International Journal of Information Technology and Management

Vol. V, Issue No. I, August-2013, ISSN 2249-4510

# DATA SECURITY AND INTEGRITY IN CLOUD COMPUTING: THIRD PARTY AUDITOR

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

*International Journal of Information Technology and Management*
*Vol. V, Issue No. I, August-2013, ISSN 2249-4510*

# Data Security and Integrity In Cloud Computing: Third Party Auditor

**Rajkumar**

Research Scholar, Bundelkhand University, Jhansi

***Abstract – Cloud computing is environment which enables convenient, efficient, 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. Cloud is kind of centralized database where many organizations/clients store their data, retrieve data and possibly modify data. Cloud is a model where user is provided services by CSP(Cloud Service Provider) on pay per use base. Means here Client has to pay for what he is using or being served. Data stored and retrieved in such a way may not be fully trustworthy so here concept of TPA(Third Party Auditor) is used. TPA makes task of client easy by verifying integrity of data stored on behalf of client. In cloud, there is support for data dynamics means clients can insert, delete or can update data so there should be security mechanism which ensure integrity for the same. Here TPA can not only see the data but he can access data or can modify also so there should be some security mechanism against this.***

***Cloud Computing is the next-generation architecture of computing. It moves the software and databases to the large data centers, where the management of the data and services can face a number of challenges. By outsourcing data, users are free from the burden of local data storage and maintenance. However, since the users does not have physical possession of large size of outsourced data makes the data integrity protection in cloud computing a very challenging task for users. So public auditability for cloud data storage security is important where users can entrust an external audit party to check the integrity of outsources data when needed. To securely introduce an effective third party auditor (TPA), the following requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without the local copy of data, and should not introduce any additional on-line burden to the cloud user; 2) The third party auditing process should preserve user data privacy.***

***Security is a major issue in cloud computing environment as the resources are dynamic, virtualized, scalable and elastic in nature. Data Integrity is to ensured. Auditing plays a vital role in providing solution to the data integrity in cloud. Highly distributed and non- transparent nature of cloud increases the complexity of Auditing process. Auditing deals with SLA monitoring and compliance. A third party auditor is essential to perform auditing to ensure data integrity on cloud services. In this paper, a Dynamic Third Party Auditing System is proposed in which a third party entity dynamically provides auditing services on cloud computing environment. TPA makes task of Client by verifying the integrity of data stored in cloud. The Dynamic third party auditing system does auditing using public key based homomorphic authentication.***

----------♦----------

## INTRODUCTION

Cloud Computing gained intention since 2007.It is the general term for anything that involves providing services on internet. It moves the data and computing from desktop to large datacenters. It is combination of parallel, grid and distributed computing.

Many big companies such as IBM, Google, Amazon, Microsoft, Yahoo and other move themselves to develop Cloud Computing. These companies have launched their own Cloud Computing infrastructures and services and achieved good application results and social impact, such as Amazon's EC2 and S3, Google' Google Apps, Microsoft' Azure and so on.

According to National Institute of Standards and Technology (NIST): "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".

Cloud computing gets name as a metaphor for the Internet. The computer industry is the only industry that is more fashion-driven than women's fashion he told to a group of Oracle analysts. So let's talk about what cloud computing is and tighten up definition and understanding of this implementation. Cloud computing has become most important propaganda issue in since 2007 and many companies used to attempt to use the cloud computing services. Typical cloud computing services are Amazon EC2 and Google app engine, amazons they use the Internet to connect to external users with the gadget, economy, high scalability and other advantages, Pick up any tech magazine or visit almost any IT website or blog and you'll be sure to see talk about cloud computing. Internet is represented in the network diagrams as a cloud, the cloud icon represents "all that other stuff" that is makes the network work. It's kind of like "etc." It also typically means an area of diagram or solution that is somebody else's concern so why diagram it all out? It is probably this notion that is most applicable to the cloud computing concept and Cloud computing promises to cut capital costs and operational more importantly let IT departments focus on strategic projects instead of keeping centralized the data centre running.

The third party match both the data it must be same as the sent one on the sender cannot deny that they sent it (non-repudiation).Downloading of data for its integrity verification is not feasible task since it's very costly because of the transmission cost across the network.

