which supports data dynamic operations. Public auditing scheme supports hashing technique. The data dynamic operations can get performed by using Merkle Hash Tree (MHT). We use multiple TPA for the auditing process which handles multiple users through batch auditing. We utilize ring signature for secure cloud storage which ensures that during the auditing process the TPA would not learn any information or knowledge about data content of group stored on cloud server. Ring signature preserves the identity of the signer from the verifier. We use HARS scheme for group of users in which they share data to each other and update and delete data block wise manner.

V. REFERENCES

[1]. C. Wang, Q. Wang, K. Ren, a n d W. Lou, "Privacy- Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM ‟10, Mar. 2010.

[2]. P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloud-computing/index.html, June 2009.

[3]. Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42.

[4]. Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010

[5]. M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com/2006/12/28/gmail disasterreports- of-mass-email-deletions/, 2006.

[6]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS ‟07), pp. 598-609, 2007.

[6]. 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.

[7]. B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-

based Distributed Stroage Systems," in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp.31– 42.

[8]. C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,"Dynamic Provable Data Possession," Proc. 16th ACM Conf.Computer and Comm. Security (CCS ¨09), 2009.

[9]. A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS ¨07), pp. 584-597, Oct. 2007

Author Details

Maragoni Mahendar has Received B.TECH Degree in Computer Science Engineering (C.S.E) from Avanthi's Scientific Technological & Research Academy, Gunthapally, Rangareddy in 2012, under Jawaharlal Nehru Technological University Hyderabad and Masters Technology in Computer Science Engineering (C.S.E) from Nova College of Engineering & Technology, Jafferguda, Ranga Reddy 2014, under Jawaharlal Nehru Technological University Hyderabad. He is dedicated to teaching field since the last 4 years. His field of interest includes Cloud Computing, Data science & Big Data. He published Two International Journals and Participated in 4 International conferences. At present working as Asst.Professor, Department of Computer science and Engineering in Avanthi's Scientific Technological & Research Academy, Ranga Reddy, Telangana, India.
Email Id : m.mahender527@gmail.com

Malipatel Anusha M.Tech Student in Dept. of CSE from AVANTHI'S scientific of technological & research academy. Telangana india