International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

DATA SECURITY IN THE CLOUD

Mr. Jiten Prithiani MCA Final year Student ,V.E.S. Institute of Technology, Mumbai, India jiten.prithiani@ves.ac.in,
Mrs. Dhanamma Jagli, Department of MCA, V.E.S.Institute of Technology ,Mumbai, India, dhanamma.jagli@ves.ac.in

Abstract

As there is a lot of development in the cloud computing, security of the data in the cloud has become the one of major aspects in the cloud computing.Cloud computing is nothing but the sharing of the resources in an open environment which leads to the security problems.

Introduction

WHAT CLOUD SECURITY IS:
Cloud security is a set of security principles which is applied to protect the data from the unauthorized users which are not reliable.

WHAT IS THE NEED FOR SECURITY:
As in the cloud the data is stored in a distributed system we have to maintain the security of the data distributed across the several system. Along with the security, atomicity of the data should also be maintained.

Cloud Storage is defined as storage of the data online in the cloud which is accessible from the
Multiple distributed resources which are connected with each other and comprises of the cloud.
Cloud storage provides some of the important benefits as follows:
1) Greater accessibility and reliability.
2) Good protection for data backup.
3) Lowers the overall Costs.
4) Manage the expensive hardware
5) Maintain the expensive hardware.
6) Determine the root cause of the Cyber-attacks.

There are many benefits provided by the clouds for storage of data and also have the potentials for security concerns related to the traditional storage systems.
Cloud Security is Security of the principles applied to protect the data, applications, infrastructure associated within the cloud computing technology.

Types of Cloud models :

1) Public Cloud: It is a type of cloud computing model in which service provider provides resources to the general public over the internet.

.2)Private Cloud: It is a type of the cloud computing models which provides the same features same as that of the public cloud but it is dedicated to only single organization.
3) Hybrid Cloud: It is combination of both private and public cloud service which performs distinct functions within same organization.

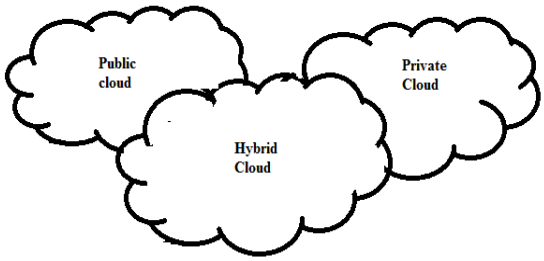

Figure 1: Types of Cloud

Literature Survey

Data: It is the any form of the information which is to be conveyed to and from others.
Security: It is the degree of the protection from an external harm.
Cloud: It is most often a metaphor of an internet and also a datacenter for all the servers that are connected to the Internet
Data Security in the cloud has become one of the most important and primary factor not only in the IT industry but also in various domains which include storage of data in a much secured method.

Related work:

Cloud Computing delivers wide range of the resources to the users via internet.The major Cloud providers those who provide the services to the users for storing the data includes AMAZON,GOOGLE, IBM, MICROSOFT, SALES FORCE, etc.
As the number of the resources are increasing for the usuage and storage of the data, it has become necessary to improve the security for protecting the data of the potential users using cloud.

There are two main scenarios which gives idea about where the security of the data resists inside the cloud.

1) Unauthorized access of the data between network and the cloud:

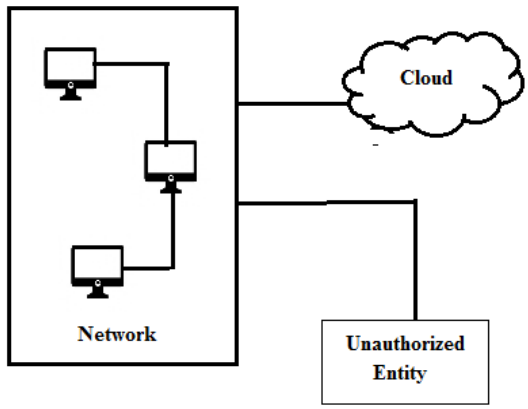

Figure 2: Access of the data between network and the cloud

In the above diagram the critical data resides in the network itself and in this case the cloud provider can not have any privilege of the data which is residing inside the network.
It showcases the typical types of the attacks that data inside the network can have.
These attacks are Passive attacks and Active attacks.