It is very important to provide public auditing service for cloud data storage. For well organization it is very essential that cloud that allows investigation from a single party audit the outsource data to ensure data security and save the data storage and user's computation. That user trusts an independent third party auditor (TPA). It provides the reasonable way for users to check the validity of data in cloud. Check the integrity of data on cloud on the behalf of users. Public auditing in addition to user provides the external party to verify the correctness of stored data against external attacks it's hard to find. However these schemes, don't involve the privacy protection of data and a main disadvantage which affect the security of the protocols in cloud computing. Cloud service provider has significant storage space and computation resource to maintain the user's data. Also it has expertise in building and managing distributed cloud storage servers and ability to own and operate live cloud computing systems. So users who depend on only TPA for their security storage want their data to be protected from external auditors. Users who put their large data files into cloud storage servers can relieve burden of storage and computation and at the same time it is important for users to ensure that their data are being stored correctly and security check. Users should be beautified with certain security means so that they can make sure their data is safe and Cloud service provider always online & assumed to have abundant storage capacity and computation power. Third party auditor is invariably online too and It makes every data access be in control.

TPA eliminates the involvement of client through auditing of whether his data stored in cloud are indeed intact which can important in achieving economies of scale for Cloud Computing third party auditor who will audit the data of data owner or client so that it will let off the burden of management of data of data owner.

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Because of number of advantages it offers cloud computing is looked upon as the architecture for next generation enterprises. Some of the advantages are on demand self-service, usage based pricing, rapid resource elasticity, location independent resource pooling etc. Users have a number of appealing benefits such as universal data access, relief of burden of storage management, avoidance of capital expenditure on hardware ,software etc. Although cloud computing has a lot of advantages it also brings security threats towards user's outsourced data. Many times correctness of data is put under risk since cloud service providers are separate administrative entities. The main threats to data are mainly due to the reasons described below. First of all there are internal and external threats even though cloud infrastructures are powerful and reliable. Secondly there are chances that cloud service provider behave unfaithfully towards outsourced data to cloud users. Since the users no longer have the possession of outsourced data it is necessary that the data is audited to ensure data integrity. In order to ensure data integrity and save cloud users computation resources it is of critical importance to enable public auditing service for cloud data storage so that users can resort to a third party auditor to audit outsourced data. Third party auditor provide easier and affordable way for users to ensure storage correctness and the audit result from third party auditor will also be beneficial for cloud service provider to improve cloud based service platform. By using public auditing services users can avoid risk and gain trust in cloud.

## LITERATURE REVIEW

Cloud environment provides immense possibility for internet application provides infinite space for storing as well as managing data and provides powerful computing capacity for users to complete all kinds of application. Users have started changing their habit of using computer totally, from services centered by desktop to services centered by Web. The aim of application of cloud computing is to combine all the resources, and let anyone use it. There are many definitions of cloud but collectively advocates the ease of use as long as the user is having a computer and connected to the internet. User does not need to

buy hardware neither the software but simply charged for the resources being utilized adding a comfort factor as well as reducing the overhead. Overall, advent of cloud era has introduced virtualization with numerous benefits including reduced capital expenditure and administration costs, enhanced scalability and improved quality of service.

Different factors such as integrity of data, data dynamics and data privacy affects The performance of a number of approaches in cloud data storage. Each and every approach has merits and demerits which make them suitable for different applications. Various mechanisms are proposed on how to use the TPA so that it can relieve the burden of data owner for local data storage and maintenance; it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both individuals and enterprises with high service-level requirements. This kind of audit service not only helps save data owners„ computation resources but also provides a transparent yet cost- effective method for data owners to gain trust in the cloud. The presence of TPA eliminates the involvement of the client by auditing whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Though this method states how to save the computational resource and cost of storage of owner's data but how to trust on TPA that is not calculated. If TPA modifies data or deletes some data and if it becomes intrusive and pass information of data owner to unauthorized user than how owner know about this problem is not solved. Thus, new approaches are required to solve the above problem.

Using Third Party Auditor this problem can be generalized as how can the client find an efficient way to perform periodical integrity verifications without the local copy of data files. If two users or more users are using a data, one is writing a data while one is reading a data than it may be wrong read by 1 user, so to resolve data inconsistency is become an important task of the data owner. Another problem how to trust on TAP is not calculated. If TPA become intruder and pass information of data or deleting a data than how owner know about this problem are not solved Consistency and Integrity. Proposed scheme in this vm, Advanced Encryption Standard (AES) are used where client encrypt and decrypt the file. In this vm, this mechanism solves the problem of unauthorized access of data in this suggested scheme that can be used for integrity and consistency of data.

Different factors such as integrity of data, data dynamics and data privacy affects The performance of a number of approaches in cloud data storage. Each and every approach has merits and demerits which make them suitable for different applications. In this paper we will discuss different approaches which are already carried out for cloud data security. Various mechanisms are proposed on how to use the TPA so that it can relieve the burden of data owner for local data storage and maintenance, it also eliminates their physical control of storage dependability and security, which traditionally has been expected by both individuals and enterprises with high service-level requirements. This kind of audit service not only helps save data owners computation resources but also provides a transparent yet cost- effective method for data owners to gain trust in the cloud. The presence of TPA eliminates the involvement of the client by auditing whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. Though this method states how to save the computational resource and cost of storage of owner's data but how to trust on TPA that is not calculated. If TPA modifies data or deletes some data and if it becomes intrusive and pass information of data owner to unauthorized user than how owner know about this problem is not solved. Thus, new approaches are required to solve the above problem.

