NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD

R.K.Ramesh 1, P.Vinoth Kumar2 and R.Jegadeesan3

1 M.Tech Student, Department of Computer Science and Engineering, S.R.M. University Chennai
2 Asst.Professor, Department of Information Technology, S.R.M. University Chennai
3 Ph.D Research Scholar Anna University Chennai (India).

ABSTRACT

Security is a major issue in cloud computing environment as the resources are dynamic, virtualized, scalable and elastic in nature. Data Integrity is to be 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.

Keywords: Cloud Computing, SLA, Auditing, Third Party Auditor.

I. INTRODUCTION

Cloud Computing is a new dimension scheme for IT industry. It provides the required scalable services 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 unaccessed 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.

1.1 Types of Cloud Services:

**Software as a Service (SaaS)** In this Service Users are provided access to software applications and Databases. This is also called as On Demand Software services. The cloud user need to pay to use the cloud software applications. **Infrastructure as a Service (IaaS)** the Cloud Service provider supply the resources on demand basis from their Data centers. The resources are Software bundles, Raw, Virtual local area networks, load balancers, firewalls, IP addresses, Virtual machine disk image library, file based storages. **Platform as a Services (PaaS)** the Cloud Service provider a computing platform to the program developers. Computing platform includes operating system, programming language execution environment, database, and web server. **Network as a Service (NaaS)** the Cloud Service provider provides network/transport connectivity services and/or inter-cloud network connectivity services to the users.

![Cloud Architecture](image-url)

**Fig. 1.1 Cloud Architecture**
1.2 Cloud Computing Models:

Private Cloud: This infrastructure owned by a single organization. Public Cloud: Open for public, that available in public networks. Need some more cloud structure and cloud security considerations.

Community cloud: belongs to several organization, they will share among this type of infrastructure. They will manage internally or by a third party.

Hybrid cloud: Combination of two or more Private, Public and Community clouds.

In private cloud, cloud is owned by private organization and they maintain their own auditing principles and process. Mostly private cloud will not connect with the public networks like internet, so the chances of external attacks is very low. The private cloud user are limited and easily can do monitoring. The public cloud connect with public network like internet and there is unlimited number of user can connect with public cloud depends upon the service providers capacity. The agreement SLA between cloud service provider and cloud user is not transparent to all Cloud users, so there is a chance of agreement violation.

1.3 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 issues arise in which entity can perform auditing. If auditing is done by Cloud providers they may hide their faults and violations. On the other hand if the user does the auditing, it adds the overhead to them. The solution is to have a third party entity to do the auditing. The third party should be neutral to both the Cloud provider and Cloud User.

1.4 Third Party Auditor (TPA):

1.5 The Cloud user send the data to Cloud service provider through the network. The user data may contains very sensitive data like user personal information, Bank details, Password, Important key Word, Business client details etc. Cloud service providers normally use Secure Socket Layer (SSL), Point to Point Tunneling protocol (PPTP), VPN for secure transaction. We are having history that attackers and intruders have win over this type of security services. While transferring the data between user and the cloud service providers very hard to avoid malicious attack. But users need assurance legally about the security over their data. For this we need a authentication mechanism based on the third party. This third party should common for both cloud user and the Cloud Service Providers. This third party monitor the activities of cloud user and cloud service provider. Normally cloud service providers and client will have a Service Level Agreement (SLA). This is a legal agreement between Cloud service provider and the client. Both parties have to follow the rules and regulations mentioned in the SLA. This agreement includes the Cloud service provider’s quality of service, Standard of the service, service monitoring and controlling. 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. 1.3 TPA in Cloud](image)

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

TPA is the external entity it supports the data integrity in the cloud. Cloud Service Providers transferring the data to cloud user from cloud server. Now the TPA have to check the integrity of transferred data. The process will be like this, The TPA will collect the receive data and send data to verify. If both data same, then there is no violation in the data integrity. Practically this is not possible for the large data. Also TPA also a external entity again if we give full set of data again data integrity question will rise in TPA end. For the multiple cloud and multiple users we need multiple auditing called batch auditing. We need to implement the new technique with Homomorphic authenticator and the bilinear aggregate signature method.

2.1 Components:

**Client**: Client uses the services provided by the owner. Client access the data provided by the owner through the Cloud server. But cloud server is an invisible entity to the Client. The Client should be an authenticated user to the data owner.

**Owner**: The owner use Cloud server to store the data. The owner provide datas to the end users through the Cloud Server. The owner provides on demand services to the user. The file to be sent is encrypted and placed in the Cloud server which is accessible by the user. The owner attaches a tag with the data to be sent so that auditor can verify the data using the tag.

**Cloud Server**: The Cloud server provides storage services to the data owner. The owner has to register with Cloud server to provide the use the storage services. Cloud server act as a platform to store the owner’s data to be accessed by the Client. Many owners can use the same Cloud server to provide services to their set of users.

**TPA**: The owner provides the datas to the Client through the Cloud server. The integrity of the data in the Cloud server is in question mark. The owner can verify the integrity of data in Cloud server by auditing. But having auditing in the owner is cost effective and it leads to headache to the owner. The solution is to have a Third Party Auditor to verify the integrity of data in the Cloud server. The Third Party Auditor is a neutral entity to the Cloud Server and the Owner. On behalf of owner the TPA will verify the owner’s data storage and security process.

TPA should be a trusted entity. But trusting a third party is not advisable. To ensure the privacy of the data, the data content is not available to the Third Party Auditor. The TPA verifies the encrypted data so that the privacy of the data is ensured. This can be done using Homomorphic authentication. The metadata is generated using Homomorphic authentication. The TPA disputes the Cloud server for the proof of data integrity. The Cloud server provides the proof which is verified against the owner’s metadata.
The TPA process works in three steps: Key Generation, Server integrity proof, integrity verification.

Key Generation: Key generation is done by the Owner. The data is encrypted using the private key of the owner and public key is transferred along with the data.

Server Integrity proof: TPA dispute the server to give a proof of data integrity. The server sends the proof.

Integrity Verification: On receiving the proof from the Server, TPA verifies the integrity without encrypting the data. The tag in the data helps the TPA to check the data efficiently.

The Auditing can be done periodically on samples of data. Over the period, the samples are collected and verification is done for the samples. This type of auditing falls under static category. On verification if the auditor is convinced with the data integrity, the auditor erases the local data.

2.2 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.

2.3 Batch Auditing:

Owner can use more than one Cloud server to store the data. Similarly the more than one owner can use the same Cloud server to store their data. If the owner user more than one cloud the auditor select the cloud severs to check the data integrity.

III. CONCLUSION

At present, cloud computing became a big computing paradigm. Number of cloud users and cloud providers grow rapidly. As the number of cloud providers increases, choosing a trusted service became tedious. The auditing mechanism is necessary to resolve the cloud integrity issues. There are various auditing framework proposed in cloud computing. But most of them are static in nature and they are implemented by cloud providers. In order to have dynamic monitoring, Dynamic Third Party Auditing System is proposed. The main advantage of the proposed system is that the data integrity is verified on dynamic data by the third party auditor. As the data integrity is verified by third party auditor, auditing becomes transparent to the Client.

The future work has to be done in concentrating on the scalability of the cloud services Auditing. Scalability is the main characteristics of the cloud. As cloud is highly distributed, the number of distributed nodes in the auditing process is a factor to be considered.
IV. REFERENCES