Passive attacks include the traffic analysis of the data residing inside the network.
Active attack includes Masquerading, DOS, Replay attacks, Modification of messages.

These attacks are likely to happen when the information is transferring client network to the cloud network.

2) Unauthorized access of data within the cloud.

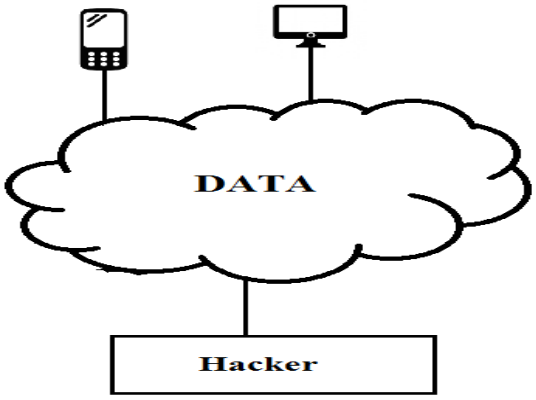

Figure 3: Access of data within the cloud

In the above system, the data is stored inside the cloud itself, where all the potential users of the cloud can access their data physically.While accessing the data from the cloud there is a possibility that an unauthorized user enters in the cloud and access the data in cloud.In this scenario, the machines which are virtual are allotted to the users of the cloud and these machines have their valid logins.
These valid logins are known to the valid and authorized users of the cloud but there is
Possibility that these logins can Cracked by the hackers

Proposed System:

5.1Working:
This process shows how we encrypt the data so that the intruder does not know what the actual data is about.
In this we use Data Masking and along with it the padding of data is applied.

1) Senders side:

Diagram

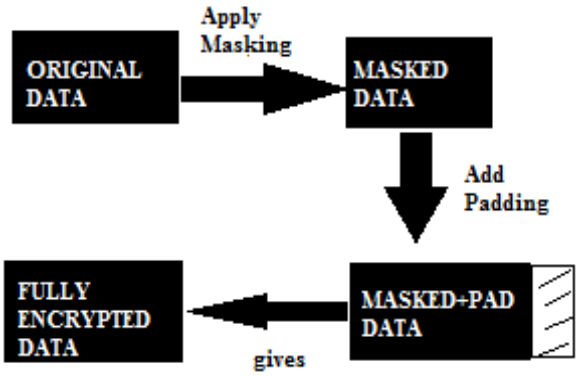

Figure 4: Encyption at senders side

Explanation:

In the above diagram, the encryption process takes place at the socket layer of the sender side.
The diagram shows us that the mask is applied to the data so that the original data is not being reflected to intruder.
After masking, the data which is masked is applied with the padding and hence the data is much more secure than it was before.
It gives us the double encryption of the data and hence the data is much more securely transferred to the receiver.

ISSN:2319-7900

2) Receiver side:

Diagram:

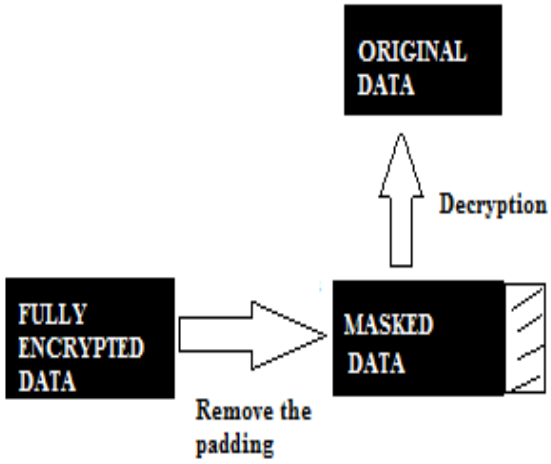

Figure 5: Decryption at receivers side

Explaination:

At the receiver side, reverse the process of the sender happens.
In this as shown in the diagram, the data which is encrypted doubly is being decrypted doubly.
At first the Padding of the data is removed and after the removal of the padding we obtained the masked data.
Now the masking of the data is being removed and hence the receiver obtains the original data.

