Efficient Auditing Task Process In Cloud Environment For Improving The Data Security

Ashish Gontiya[1]
[1](Computer Science & Engineering , RGPV, Jabalpur, India ,ashishgontiya@gmail.com)

Abstract—*In the Cloud environment the major issue is security, as various researcher are mention in the various article or in the researcher paper. The simple definition of Cloud or cloud server is the different type of data and information save in cloud storage server or in other word we can say user are able to store the data or information in the cloud Server and fetch this data when the user required this data or information is also retrieve by the some other user in the well define manner. We are used signature Algorithm with Signature Algorithm key value data encryption. In this paper we are introduce the mechanism that support the public auditing task for the cloud data that store by the cloud user in the cloud storage so in this process the signatures algorithm is compute the data verification task or done the audit task in the cloud domain.*

Keywords—*Cloud Computing , Cloud Storage , TPA, Encryption , Decryption , Cloud Service Model , Cloud Deployment Model .*

1.1 Introduction of Cloud Computing

Cloud computing was coined for what happens when applications and services are moved into the internet "cloud." Cloud infrastructure provides extensive facilities for the client such as process, storage, power, networks, space and other computational possessions, so that the customer can set and perform their convention software as well as applications and operating system. More currently though, cloud computing refers to the many different types of services and applications being delivered in the internet cloud, and the fact that, in many cases, the devices used to access these services and applications do not require any special applications .It provides resources as a part of service using internet technology.With the increasing demand of security the servers are not secure enough to meet user's demand. definition provided by the National Institute for Standards and Technology NIST[1] (Badger et al., 2011),

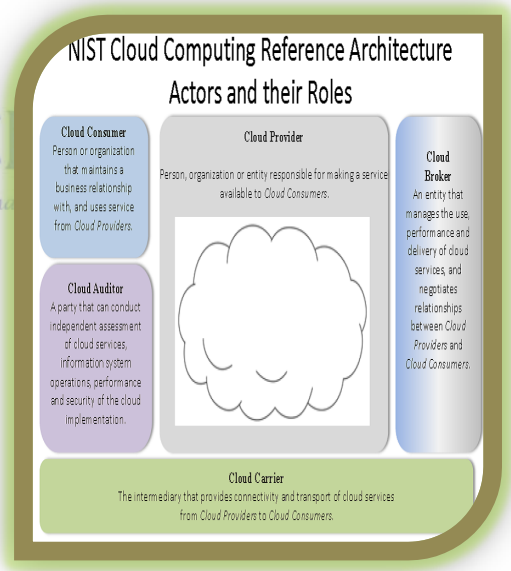

Figure 1.1Cloud Architecture

Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and justintime availability of resources". List of Companies that are provide the Cloud service as shown in the table 1.1 .

Service Provider Name	Service Description
Microsoft	Has Microsoft SharePoint online service that allows for content and business intelligence tools to be moved into the cloud, and Microsoft currently makes its office applications available in a cloud.
Google	Has a private cloud that it uses for delivering many different services to its users, including email access, document, applications, text translations, maps, web analytics, and much more.
Salesforce.com	Runs its application set for its customers in a cloud, and its Force.com and Vmforce.com products provide developers with platforms to build customized cloud services.

Table 1.1 Cloud Service Model

1.2 Cloud Computing Characteristics

The characteristics of cloud computing include ondemand self service, broad network access, resource pooling, rapid elasticity and measured service. Ondemand self service means that customers (usually organizations) can request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centers. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

1.3 Cloud Service Model

There are four basic cloud delivery models, as outlined by NIST , based on who provides the cloud services these service model are mention are as

1.3.1 IASS-This is the bottom layer of the cloud stack. It serves as a foundation for the other two layers, for their implementation. The keyword at the back this stack is virtualization. Usually plat form independent, infrastructure expenses are shared and thus abridged, service level agreements (SLAs), self scaling, pay by usage. Keep away from capital expenditure on hardware and human resources, reduced ROI risk; low barricade to entry, streamlined and automated scaling but shortcoming are business competence and productivity mainly depends on the merchant capabilities, potentially larger long term cost, centralization have need of new/different defense measures. With, a corporation can rent essential computing resources for deploying and storing data or running applications. IaaS enables express deployment of applications and get better the quickness of IT services by instantly adding computing processing command and storage capacity when necessary.

