ISSN:0975-9646

Secure Storage and Data Integrity Proof in Cloud

Adarsh R.
Department of Computer Science and Engineering
Jain Global Campus, Jain University, Jakkasandra Post
Kanakapura Taluk, Ramanagara District-562112

P. ChidanandaMurthy
Department of Computer Science and Engineering
Jain Global Campus, Jain University, Jakkasandra Post
Kanakapura Taluk, Ramanagara District-562112

Abstract. Cloud computing requires broad security solutions based upon many aspects of a large and lightly integrated system. The cloud data storage service releases the users from the burden of huge local data storage and their preservation by out- sourcing mass data to the cloud. One of the significant concerns that need to be spoken is to assure the customer of the integrity i.e. rightness of his data in the cloud. This paper emphasis on the integrity and security of data storage in cloud computing. The data integrity verification is done by introducing third party auditor (TPA) who has privileges to check the integrity of dynamic data in cloud on behalf of cloud client. Cloud client can get notification from TPA when the data integrity is lost. These systems have sustenance data dynamics via the data operation such as data modification, insertion, deletion. There is many work has been done but there it lacks the support of either public auditability or active data processes. This paper realizes both public auditability and data dynamics. This work displays that projected systems are highly effective and protected.

Keywords –cloud storage server, data dynamic, public auditability, cloud computing.

1. INTRODUCTION

Cloud computing is a prototypical for enabling suitable, on-demand network entrance to a shared pool of configurable calculating resources (e.g., networks, servers, storage, applications, and services) that can be fast provisioned and released with negligible management effort or service provider interaction. This cloud model endorses obtainability and is composed of five indispensable characteristics, three service models, and four deployment models. In cloud computing, everything is delivered as a Service (XaaS). Thus, today there are three main service models such as Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).

A. Software as a Service

Through cloud computing, cheaper and powerful processor, come together and form "software as a service" service model architecture and put them at centralized data storage server because of this network bandwidth increases and network connection should be reliable.

B. Platform as a Service

PaaS offers a high-level integrated environment to build, test, and deploy practice applications. A client (developer) have the flexibility to build (develop, test and deploy) requests on the provider's platform (API, storage and infrastructure).

C. Infrastructure as a Service

It provides software, hardware and equipment's to deliver software application infrastructure with a resource usage based pricing model.

This has many challenging design issues which demand great knowledge affecting on the security and performance of the overall system. One of the biggest concerns with cloud data storage is that truth verification of cloud data at untrusted server. In order to solve the problem of data integrity confirmation, there are many security models & scheme has been proposed. In these works, great efforts are made to build the solution that meet requirement like high efficiency, retrievability of data. Due to, involvement of verifier i.e. TPA on behalf of the cloud customer, scheme is reduction into two categories: private auditability and public auditability before they presented. Although, private auditability achieve higher scheme efficiency and public auditability allow anyone, not only data owner but also publicly, to challenge the cloud server for correctness of the data storage while keeping no private information. Then, clients are given all the privilege to an independent third party auditor (TPA) without devotion of their computing supply. In cloud, clients are may not able to performing frequent integrity checks. So that, there is need to develop verification protocol which has public auditability. Another major design issue to supporting dynamic data operation for cloud data storage which will provide not only access but also update the data stored at remote location by client. So here we focus on the public auditability and data dynamics.

2. RELATED WORK

In Cloud Computing there are many pressures which are avoiding the wide receipt of cloud as explained above. One of the main threats is data confidentiality and data integrity in cloud storages. There is lot of investigation going on in this field to guarantee and provide data integrity in cloud storages. Many answers have been provided to focus on resolving the subjects of integrity. Juels and Kaliski[1] proposed a prototypical Proofs of Retrievability(POR) was one of the first most significant efforts to formulize the notion "guaranteed remotely and dependable integrity of the data lacking the retrieving of data file." It is essentially a data encryption mechanism which notices data corruptions and retrieve the complete the data without any destruction. Shacham and Waters[2] gave a new model for POR enabling verifiability of unlimited number of queries by user with reduced overhead. Later Bowels and Juels[3] gave a theoretical model for the operation of POR, but all these mechanisms proposed were weak from the safety point because they all work for single server.Therefore Bowels [4] in their further work gave a HAIL protocol extending the POR mechanism for multiple servers. Priya Metri and Geeta Sarote[5] proposed a risk model to overcome the threat of integrity and provide data privacy in

the cloud storage. It uses TPA(Third Party Auditor) and digital signature mechanism for the purpose of reliable data retrievable. The TPA being used notifies any illegal access attempting to make changes, avoiding the changes in data and maintaining the originality of data. Atienies and Burns[6] gave Provable Data Possession(PDP) mechanism which verifies the integrity of data being outsourced, noticing all kind of errors occurring in data but doesn‟t guarantee complete data retrievable. In their later work Atienies and Pietro[7] planned a scheme which overcome all problems in PDP, but the main and basic problem on both proposed system didn‟t overwhelmed was they work on single server. Therefore, later Curtmola[8] proposed a scheme to ensure data reliability and retrievability of data for multiple servers. Many mechanisms has been proposed till now to guarantee and ensure complete data integrity and data privacy of cloud storages based on encryption and cryptographic mechanisms using hash values and data encoding. Filho[9] proposed a RSA-based hash data integrity mechanism for peer-to-peer file sharing networks and exponentiation of complete data file is done, but this mechanism can be followed for the files and data of large size, and also this mechanism focuses on the static data files and not on files being dynamic in nature having localization problem.