5.2 Categories or types of the services offered by cloud

Diagram:

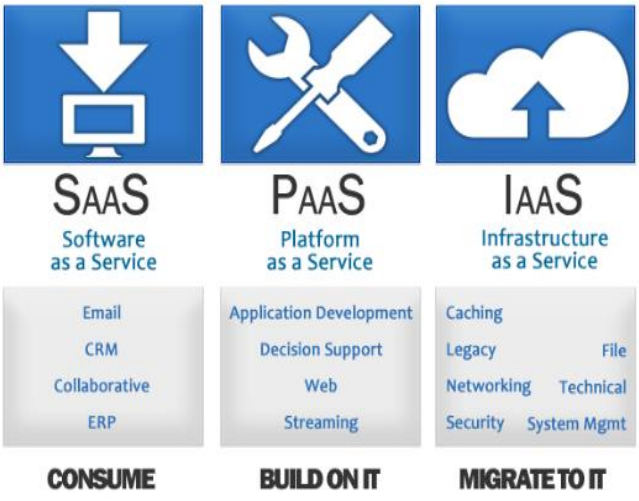

Figure 6: Types of the services

Explanation:

SaaS: Software as a service is a distribution model in which applications are hosted by vendor or service provider and made available to the customers over the network i.e Internet. This cloud service model offers anywhere access but along with this security is also increased.

PaaS: Platform as a service is a service model that delivers applications over the internet.In this cloud provides various hardware and software tools to the users as a service those are needed for the application development. This model requires strong authentication to identify the users.

IaaS: Infrastructure as a Service model hosts servers, hardware, software and many more infrastructure components on behalf of its users. It also handles the task such as system maintenance, system backup, etc. It is well suited for the system that frequently changes unexpectedly due to the workload or other options.

System Architecture:

Security algorithms are used for protecting the data from attackers. These algorithms are based on how confidential the data is for the user. More confidential the data is strong is the security algorithm which is to be selected. The security server will help us to secure the document and save it inside security server itself. When any user connected to that network wants to access the document then it should be connected to that security server only to get the original document of the data. This helps in security and privacy of the data.

Process flow at sender's side:

Diagram:

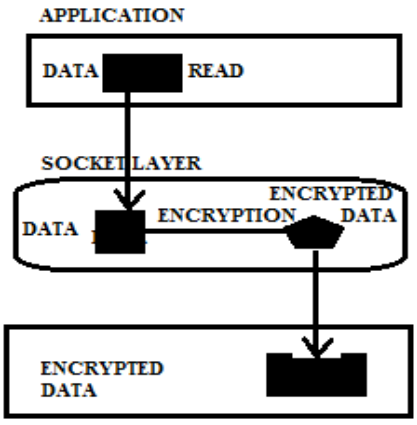

Figure 7: Process flow at sender's side

ISSN:2319-7900

Explanation:

The data at the senders side is set by the user. User then selects the appropriate approach for the encryption of the data with help of user interface. At the senders side data is only read and before sending it to the receiver's side remotely each byte of the data will be encrypted and then this encrypted data is sent remotely.

The data is carried to other end with the help of the protocols to process the commands. The data will be securely transferred from sender and security framework helps in securely transfer the data.