1.3.2 PASS — Consumers purchase access to the platforms, enabling them to deploy their own software and applications in the cloud. The operating systems and network access are not managed by the consumer, and there might be constraints as to which applications can be deployed. In PaaS, an operating system, hardware, and network are provided, and the customer installs or develops its own software and applications.PASS is used to avail the users with the platform required. Take the example of the .NET platform. The platform will be availed by the cloud server and again the user will have to pay for such work space [1] .

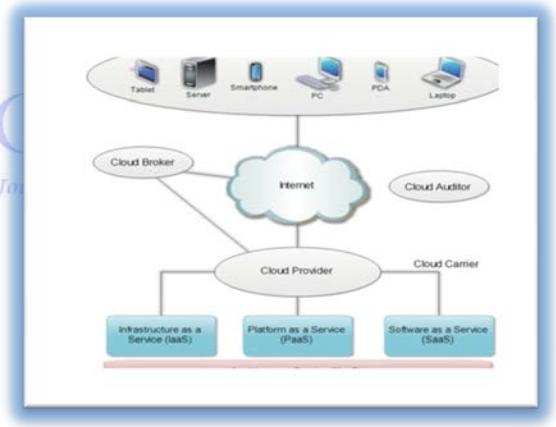

Figure 1.2 Cloud Service Model

1.3.3 SASS –In a Software as a Service model, a premade application, along with any required software, operating system, hardware, and network are provided. Consumers purchase the ability to access and use an application or service that is hosted in the cloud. A benchmark example of this is Salesforce.com, as discussed previously, where necessary information for the interaction between the consumer and the service is hosted as part of the service in the cloud. it covers all the software required by the user like Media Player , Job Schedulers etc.

1.4 Deployment Models of Cloud Computing

Deployment models define the type of access to the cloud, i.e., how the cloud is located? Cloud can have any of the four types of access: Public, Private, Hybrid and Community. Here I am introduce a brief introduction of cloud deployment model , these all the model are basically provide the facilities to user to use the cloud service in the very lower cost and without need of any other infrastructure . this is show the information or cloud technology that able to shifted this to in cloud environment.

1.4.1 Private Cloud –

This service of cloud computing is done in offline manner now here no need of internet facilities in the private cloud model manage and work with third party auditor .

1.4.2 Public Cloud –

This is a Public cloud now here in this service model public cloud is mage and organize it's example are Amazon cloud service .

1.4.3 Hybrid Cloud –

This is the combination of two cloud is call Hybrid cloud in hybrid cloud is the information are stored in private cloud environment after the manipulated by a program running in on the public cloud environment .

1.4.4 Community Cloud – The cloud infrastructure is collective by quite a few organizations and supports a precise community that has shared apprehension (e.g. Security, mission, requirements, considerations, or compliance policy). It possibly will be managed by the organizations or a third party and may exist on premises or off premises.

2 Cloud Security[2]

Cloud Computing, an emergence technology, has placed many challenges in different aspects Some of these are shown in the following diagram:

Figure 1.4 Cloud Security

4.1 Literature survey

Analysis of literature on the variants and methodologies of privacy preserving in cloud computing reveals the following: So many method are already exiting for auditing cloud content before storing cloud Environment , this will be done Third person or some time called TPA . Maggi and Zanero, addressed countermeasures (antiviruses, intrusion detection systems) developed to mitigate wellknown security threats. The focus is mainly on anomalybased approaches which are mostly suited for modern protection tools and not for intrusion detectors. The patternbased changes (example: from thin client connected to the main frame or powerful workstations connecting to thin clients) are observed, which cause some simultaneous changes in work environment and new problems to security of CC[3]The user might give his/her identity of proof certificate [4] This paper includes the problems of misuse of the proof of identity (POI) certificate if fallen into unauthorized person. However, public auditing on the integrity of shared data with these existing mechanisms will inevitably reveal confidential informationidentity privacyto public verifiers. Subashini and Kavitha, dealt with the security risks faced in the CC. The public mechanism proposed by Wang *et al.* [5]is able to preserve users' confidential data from the TPA by using random masking's. In addition, to operate multiple auditing tasks from different users efficiently, they extended their mechanism to enable batch auditing by leveraging aggregate signatures leveraged homomorphic tokens to ensure the correctness of erasure codesbased data distributed on multiple servers. This mechanism is able not

