ISSN 2319-2720

Volume 6, No.2, April – June 2017

International Journal of Computing, Communications and Networking

Available Online at http://www.warse.org/ijccn/static/pdf/file/ijccn01622017.pdf

A Survey: Privacy Preserving Encryption Technique In Cloud Storage

Chandraprabhat Sahu, Ayonija Pathre

M.Tech C.S.E., AISECT UNIVERSITY, BHOPAL, INDIA, c.prabhat18@gmail.com

Asst. Professor C.S.E., AISECT UNIVERSITY, BHOPAL, INDIA, ayo.pathre@gmail.com

ABSTRACT

Cloud computing introduces a new framework to access data and resources over internet , it allow user to remotely store data and use high on demand services and applications from a shared pool of resources but in that case data is outsourced ,thus data is vulnerable to many online security threats . These problem demands a secure framework which provides security for that data Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. So for that purpose a Third Party Auditing system (TPA) which take care the auditing task of outsourced data to check data integrity and make it worry free. Also TPA should be efficient and to audit outsourced data without asking the duplicate copy of that data and also not put any extra burden on the cloud user. We propose an advanced auditing system which provides following features.

Keywords : Third Party Auditing (TPA), Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS).

1. INTRODUCTION

Cloud computing is synonyms of any service you get over internet, since it emerges in 2007 it is the favorite topic for researchers. There many big companies like IBM ,VMware, Amazon etc, are provide cloud services for the users.

Cloud computing is the delivery of computing services—servers, storage, databases, networking, software, analytics and more—over the Internet (“the cloud”).

Cloud Computing is also defines by:

- 5 essential characteristics
- 3 cloud service models
- 4 cloud deployment models

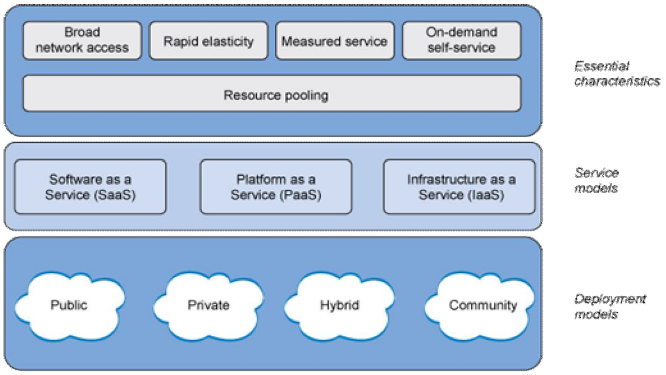

Figure 1: Three types of cloud computing (SaaS),(PaaS) and (IaaS)

a cloud user can use the following types of cloud providers: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

These three types of cloud computing differ in the amount of control that user have over his information and how much user can expect his provider to do for him. In this IaaS is most basic and each higher model abstracts from the details of lower models.

1) Software as a Service (SaaS):In cloud computing in this model, users use the applications of service provider that run on cloud infrastructure. The users need not to install and run the applications on his system. The user can use these applications through any thin and thick client devices. This eliminates the user need to upgrade their applications. The user is billed according to his usage. Users do not maintain the underlying the cloud infrastructure including the network, server, operating system, storage or applications. For example: Google Docs, Sales Force , SAP Business by Design etc.

2) Platform as a Service (Paas): In cloud computing in this model user can deploy their applications on cloud infrastructure created using some programming language, libraries and tools provided by cloud service provider. This elements the user need to install the software and hardware required for it. Users do not maintain the underlying the cloud infrastructure including the network, server, operating system, storage but has controlled upon the deployed applications. For example: Force.com, Google App Engine, Window Azure etc.

3) Infrastructure as a Service (Iaas): In cloud computing in this model users have capability to provision processing, storage, networks and their fundamental computing resources so that user can deploy and run arbitrary software, which includes operating system and applications. The users don’t

manage or control the infrastructure. He does manage or control the operating system, storage, applications, selected network components. For example: Amazon's EC2, Amazon S3, etc.

