International Journal of Latest Engineering and Management Research (IJLEMR)
ISSN: 2455-4847
www.ijlemr.com || Volume 06 - Issue 04 || April 2021 || PP. 19-21

Methodologies and Responsibilities for a TPA in Maintaining Security of the Data over Cloud

Saurabh R. Dahake
PG Student

E. M. Chirchi
Professor and Head

Department of Computer Science and Engineering,Shreeyash College of Engineeringand Technology, Aurangabad (Maharashtra), India.

Abstract: Cloud computing is a very fast growing technology in the IT field. A cloud is a collection of various types of devices that provides services of software, applications and platforms to the users all over the world via internet. One of the main uses of cloud network is to save the user data and make it available to him on his demand. Securing the data is also one of the responsibilities of the cloud Service Provider (CSP). But, the problem arises when a user has to bank upon the cloud service provider (CSP) for the security of his data. It is when the user cannot believe on the CSP, the Third Party Auditor is introduced in the midst of things. The TPA checks the user data on his request and reports the result back to him. This paper elaborates what a TPA is and what he does.

Keywords: Cloud Service Provider (CSP), Third Party Auditor (TPA), Security.

I. Introduction

A cloud is a network that is situated over a remote location. This network provides services to a user via internet. With the help of cloud computing we can use the applications those are not physically available in our workplace using internet. It facilitates the manipulation and configuration of the applications present over the internet. But the main service provided by the cloud, which concerns us more than all the others, is its service to store data. A cloud can be broadly divided into two models, namely, Deployment Model and Service Model.

a) Deployment Models: It defines how the cloud can be accessed.
   - Public cloud: Accessible by general public.
   - Private cloud: Accessible within an organization.
   - Community cloud: Accessible by more than one organization.
   - Hybrid cloud: Combination of public and private cloud.

b) Service Models: It defines the type of service provided by the cloud to its users.
   - Infrastructure as a service (IaaS): Provide users with hardware support like virtual machines, servers, etc. to use.
   - Platform as a service (PaaS): Provide users with back end facilities like databases, tools, etc. to use.
   - Software as a service (SaaS): Provide users with the software like E-mail, CRM, etc. those can be used online.

However, the most widely used facility of cloud computing is as a storage medium, which belongs to IaaS model. Many users, these days, due to lack of personal storage capacity, imagine of having a storage area which will not be their own, yet secure, where they can store their personal data. Cloud Service Provider (CSP) facilitates this to the user where he can upload his personal data online, which is made available to him whenever he demands.

II. Security Over Cloud

Security over cloud implies that the data uploaded on the cloud infrastructure should be in the same state over any period of time after it has been uploaded. And if any data violation takes place, then it should not be implicit.

However, with the loss of physical possession of the data, rise the external security threats where the data protection becomes tedious. No matter how much the CSP boasts of securing the user data from external threats, the user remains skeptical of the data security from the CSP. The main concern of a user is what if the CSP manipulates the data for his own good like erasing the data which has not been used over a long period of time. CSP can also hide the data theft events to preserve his reputation in the market.

To prevent all such illicit activities, the data owner i.e. the user should be able to ensure that his data is safe over the cloud. A way to do this is to download his data every time checking needs to be done. But, this is time consuming and requires a very high speed of the transmission link. Another way is to assign this activity of data checking to a third person. This third person goes by the name Third Party Auditor (TPA) [1].

III. Third Party Auditor

A Third Party Auditor is a person appointed by the user to check his data stored on the cloud. A TPA has more capabilities and proficiency than a user does to check the data integrity, which can be difficult for a user. The TPA knows the security concerns and the best ways to do the job. The TPA acts as a mediator between a user and a CSP. TPA checks the user data and prepares an audit about the data. This audit helps the user to analyze his data integrity and derive a conclusion over the security provided by the CSP. And in turn, it also helps the CSP to improve its own performance [2]. The responsibilities of a TPA are as follows:

1) No Data Acquaintance: The TPA should not come to know the content while auditing.
2) Auditing over the Cloud: The TPA should check the data without fetching it from the cloud server.
3) Communication Overhead: While checking the data integrity, the communication overhead should be low.
4) Scalability: As the cloud network is a dynamic network, the working of TPA should not be affected by the increase or decrease in the number of cloud service users.
5) Batch Auditing: The TPA should be able to serve the request of multiple users at a time.

