International Journal of Multidisciplinary Allied Research Review and Practices

IJMARRP

ISSN No: 2455-1570 (Volume II, Issue XII, December 2016)

A Study on the Security of Database in Cloud

Pankaj Mudholkar[1], Shirshendu Maitra[2], Megha Mudholkar[3]

Assistant Professor

Thakur Institute of Management Studies,

Career Development and Research (TIMSCDR)Mumbai

***Abstract*—This Cloud database is seen as the next generation architecture of IT in which data is transferred between the server and client. The main issue in networking is the high speed whereas the current discussion in IT world is the security of the database. Our research paper will help to secure the data whereas it also protects cloud data from any unauthorized use. Cloud storage gives facility to their users to remotely store their data and they can also retrieve their data on-demand without any burden of hardware and software management**

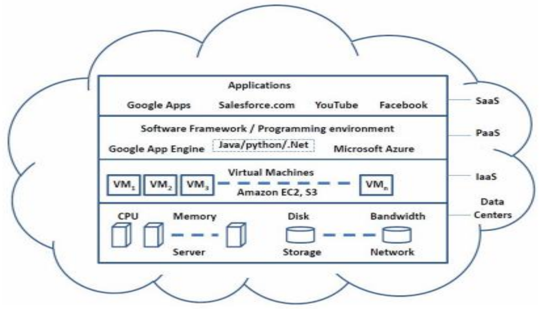
Keywords—component; formatting; style; styling; insert (key words)

I. Introduction

In Cloud computing the data is stored in data centers and not in personal PCs. The best definition of cloud is large pool of easily accessible data which can be dynamically reconfigured to adjust variable load. The cost of resources can be reduced by sharing the resources. Many trends are opening up era of cloud computing, which is internet based and by using computer technology. The key aspects behind the cloud computing is the omnipresence of broadband and falling storage costs, and progressive improvements in Internet computing software. The key technical supporting for cloud computing services include virtualization, service-oriented software, management of large facilities, and power efficiency. The internet-based online services do provide large amounts of storage space and computing resources, this computing platform shift, however, is eliminating the responsibility of local machines for data maintenance at the same time. From the view point of data security, which has always been an main aspect of quality of service, Cloud Computing poses new challenging security threats for many reasons. Firstly, considering several kinds of data for each user stored in the cloud and the demand of long term continuous assurance of their data safety, the problem of verifying correctness of data storage in the cloud becomes even more challenging. Secondly, The data stored in the cloud may be frequently updated by the users. In this paper work the first few ones in this field to consider distributed data storage in Cloud Computing and secure data transmission. The rest of the paper is introduces the system model, introduce adversary model, introduce our design goal and security architecture. Then we are providing Security framework for server and client network. Then we provide the detailed design of the system and detailed about data transmission in and finally, the concluding remark of the whole paper.

II. Cloud Computing Building Blocks

The cloud services can be divided into three categories: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).



A. *Software-as-a-Service (SaaS)*

It can be described as a process by which Application Service Provider (ASP) provide different software applications over the Internet. This makes the customer to get rid of installing and operating the application on own computer and also eliminates the tremendous load of software maintenance; continuing operation, safeguarding and support [1]. Examples of SaaS includes: Salesforce.com, Google Apps.

B. *Platform-as-a-Service (PaaS)*

It is the delivery of a computing platform and solution stack as a service without software downloads or installation for developers, IT managers or end-users. It provides an infrastructure with a high level of integration in order to implement and test cloud applications. The user does not manage the infrastructure (including network, servers, operating systems and storage), but he controls deployed applications and, possibly, their configurations. Examples of PaaS includes: Force.com, Google App Engine.

C. *Infrastructure-as-a-Service (IaaS)*

It refers to the sharing of hardware resources for executing services using Virtualization technology. Its main objective is to make resources such as servers, network and storage more readily accessible by applications and operating systems. Thus, it offers basic infrastructure on-demand services and using Application Programming Interface (API) for interactions with hosts, switches, and routers, and the capability of adding new equipment in a simple and transparent manner. Examples of IaaS includes Amazon Elastic Cloud Computing (EC2), Amazon S3, GoGrid.

III. CLOUD DEVELOPMENT MODELS

A. *Private cloud*

It can be owned by the organization or a third party and it is more expensive and secure when compared to public cloud. In this cloud there are no additional security regulations, legal requirements or bandwidth limitations that can be present in a public cloud environment. One of the best examples of a private cloud is Eucalyptus Systems [2].

B. *Public cloud*

This cloud infrastructure is provided to many customers and is managed by a third party and multiple enterprises can work on the infrastructure provided, at the same time and users can dynamically use and access the resources. Customers are only charged for the resources they use, so under-utilization is eliminated. Examples of a public cloud includes Microsoft Azure, Google App Engine.

C. *Hybrid cloud*

It is composition of two or more cloud deployment models, linked in a way that data transfer takes place between them without affecting each other. An example of a Hybrid Cloud includes Amazon Web Services (AWS).