B. In cloud computing Deployment models Enterprises can choose to deploy applications on four types of cloud that are Public, Private, hybrid or community cloud.

These deployment models describe who owns, manages and is responsible for the services provided.

1) Public Cloud: In cloud computing the cloud infrastructure is open to use by the general public. It can be accessed by any user with an internet connection and access to cloud space. They do not know about the other users who are using the same server or network. However public clouds are less secure as compared to the other cloud models because public cloud is more prone to attacks. For example: Amazon, Google Apps, Window azure.

2) Private Cloud: In cloud computing the cloud infrastructure is used by a single organization. It is created for a specific group or organization and having access to that group or organization. This is more secure as compared to public as only the users of organization have access. For example: eBay.

3) Community Cloud: In cloud computing the cloud infrastructure is used by a specific community of users. The community is made of two or more groups or organizations that have similar cloud requirements. For example: zimory and RightScale [8], [1].

4) Hybrid Cloud: In cloud computing a hybrid cloud is a combination of public or private cloud. The cloud infrastructures will be unique entities, but bound together by technology that enables data and application portability. It is created to fulfill the demand of the organization. There are not many hybrid clouds but some companies like IBM and Jupiter have introduced their basic technologies for hybrid cloud.

In cloud computing user can remotely access different on demand high quality cloud services and remotely store their data and reduce the burden of users to store data.

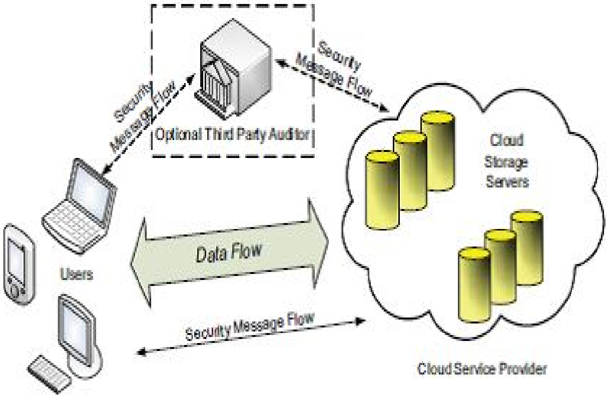

Figure 2: Cloud computing TPA service provisioning architecture

But in that case data is vulnerable to third party access and also misuse of that data many illegal activities, so in this way secure public auditing to provide a third party auditor that take care of all the auditing task of the data and reduce overhead of the user. The third party auditor is a tool that perform the task of integrity check for the user, when we store data on server we need to check that data is not altered or lost or compromised while processing ,so take care of these tasks a TPA is used .

There are two modules of auditing used in cloud computing:

Privacy preserving public auditing:-In cloud computing Homomorphic authenticators are verification generated from individual data blocks, which can be securely aggregated in such a way that to assure an auditor that a linear combination of data blocks is correctly computed by verifying only by the aggregated authenticator.

Batch auditing:- In cloud computing TPA may concurrently handle multiple auditing upon different users' requests. The individual auditing of TPA can be tedious and very inefficient. Batch auditing not only allows the TPA to perform multiple auditing tasks simultaneously, but also properly reduces the computation cost on the TPA side.

2. LITERATURE REVIEW

Cong Wang, S.M.chow[1]propose a privacy preserving public auditing system for cloud data storage. Authors use homomorphic linear authenticator and random masking to prevent TPA to access data content stored on server while the process of auditing, in this way it eliminates the burden of expensive auditing task and fear of data leakage for cloud user.

Anne Shrijanya K, N. Kashivishwanath [2] Most of the times user store their data in private cloud but when extra space is needed user moves towards public cloud, security mechanism in public cloud are there but these are not sufficient to maintain the data integrity. So some other third party mechanism is required for this purpose we use TPA to perform auditing tasks, in this paper author propose an auditing model based on Markel hash tree. This provides a TPA service and store data safely on server.

