IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 5 Issue 4, April 2018
ISSN (Online) 2348 – 7968
www.ijiset.com

Cloud Data Integrity Checker Using TPA

[1]Ganesh Moorthi M, [2]Jayakumar D
[1]Post Graduate Student, BIHER, Chennai, India,
[2]Assistant Professor, BIHER, Chennai, India,

Abstract

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. In order to reduce 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. In particular, we leverage the third party auditor (TPA) in many existing public auditing designs, let it play the role of authorized party in our case, and make it in charge of both the storage auditing and the secure key updates for key-exposure resistance. In our design, TPA only needs to hold an encrypted version of the client's secret key while doing all these burdensome tasks on behalf of the client. The client only needs to download the encrypted secret key from the TPA when uploading new files to cloud. Besides, our design also equips the client with capability to further verify the validity of the encrypted secret keys provided by the TPA. All these salient features are carefully designed to make the whole auditing procedure with key exposure resistance as transparent as possible for the client. We formalize the definition and the security model of this paradigm. However, it is possible for the TPA to get the client's data after it executes the auditing protocol multiple times. Auditing protocols in and is designed to ensure the privacy of the client's data in cloud. Another aspect having been addressed in cloud storage auditing is how to support data dynamic operations.

INTRODUCTION

CLOUD Computing has been envisioned as the next-generation information technology

(IT) architecture for enterprises, due to its long list of extraordinary advantages in the IT history: on-demand self-service, location independent resource pooling, rapid resource elasticity, ubiquitous network access, usage-based pricing and transference of risk[1,2]. Cloud computing is widely used in the commercial field, such as Data Store, and cloud application has achieved good effect. In cloud computing, data is moved to a remotely located cloud server. The cloud computing refers to the services and application delivered through internet. The software and hardware are embedded in the data centers providing those services. The data centers are also called cloud (comprise of hardware and software). The National Institute of Standard and Research has given the standard definition of Cloud Computing which is being Accepted Worldwide:- 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 services provider interactions. Cloud computing is a computing paradigm, where a huge pool of systems are connected in public or private networks, to provide energetically scalable infrastructure for application, data and file storage. With the beginning of this technology, the cost of computation, content storage, application hosting and delivery is reduced significantly. Cloud computing is a realistic approach to experience direct cost benefits and it has the prospective to transform a data center from a capital-intensive set up to a variable priced environment. Provides PAAS (platform as a service) and IAAS (Infrastructure as a service). Cloud can be deployed in various forms like: Private cloud: In this cloud owned by an organization and data centers are not available to general public. Public cloud : In public cloud data centers are available to general public and the organization sell the services in payas-you-go manner. Community cloud: In community cloud shared by a number of organizations and provide services to a specific community), Hybrid cloud: In hybrid cloud composition of one or more cloud.

CLOUD COMPUTING

Cloud computing is a technology that uses the internet and central remote servers to maintain data and applications. Cloud computing allows consumers and businesses to use applications without installation and access their personal files at any computer with internet access. This technology allows for much more efficient computing by centralizing storage, memory, processing and bandwidth.

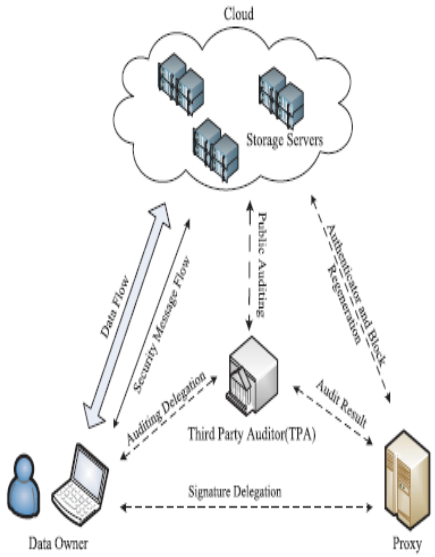
CLOUD SYSTEM MODEL

Whole system of cloud architecture can be partition into three significant components: 1) Client: An entity, which contains huge data and data files that are to be stored in the cloud for the monitoring and computation purpose. Client totally relies on the cloud provider for security of their data and they can be either individual consumers or organization. 2) Cloud Services Provider (CSP): It is an entity, which manages and stored all the data stored by the client. The Cloud storage service provider makes all the computation resources available to manage the data files.

Third party auditor

TPA is the third party auditor who will audit the data of data owner or client so that it will let off the load of management of data of data owner [3]. TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would not only help owners to estimate the risk of their subscribed cloud data services, but also be advantageous for the cloud service provider to improve their cloud based service platform [4,5].This public auditor will help the data owner that his data are secure in cloud. With the use of TPA, management of data will be easy and less burdening to data owner but without encryption of data, how data owner will ensure that his data are in a safe hand.