only to support dynamic operations on data, but also to identify misbehaved servers. To minimize communication overhead in the phase of data repair, Chen *et al.* [6] also introduced a mechanism for auditing the correctness of data with the multiserver scenario, where these data are encoded by network coding instead of using erasure codes.

Problem Definition

After Reading some research paper mention in section two that is literature review . I am find the some major problem in existing system. Now here Existing system is give the permission to user who upload the data in cloud environment , also give the permission public data verifier for performing a some operation on the uploaded data these operation are data integrity verification for this work public verifier download the all data from cloud data center for this work it used the public auditing . in the public auditing data or information is fragment into the more then one fragment or small block these block is include a information or data , these all data block is separately signed by the user .for data integrity checking full data will be fetched from the cloud data center at a time . the data auditing is done in public manner or in a Private manner in a private data auditing personal user is not show the data or information to public data verifier for checking purpose .so this is the main problem of I am solve in my dissertation work . as we all know that cloud is provide the facilities to Sharing data or information for more then one users. so It is very important to ensure the integrity of shared data in the cloud is ok or not .A public verifier could be a data user who would like to utilize the owner's data via the cloud or a thirdparty auditor (TPA) who can provide expert integrity checking services. But in the private data auditing it is not possible . so main problem in the existing system is data privacy is not available in cloud environment , not have privacy identity , and mainly no public verifier is available in the existing system .Auditing task where data will be shared after completion auditing task , this task is done by public verifier / auditor. So during literature survey I have read so many method describe for solving this problem . data will be audit by public verifier now here we just assume that a public verifier is doing his work honestly , solving this problem I have introduce a new cloud data public verifier architecture that supervise a working of third party public auditor .

Proposed Work

In this section, I am present our new architecture of public data verifier in highly secure manner. In my proposed work I am verify the public data auditor . Distributed access control of data stored in cloud by the private user for verification so this data is verify by the so that only authorized public verifier. only the registered user are able to modify their data on the cloud this will be only done by valid public auditor .in the proposed new architecture we try to protect the user identity during data verification this new proposed architecture is decentralized, it means that I am used so many key management that will be generate automatically by the modified algorithm .this new architecture supports multiple read and write on the data stored in the cloud.

Result /Out put Screen

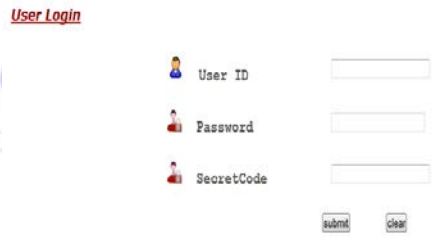

Figure 7.2 User Login Page

Figure 7.2 User Login Page

Reference

[1] Cloud Computing Security Issues Randy Marchany, VA Tech IT Security, marchany@vt.edu NIST Cloud

Computing erence Architecture & TaxonomyWorking Group Robert Bohn Information Technology LaboratoryJune 21, 2011

[2] A Three Party Authentication for Key Distributed Protocol Using Classical and Quantum Cryptography.

[3] Jaatun M., Zhao G. and Rong C., "Access Control of Cloud Service Based on UCON", CloudCom 2009, NCS 931, pp. 559564, 2009.

[4] Bertino, E.; Paci, F.; Ferrini, R. 2009 Privacypreserving Digital Identity Management for Cloud Computing, IEEE Computer Society Technical Committee on Data Engineering.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, “PrivacyPreserving Public Auditing for Data Storage Security in Cloud Computing,”in Proc. IEEE International Conference on Computer Communications (INFOCOM), 2010, pp. 525–533.

[6] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote Data Checking for Network Codingbased Distributed Stroage Systems,” in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp. 31–42.