3. PROPOSED SCHEME

By keeping project goals in mind, here we put the new scheme which guarantees the security of cloud data. The protocol developed chains public auditability with dynamic data operations. The planned system enables public auditability without recovering block of data from file for this we uses Homomorphic authentication method that was used in preceding model. There is the unforgivable metadata generator computed from separate data blocks. In the upcoming work two authenticators such as BLS signature [3] based authenticator. The safety mechanism is further described here. The procedure of protocol is divided into

1) Public auditability for storage correctness declaration: To allow anyone, not just the clients who originally deposited the file on cloud servers, to have the capability to verify the accuracy of the stored data on demand

2) Dynamic data operation support: This will allow the clients to do block-level operations on the data files while preserving the same level of data correctness assurance. The design should be as efficient as conceivable so as to ensure the seamless integration of public audit ability and dynamic data action support.

1) Setup

In this stage KeyGen() method is raised to generate public key and private key. SigGen() is meant for pre-processing and Homomorphic authenticators and along with meta data. The SigGen() method takes two arguments namely secret key and file. The file gratified is divided into blocks. Then signature is computed for each block. Each block's hash code is taken and two nodes' hash is merged into one in order to produce the next node. This process continues for all leaf nodes until tree node is originate. The root element is then taken by client and signs it and send to cloud storage server.

2) Default integration verification

The content of outsourced data can be verified by either client or TPA. This is done by stimulating server by giving some file and block randomly. Up on the test, the cloud storage server computes the root hash code for the assumed file and blocks and then returns the computed root hash code and first stored hash code along with signature. Then the TPA or customer uses public key and private key in order to decrypt the gratified and compare the root hash code with the root hash code returned by clients.

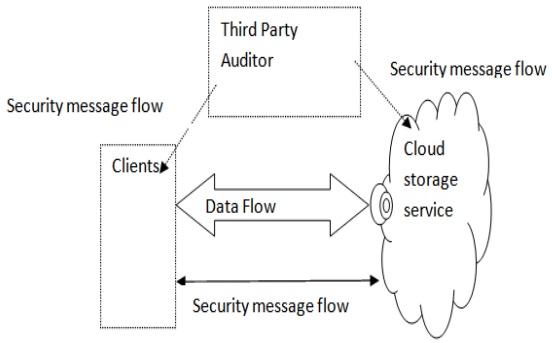

Figure 1: System Architecture

The content of outsourced data can be confirmed by either client or TPA. This is done by challenging server by giving some file and chunk randomly. Up on the test, the cloud storage server computes the root hash code for the given file and blocks and then returns the calculated root hash code and originally deposited hash code along with signature. Then the TPA or client uses public key and private key in order to decrypt the content and match the root hash code with the root hash code returned by clients.

3.1 Algorithms Working

Algorithm for data integrity verification

- Start/begin
- TPA creates random set.
- CSS calculates root hash code based on the file name input.
- CSS calculates the originally stored value.
- TPA decrypts the given content and matches with generated root hash.
- After verification, the TPA can regulate whether the integrity is breached.
- Stop.

Data modifications are the recurrent operations on cloud storage. It is a process of substituting specified blocks with new ones. The data alteration operation can't affect the reason structure of client's data. Another process is known as data insertion. Data Insertion is a process of inserting new record in to existing data. The new blocks are inserted into specified locations or blocks in the data file F.

- Starts/begin.
- Clients produce new Hash for tree then sends to CSS.

- CSS updates F and calculates new R'
- Client computes R.
- Clients confirms signature. If it fails output is FALSE.
- Compute new R and verify the update
- If prove succeed, CSS update R'.
- Stop

4. CONCLUSIONS

For guaranteeing security of cloud data storage, it is tough for enabling a TPA for assessing the quality of service from an objective and self-governing point of view. Public auditability is able to permit clients for delegating the tasks of truth verification to TPA while they are independently not dependable or cannot promise required resources of calculation performing confirmations in a constant manner. One more significant concern is the procedure for construction of verification protocols which can be able to accommodate data files that are active. In this paper, the problem of employing simultaneous public auditability and data dynamics for distant data integrity check in Cloud Computing is explored. The construction is designed for gathering 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 improved through manipulation of the structure of classic Merkle Hash Tree for authentication of block tag. Huge security as well as performance analysis proves that the proposed scheme is efficient and secure to a greater extent.

REFERENCES

[1] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS˝07: Proceedings of the 14th ACM conference on Computer and communications security.

[2] H. Shacham and B. Waters, "Compact Proofs of Retrievability," In Proceedings.of Asiacrypt ˝08, Dec. 2008.

[3] K. D. Bowers, A. Juels, and A. Oprea, "Proofs of Retrievability: Theory and Implementation," Cryptology ePrint Archive, Report 2008/175,2008

[4] K. D. Bowers, A. Juels, and A. Oprea, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Cryptology ePrint Archive, Report 2008/489, 2008.

[5] Jia Xu and Ee-Chien Chang, "Towards efficient proofs of retrievibility in cloud storage".

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores,"In Proceedings.Of CCS ˝07, pp. 598–609, 2007.

[7] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," In Proceedings of SecureComm ˝08, pp. 1–10, 2008.

[8] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "MR-PDP: Multiple-Replica Provable Data Possession," In Proceedings of ICDCS ˝08, pp.411–420,2008.