## CLOUD DATA INTEGRITY

Data integrity means data should be correctly stored on the cloud server without any modification and if any violations i.e. if the data is get lost, altered or compromised can be detected. It must remain in the same state. But the integrity of data is at risk in cloud server. As the user does not have physical possession of data so the integrity and security of data become the major concern in the cloud computing. Data can get modified by other users or even sometimes cloud service provider for his own benefit can behave unfaithfully towards the users regarding outsourced data. For example cloud service providers for more space on data centre can discard the user data which has not been or rarely accessed by the user for a longer time or even can hide the data loss incidents to maintain his reputation.

We need to ensure the integrity by making the user capable to check over the cloud data from any unauthorized modification. One solution is to first download the files whose integrity have to check but downloading the files requires high transmission cost. So to maintain the data integrity and to minimize the storage risk it is important to take assistance of a Third party auditor (TPA) who checks the data integrity for the cloud user and helps the user in minimizing his risk.

## THIRD PARTY AUDITOR

Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client (data owner), to challenge the cloud

server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that 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 help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will help data owner to make sure that his data are safe in the cloud and management of data will be easy and less burdening to data owner.

## THIRD PARTY AUDITING FOR DATA INTEGRITY

Cloud Computing is new dimension scheme for IT industry. It provides the required scalable services in on demand basis with minimum operation cost. The famous cloud computing providers are Amazon, Google, Microsoft, Yahoo and Sales force. All these companies are independent entities, each having their own data services and security policies. Cloud Computing is a highly distributed computing paradigm in which dynamic, virtualized, on-demand, scalable resources are provided to the cloud users as a service. Depending on the services, the cloud services are broadly classified as software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS). Depending on service deployment, cloud is categorized as Public Cloud, Private Cloud, Hybrid Cloud, and Community Cloud. Cloud users do not own the resources. Users can access the resources hosted by the cloud providers on the internet. This reduces the management overhead of the client as the users do not own the resources. Moreover the highly distributed nature and scalability adds advantage to the cloud. But the advantages of cloud Computing turn into a critical security issue as the cloud user does not have control over their data. There is a chance the service providers may delete the un accessed data of the normal user. Also data User does not know the location of their data. Various security mechanisms are insufficient as cloud is highly distributed and dynamic. Provisioning of shared resources to the untrustworthy users added a challenge in cloud environment. Cloud Computing is a model that provides on demand services to the users in convenient and efficient manner. This model contains a shared pool of resources like networks, servers, storage, Applications and services.

Auditing: As the SLA agreement is not transparent to the users, there comes the need to have auditing to check for SLA violation. There are two types of auditing depending upon which is being audited: Internal Audit and External Audit. Internal Audit audits the processes that takes place in providing the service. External Audit audits the quality of service such as CPU performance, availability and SLA parameters.

Audit can be both static and dynamic. In static auditing, auditing is done periodically to verify the integrity of data. Samples are taken from the data and it is verified for integrity of data. In dynamic auditing, auditing is done on dynamic data. The dynamic data operations are modification, insertion and deletion. Batch auditing is required when there is multiple owner and multiple cloud servers.

The Cloud service may give lot of commitment and service offers to the cloud user due to market competition. But any point of time he has to follow it. The cloud service providers for their own benefits they will hide the data errors from the cloud user. To avoid this problem and to maintain the security standard we need a Third Party Auditor (TPA).The TPA will monitor the both client and Service Provider side activities. TPA will follow the auditing norms and techniques, also they will have list of auditing strategies. The TPA should familiar with the SLA between cloud service provider and cloud user. TPA will play promising role between this two parties. TPA having ability to check the integrity of the data which stored in the cloud. The auditing should not affect the privacy of the cloud users.

Here the cloud user mainly concern about their data security. Data Security comprises of Data integrity, Data Availability, Data Confidentiality. As the data is stored In order to verify the data integrity at un trusted servers become a big concern with cloud environment. Data security means protecting the data from the unwanted actions from unauthorized users and protecting from destroy forces. The forces may in any form of hardware failure, software failure, network failure, system failure, external forces, natural calamities etc. The unauthorized user may be intruder. We have to monitor the all user activities, if we found any unauthorized function from any user, immediately we should block the particular user before damaging the data. Data Integrity means maintaining the accuracy and consistency over the cloud user data at any point of time. The cloud user may store key information in the cloud storage, the accuracy of the user data information should be accurate in any point of time. Data Confidentiality means maintaining the secrecy about the user data. Confidentiality is a set of rules and promises to maintain the secrecy over some cloud user data information. The Cloud Service Provider should not enclose that information to anybody in any point of time. The auditing process consists of three different type of phases. Planning, Execution and Reporting. In planning stage the TPA have to finalize the following important tasks, Content to audit, Time schedule of the auditing, duration of auditing, area of auditing, audit team size etc. The audit time and team size depends up on the size of the content. Execution is the important phases. In this phase we have to analysis the security threats in the cloud storage, monitor the previous threats and determine the level of previous threats. Also have to do the data integrity check. Reporting is the report of execution phase, this report will help the Cloud