USECASE DIAGRAM



LITERATURE REVIEW

Cloud computing is an rising trend in the field of technology. There are different issues related to cloud computing, major ones being the security and integrity of data. Many algorithms have been proposed and many frameworks have been designed to resolve such issues. Nirmala et al. [6] proposed a new proposal to resolve integrity problem by introducing user authenticator to audit and check the integrity of data. Their research focused on providing solutions to all issues of cloud computing and to develop a mold that would provide secure cloud infrastructure which would facilitate to adopt the cloud as and when required. Raju et al. [7] introduced a protocol for integrity checking of cloud storage that would provide integrity protection of user information. This protocol supports public verifiability and is evidenced to be secure against relate un-trusted server. It's additionally non-public against third-party verifiers. Attas and Batrafi [8] proposed an integrity checking model over cloud with help of TPA using DSA algorithm. With the help of the model, user can examine and verify the data from unauthorized people who manipulate with the cloud or extract data. Evaluation of the model was done using Windows Azure project that involved digital signature coding. The results showed that the proposed model worked according to what was claimed. Ateniese et al. [9] are the first to consider public auditability in their defined "provable data possession" (PDP) model for ensuring possession of files on entrusted storages. In their scheme, they utilize RSA based homomorphism tags for auditing outsourced data, thus public audit ability is achieved. However, Attendees 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 security and design problems.

SYSTEM IMPLEMENTATION

Modules:

It consists of following modules such as

- NETWORK FRAME
- SIGN IN FRAME
- TPA FRAME
- INFORMATION FRAME
- TPA LOGIN

NETWORK FRAME

In this module, the user has to give request to download the file. This request will be stored and processed by the server to respond the user. It checks the appropriate sub server to assign the task. A **job scheduler** is a computer application for controlling unattended background program execution; job scheduler is created and connected with all servers to perform the user requested tasks using this module

TPA LOGIN

TPA Login the process by which an individual gains access to a computer system by identifying and authenticating themselves. The user credentials are typically some form of "username" and a matching "password", and these credentials themselves are sometimes referred to as **a login.**

SIGN IN FRAME

This module we used to sign in to the cloud to store the data in the server. In this which the user can upload the files sign in frame also have a ‘username and password”.

TPA FRAME

In this module we explain about the third party authentication, every data send by the user is estimated their size and it will take the image of the data and store in the server and main source is in other server. This image data is audit by the third part.

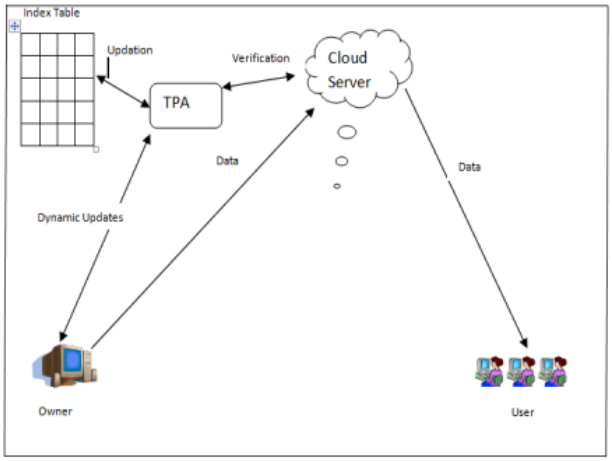
INFORMATION FRAME

In this frame we have all information that is inside the server what are flies available in the frames if any files are missing then the third party audit will set their a back of particular file.

Dynamic Auditing

As data in Cloud is dynamic, static auditing is not enough. A dynamic auditing is needed to verify the data integrity of the dynamic data. But as data are dynamic in cloud, it is not easy to have an auditing efficiently. Server can enforce Replay attack and forge attack to fail the auditing process. The dynamic operations include modification, insertion and deletion. Whenever dynamic operation is performed, the owner sends the update message to the auditor representing the index number of that message. The Auditor updates the table. The message m and the tag are replaced by the new message and tag in message modification. The new message m and new tag are inserted in insertion operation. The message m and tag are deleted from the index table and all the

entries below the deleted message move upwards.



After performing updates in the table, the auditor conducts the data integrity test for the updated data. Auditor sends the result to the owner and he deletes the local copy of updated data.

CONCLUSION:

In this paper, we propose a privacy-preserving public auditing system for data storage security in cloud computing. We utilize the holomorphic linear authenticator and random masking to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of our design on both the cloud and the auditor side. We leave the full-fledged implementation of the mechanism on commercial public cloud as an important future extension, which is expected to robustly cope with very large scale data and thus encourage users to adopt cloud storage services more confidently.

REFERENCES

- C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
- P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/ index.html, June 2009.
- Mr.D.Jayakumar, "A Resourceful Allocation of Data Storage in Cloud Computing" International Journal of Advances in Engineering and Emerging Technology,VOL 1,ISSUE 1,MARCH 2013.
- M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.

- Cloud Security Alliance, “Top Threats to Cloud Computing,”http://www.cloudsecurity alliance.org, 2010.

- M. Arrington, “Gmail Disaster: Reports of Mass Email Deletions,” http://www.techcrunch.com/2006/12/28/gmail-disasterreportsof-mass-email-deletions/, 2006.