Process flow at receiver's side:

Diagram:

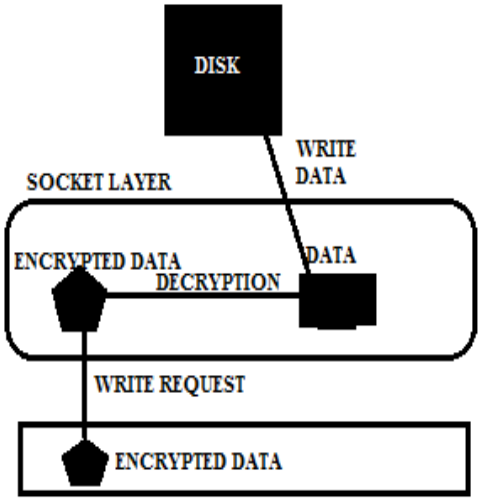

Figure 8: Process flow at receiver's side

Explanation:

At the receiver, the data is received and then it is decrypted and after decryption of data, it is written on the disk. The decryption will be done with the same security approach used at the senders end for the encryption. This who;e process occurs above the transport layer where packets arrive. The protocols then give the write request and security frame work then decrypts this data and after decryption of the data it is saved on a disk.

The same process continues over both the ends. This ensures us that the data sent over the network is in a secure mode. In this way the confidentiality and the integrity of the data at the receivers end is been repainted and ensure secure data checks.

Conclusion:

Storage of the data on the cloud refines the way we construct the data, manage the storage of the data and access the data from the cloud storage. Data stored on the cloud is considered as much more secure than storing the data on the transient servers. In this it is also motioned about the various Cryptography algorithms which helps us in encrypting the data at the senders side and then transferring it to receiver with help of secure channel and different types of keys.

References:

[1] Raj kumar Buyya Cloud computing:Vision ,Hype and delivering IT Services.

[2] Subashini S, Kavitha V., "A survey on security issues in service delivery models of cloud computing," Journal of Network and Computer Applications (2011).

.

[3] Steve Mansfield-Devine, "Danger in Clouds", Network Security (2008),.

[4] www.wikipedia.org

[5] Lombardi F, Di Pietro R. Secure virtualization for cloud computing. Journal of Network Computer Applications(2010)

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

[7] R. Latif, H. Abbas, S. Assar, and Q. Ali, "Cloud computing risk assessment: a systematic literature review," in Future Information Technology.

[8] Z. Mahmood, "Data location and security issues in cloud computing," in Proceedings of the 2nd International Conference on Emerging Intelligent Data and Web Technologies.

[9] M. Y. A. Younis and K. Kifayat, "Secure cloud computing for critical infrastructure: a survey," Tech. Rep., Liverpool John Moores University, Liverpool, UK, 2013.

[10] R. Neisse, D. Holling, and A. Pretschner, "Implementing trust in cloud infrastructures," in Proceedings of the 11th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing

[11] Patrick McDaniel, Sean W. Smith, "Outlook: Cloudy with a chance of security challenges and improvements,"

Authors:

Mr. Jiten Prithiani

Short Biography:

Jiten Prithiani is currently a final year MCA student in Vivekanand Education Society's Institute of Technology (V.E.S.I.T), Mumbai.

He had completed his Bsc (I.T) graduation in the year 2013. He had secured 99.43 percentile in the MAH-MCA CET Examination. He has an abiding interest in Software Engineering and programming languages like Java.

Mrs. Dhanamma Jagli

Short Biography:

Mrs.Dhanamma Jagli is an Assistance professor in V.E.S Institute of Technology, Mumbai, currently Pursuing Ph.D in Computer Science and Engineering and received M.Tech in Information Technology from Jawaharlal Nehru Technological University, Hyderabad and Andhra Pradesh. She has 12 Years Plus teaching experience at the post graduate and under graduate level. She had published and presented papers in refereed international journals and conferences. Her areas of research interest are Data Mining, Cloud Computing, Software Engineering, Database Systems and Embedded Real time systems. She has been associated with Indian Society of Technical Education (ISTE) and Computer Society of India (CSI) as a life member.