service provider to improve their service. The third party audit report mention the complete details about the cloud user activities and performance of the cloud service providers. According to this audit report Cloud Service Providers can monitor the activities of the user, if any user acting like the attacker we can cancel the agreement. At the same time Cloud Service Provider can improve the service efficiency of the service by this audit report. Because this audit report indicate the both user and cloud service provider performance.

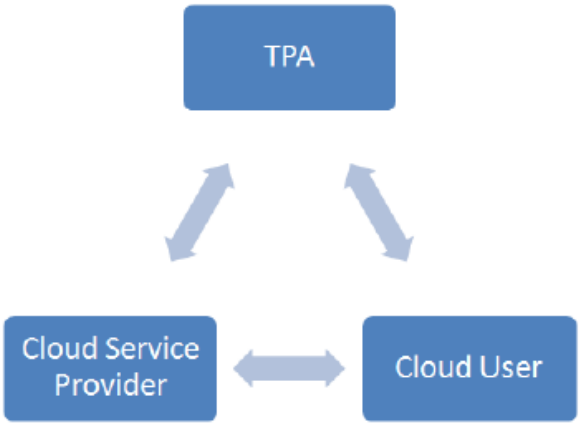


**Fig. 1 TPA in Cloud.**

Public Batch Auditing means TPA can do simultaneous integrity check on multiple cloud user's data, which stored in a multiple cloud.

## CONCLUSION

In this paper we explained different existing paper techniques and their merits and demerits. We discussed their methods of data security and privacy etc. In all those papers some haven"t described proper data security mechanisms, some were lack in supporting dynamic data operations, some were lack in ensuring data integrity, while some were lacking by high resource and computation cost. Hence this paper gives overall clue of all existing techniques for cloud data security and methods proposed for ensuring data authentication using TPA.

In this paper secure cloud storage privacy preserving public auditing system is proposed. Homomorphic linear authenticator and random masking is used 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 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.

Cloud computing security issues have brought us with great opportunities and challenges. Security in cloud computing can be addressed with TPA and without TPA. In the cloud computing by using the TPA mechanism we can increase the data security which is essentially a distributed storage system. To ensure each data access in control and reduce the complexity of cloud computing by help of Advance Encryption Technique (AES). In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. TPA can perform multiple auditing tasks simultaneously. Here Work is focuses on RC5 Encryption Algorithm for stored data in cloud. Resulted encrypted method is secure and easy to use.

## REFERENCES


- Abhishek Mohta, Ravi Kant Sahu and LK Awasthi, "Robust Data Security for Cloud while using Third Party Auditor" in International Journal of Advanced Research in Computer Science and Software Engineering, Vol No. 2, Issue 2,Feb 2012.
- Cloud Security Alliance, "Security Guidance for Critical Areas of Focus in Cloud Computing," http://www.cloudsecurityalliance.org, 2009.
- Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren, and Wenjing Lou (2013) Privacy Preserving Public Auditing for Secure Cloud Storage.
- D. Attas, and O. Batrafi, "Efficient integrity checking technique for securing client data in cloud computing", International journal of electrical & computer science, pp. 43-48, 2011
- Elsenpeter Robert ,Anthony T. Velte and Toby J.Velte, 2010. Cloud Computing A Practical Approach.
- K.D. Bowers, A. Juels, and A. Oprea, "Proofs of Irretrievability: Theory and Implementation," Proc. ACM Workshop Cloud

Computing Security (CCSW '09), pp. 43-54, 2009.

- Kan Yang, and Xiaohua jia (2013) An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing.
- P.Mell and t. Grance 2009. Draft Nist Working Definition of Cloud Computing, referred.
- Ravi Kant Sahu and Abhishek Mohta, L.K. Awasthi 2012. Robust Data Integration While Using Third Party Auditor For Cloud Data Storage Services, conf. IJARCSSE, Vol 2, Issue 2,ISSN: 2277 128X.
- S. Balakrishnan, G. Saranya, S. Shobana, and S. Karthikeyan, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of Computer Science and Technology, pp. 397-400, June 2011.