D. *Community cloud*

The infrastructure which is shared by several organizations for a shared cause and may be managed by them or a third party service provider and rarely offered cloud model. An example of a Community Cloud includes Facebook.

IV. SYSTEM MODELS

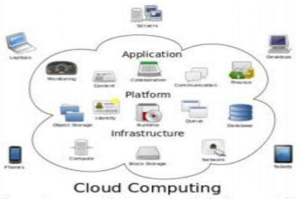


Figure 1 - general structure of clod computing

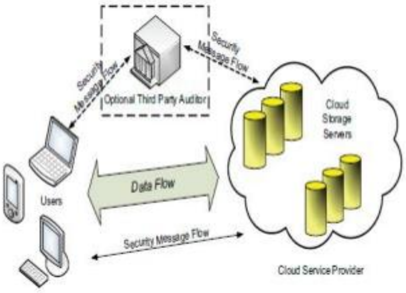


Figure 2 – cloud data storage architecture.

Fig. 1 and 2 indicates the Representative network architecture for cloud data storage and three different network entities are as follows:

- User
- Cloud Service Provider (CSP)
- Third Party Auditor (TPA)

A user reserves his own data with the help of a CSP into different types of cloud database servers which are functioning in a concurrent, unite as well as appropriated manner. Data redundancy can be employed with technique of wiping out correcting code to further tolerate faults or server crash as user's data grows in size and importance. Thereafter, for application purposes, the user communicates with the cloud servers by using CSP to retrieve his data. In some of the cases, the user may need to perform block level operations. In our model, we assume that the point-by-point communication channels between each and every cloud server and the user is authenticated and reliable. Security problems faced by cloud data storage can arise from two different sources. A CSP can be self-interested, un-trusted and possibly malicious. Also there exist an economically motivated adversary, who has the ability to accommodate a number of cloud data storage servers in different time intervals and afterward is able to change users' data while remaining undiscovered by CSPs for a convinced period.
Specifically, we consider only two types of adversary who has different levels of capability in this paper:

a) Weak This adversary is interested in corrupting the user's data files stored on individual servers by modifying or *introducing its own fraudulent data to prevent the original data from being retrieved by the user.*

b) Strong

This is the worst case, in which we assume that the adversary can compromise all the storage servers so that he can intentionally change the data files as long as they are internally persistent. In fact, this is equivalent to the case where all servers are colluding together to hide a data loss or corruption incident.

V. DESIGN GOALS

For ensuring the dependability and security of cloud storage under the adversary model, we intent to design mechanism for dynamic data verification and conclude the following goals:

A. Correctness of storage:

It ensures users that their data are absolutely stored accordingly and kept perfect all the time in the cloud.

B. Fast detection of data error:

It adequately locates the improper functioning of server when data corruption has been detected.

C. Support for dynamic data:

It keeps the same level of storage correctness guarantee even if users change, wipe out or add their data files in the cloud.

D. Less weight:

It enables users to perform storage correctness checks with minimum overhead.

VI. SECURITY ARCHITECTURE

There are many researcher have intense interest in designing security architectures which help for secure cloud computing database. The following are described below: Gary Anthes [3] has described the various security research works in cloud and he brought forward the research works done in companies like IBM, HP, and Microsoft. There is lots of security risks involved in cloud computing, which are pointed below.
1) Research department of HP are prototyping cells as a service to automate security management in cloud.
2) IBM research people doing virtual machine introspection which puts security inside protected VM running on same machine. This applies number of protective methods listing the kernel functions.
3) Microsoft research people described about the cryptographic cloud storage where the data is secured by user by encrypting functions which will encrypt the data which is not understandable such that the provider cannot get what the data is present.
Flavio Lombardi and Roberto Di Pietro has discussed [4] about a secure virtualization technique for ensuring security at hypervisor level. In a general system at base OS level, there is a problem like a user at one guest OS may interact with other Guest OS, which may lead to data loss if they are any attackers. So the new proposal ACPS (Advanced Cloud Protection System) was introduced. This will maintain security by preventing unnecessary logins into the other guest OS
by weak passwords or weak SSH. Cong Wang [5] has proposed their work on Data Storage security with respect to Quality of service. They have proposed approach which checks whether their data has been attacked or any integrity loss is done or not over the cloud. They will generate a homomorphism token which will ensure that the data is not lost. It is like a simple hash function which will be enabled to fast recover and storage errors. These works help in securing the cloud systems, Virtualization, Data confidentiality and data storage security, there are still issues need to be discussed in secure data transmission between cloud Provider, service provider and cloud User. The secure data transmission is anyhow achieved by protocols like IPSec, SSL over web and the data over are also through web applications these current methods can be used for secure data transmission. The secure data transmission works designed for storage networks are discussed by Kikuko Kamiasaka [6] who discussed in his paper for secure data transmission over IP Networks by developing Middleware works below application layer and selects suitable security approach based on the cluster of data items available in Application. This was proved that will help in securing the data as well as this works well than IPSec. Sudha M has proposed an idea for secure data transmission in cloud computing using transport layer techniques, the idea proposed in that is used is socket programming for secure data transmission over the client and server. This paper has compared the general secure data transmission by applying socket programming, a key exchange and secure data over cloud. The comparison is done response time and processing time.