IV. Related Works

A traditional way was using the MAC based solution for the encryption to protect it from the cloud. Here the files to be sent are divided into multiple blocks and MAC for each block is calculated. These blocks and MACs are sent to the CSP while the secret key is shared with the TPA. Then to check the data, the TPA demands for a random block with its MAC and uses the secret key to check the data. But this method has some disadvantages as follows:

- The privacy of data is not preserved from the TPA.
- Communication Overhead is high.

Yang and Jia, 2012, [3] provided the solution of using four algorithms, which are as follows:

- KeyGen: Here the user generates his own public and private key.
- SigGen: The cloud user then generates the metadata like signatures for verification purpose.
- GenProof: Here the CSP provides the proof of data integrity.
- VerifyProof: The proof generated by the cloud is verified here by the TPA

These algorithms are carried out in two phases:

- SetUp Phase: The KeyGen and SigGen algorithms are carried out in this phase.
- Audit Phase: The GenProof and VerifyProof are carried out here.

Govinda et al [4], 2012 proposed the use of digital signatures for data security. They preferred RSA algorithm for the encryption and decryption. They used digital signatures for message authentication and verification.

Arasu et al [5], 2013, used the HMAC based cryptography. HMAC stands for Hashed Message Authentication Code. Here the authentication code is calculated using a secret key. This authentication code is then used to verify the data integrity.

Sathiskumar and Retnaraj [6], 2014, Proposed the use of Homomorphic Linear Authenticator (HLA). This prevents the fetching of the actual data by the TPA to audit. HLA is similar to MAC. The main drawback here is that HLA can be aggregated and computed and hence the original data is again at risk.

Parvekar et al [7], 2014, proposed a privacy preserving Public Auditing. They proposed the use of Homomorphic Linear Authenticator (HLA) and random masking based on a public key.The main advantage of this system is that it provides the data security from the TPA as well. But here the TPA is strictly bounded by a single task. When he serves a user, the other users have to stay in a queue. Hence this is time consuming.

V. Conclusion

Here we studied the various methodologies those have been used to protect the data over the cloud. The concept of TPA was a great revolution in the field of providing security over the cloud data. Various researchers provided various methods for the TPA to carry out its duties, but each one having its own limitations. Public key based HLA with Random Masking is the best of all only if the TPA can serve multiple users at a time.

References

[1] Farzad Sabahi, "Cloud Computing Security Threats and Responses", IEEE conference, 978-1-61284-486-2/111, 2011.

[2] Bhagat and R. K. Sahu, "Using Third Party Auditor for Cloud Data Security: A Review" International Journal of Advanced Research in Computer Science and Software Engineering 3(3), pp. 34-39, March – 2013.

[3] K. Yang, and X. Jia, "An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing", IEEE Transactionson Parallel & Distributed Systems, vol. 24, no. 9, pp. 1717-1726, 2012.

[4] K. Govinda, Gurunatha prasad and H Sathsh kumar, "Third Party Auditing for Security Data Storage in cloud through digital signature using RSA" IJASATR, issue 2,vol-4, ISSN 2249-9954,2012.

[5] Ezhil Asaru, B. Gowri, S. Ananthi, "Privacy Preserving Public Auditing in Cloud Using HMAC Algorithm", International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-2, Issue-1, March 2013.

[6] Sathis kumar R and Dr. Jeberson Retnaraj," Secure Privacy Preserving Public Auditing for

[7] Cloud storage", International Journal of Innovative Research in Science, Engineering and Technology ISSN: 2319-8753, 2014

[8] Preeti Parvekar, Mayuri Saxena, Prakash Kumar and Sakshi Saxena, "Public Auditing: Cloud Data Storage",5th International Conference- Confluence the Next Generation Information Technology Summit (Confluence),978-1-4799-4236-7, IEEE, 2014.