Ankit R. Mune, R. Pardhi[3] in old days user encrypt data and send it to the server to store data but now days after the emergence of cloud computing data mostly saved on cloud so it to tedious and expensive for user to take extra burden of encrypting data for this purpose author propose a technique security cloud in which it perform the task of auditing data and maintain the integrity of data keep it safe from any kind of unauthorized access.

RenukaGoyal, NavjotSidhhu [4] security is the biggest concern in cloud computing, user save their data on cloud, sometimes the is lost or corrupted or discarded by the data center .all these things are the threat for data for this purpose a third party auditor (TPA) is used to take care of all these tasks, in this paper a study on various TPA techniques is presented all the techniques have their merits and demerits.

Nooper M. Yawale, V.B. Gadichha [5] to perform data security on cloud storage TPA is used, in this paper A RC5 based Third Party Auditing Mechanism is proposed, that system uses RC5 encryption for data integrity author further extends their results for multiple user that system provides an highly secure and easy to access third party system.

Nandeesh.B.B, Ganesh Kumar R, JitendranathMungara [6] in this paper author proposed an dynamic data support for cloud storage including block update, delete, append. It ensure about the correctness of code to provide redundancy parity vector and guarantee the data dependability. It also provide an third party system which can be perform the task of auditing of data and make user worry free about their data.

3. PROPOSED WORK:

On the basis of literature study we proposed an enhanced TPA which has following characteristics-

- The user is only allowed to perform the duplicate check for files marked with the corresponding privileges.
- We present an advanced scheme to support stronger security by encrypting the file with differential privilege keys.
- Reduce the storage size of the tags for integrity check.

4. CONCLUSION:

Here in this paper we proposed a technique in which we have reviewed different papers on auditing technique where the batch auditing and single file auditing is performed. We discussed about the privacy preserving technique and security approaches while working with the multi copy batch auditing. In this paper we have discussed different security and auditing approach over the cloud and thus the maximum privacy preserving technique to audit the multiple copy verification using efficient signature based scheme is need to opt out for the further work.

REFERENCES

1. Cong Wang, S.M. chow, Qian Wang, KuiRen, Wenjing Lou ”**Privacy Preserving public auditing for Secure cloud storage**” IEEE Transaction for Computers Vol.62, No.2, February 2013.
2. Anne Shrijanya K, N. Kashivishwanath “**Data Integrity Verification By Third Party Auditor in Remote Data Cloud**”IJSCE Vol.3, Issue 5, November 2013.
3. Ankit R. Mune, R. Pardhi “**Security for cloud computing data using a security cloud as a third party auditor (TPA):A Survey**” IJARCCE Vol.3, Issue 3 March 2014.
4. RenukaGoyal, NavjotSidhhu “**Third Party Auditor: An integrity Checking technique for client data security inn cloud computing**” IJCSIT Vol. 5(3) 2014.
5. Nooper M. Yawale, V.B. Gadichha “**Third Party auditing for Data storage Security in cloud with RC5 algorithm**” IJARCSSE Vol.3 is Issued on 11 November 2013.
6. Nandeesh.B.B, Ganesh Kumar R, JitendranathMungara”**Secure and Dependable Cloud Service for TPA in Cloud computing**” IJITEE Vol.1 Issue 3 August 2012.
7. Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou, “**A Hybrid Cloud Approach for Secure Authorized Deduplication**”, IEEE Transactions on Parallel and Distributed Systems, 2014.
8. LluisPamies-Juarez, Pedro Garc__a-L_opez, Marc S_anchez-Artigas, Blas Herrera, “**Towards the Design of Optimal Data Redundancy Schemes for Heterogeneous Cloud StorageInfrastructures**” ,” Computer Networks, 2011.
9. Deyan Chen, Hong Zhao, “**Data Security and Privacy Protection Issues in Cloud Computing**”, International Conference on Computer Science and Electronics Engineering 2012.
10. Boyang Wang, Baochun Li, Hui Li,” **Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud**,” IEEE TRANSACTIONS ON Cloud Computing, VOL. 2, NO. 01, March 2014.