VII. SECURITY FRAMEWORK FOR SERVER-CLIENT NETWORK

In the new design architecture (Figure 3) which is designed for private cloud consists of new security layer and it is present between transport and session layer and also it is transparent for application and other lower layers. When client sends data first it is authenticated by certain protocols and after that the data will be saved on the server side. So, the data will be saved on the sever side in secured manner.

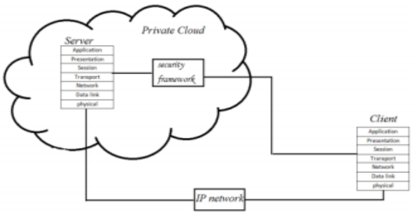


Figure 3– high level design

VIII. DESIGN OF THE SYSTEM

A. *Security Framework Model*

Figure 4 shows the detailed design frameworks of security mode whose nodes which are connected to server will be also connected to security layer. Whenever user wants to send some data to private cloud then he needs to choose certain algorithms of security which are based on the documents privacy level. If user wants more security for his data in cloud then they need to choose more strong security algorithm. The security servers will save the data inside database securely.

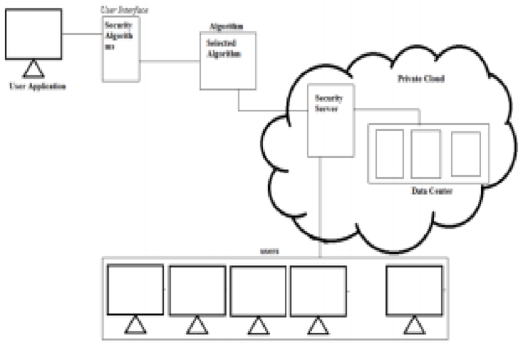


Figure 4– system architecture

B. *Process at sender*

The client will set all his data and encrypts his data by selecting the most appropriate algorithm from the interface and sends that data to the server. As Figure 5 indicates that client end read the data and ready to send his data. Before sending the data to the remote end at the socket layer the data will be encrypted byte by byte and send encrypted data. The protocol will carry forward the data the other commands which will happen in network. Therefore, data will be secured by security framework at the sender side which helps in securing data transfer.

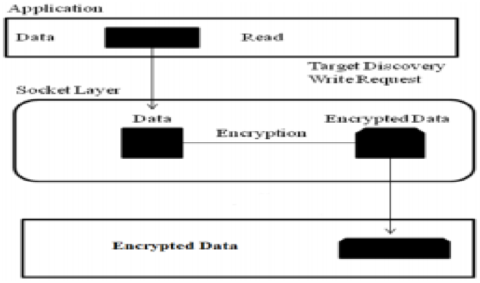


Figure 5: process at the sender

C. *Process at receiver end*

The receiver end (Figure 6) when received the data the data will be decrypted by security algorithm which was used at sender end. This also worked just above the transport layer where packets at end application. The protocols give the write request and the security framework decrypts the data and saves on the disks. The same process will be happened when the client requests file from server. This ensures that data is secure over the network and we can also have integrity and confidentiality check at the receiver side.

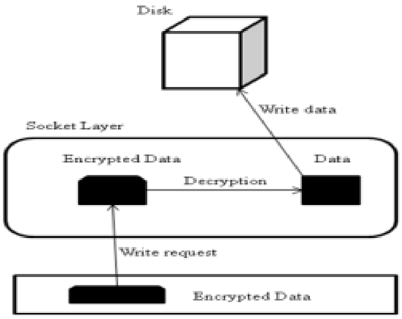


Fig 6: process at the receiver

IX. CONCLUSION

In our research paper we studied the different problems which arise in cloud data storage and during transmission of data. For ensuring the correctness of data we invented a useful and flexible shared scheme, this scheme achieves the data integration of insurance for correctness of storage and indication of error. In transmission of data the data is encrypted in upper layer instead of using IPSec or SSL on the top of transport layer. Therefore, the performance improvement scheme can be applied without modifying IP layer implementation. The security is applied in background to the data by using some standard algorithms of encryption such as AES, DES. After detailed performance analysis it is visible that our scheme is much efficient to resist modification attack or unauthorized access whereas many research problems are still need to be identified.

X. References

[1] "Security and Privacy Challenges in Cloud Computing Environments" co-published by the IEEE computer and reliability ieee november/december 2010

[2] Boris Tomas1and Bojan Vuksic2 "Peer to Peer Distributed Storage and Computing Cloud System" International conference on information technology interfaces, june 25-28, 2012, cavtat, croatia

[3] Gary Anthes, "Security in the cloud," In ACM Communications (2010), vol.53, Issue11, pp. 16-18.

[4] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications (2010), doi:10.1016/j.jnca.2010.06.008.

[5] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011) vol. 34 Issue 1, January 2011 pp. 1 - 11.

[6] Balachander R.K, Ramakrishna P, A. Rakshit, "Cloud Security Issues, IEEE International Conference on Services Computing (2010)," pp. 517-520.