Security Issues in Infrastructure as a Service

Adesh Kumar
SLBSRSV, New Delhi, India

Abstract- Cloud computing is the most popular and burning topic in current scenario. Cloud computing allows less money investment in computing by cloud users. Cloud computing allows cloud users to use cloud services as needed without the being worried about the costly hardware and software implementation by cloud service provider. The cloud users do not need to buy costly software and hardware but only what they need are to use hardware and software which are provided by cloud service provider. Different users can use different types of service on cloud. The internet pays a crucial role in providing cloud services to the users. The user's data may be stored at server of cloud and users do not know the location of their data where the data is actually stored. So data security is a big concern in cloud computing. The CIA (Confidentiality, Integrity, Availability), Authenticity and Privacy are essential concerns in cloud computing. There are stacks of service layers in cloud computing and Infrastructure as a Service (IaaS) is the foundation layer hence security in this layer is very crucial and which can affect other layers too. In this paper I will discuss about the security issues in Infrastructure as a Service (IaaS).

Keywords- Cloud, Infrastructure, Service, Security

I. Introduction

In cloud computing computer resources such as computer hardware, software, networks, database and computing time are provided on pay per uses basis to the cloud users. In cloud computing the cloud user do not have direct access to cloud resources instead cloud resources are provided in form of services. Cloud computing is a technique or model in which all computer resources are made available to the user on pay per use basis. A cloud user can buy any computer resource as per his/her requirement for limited period of times. The cloud users can pay only how much resources are consumed by them and for how much time they have used them. Cloud can be deployed differently as per requirement. The cloud deployment model can be categorized as private cloud, public cloud, community cloud and hybrid cloud. There are various services which are provided on cloud by cloud service provider such as Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), Network as a Service, Security as a Service (SaaS) etc.

A. Cloud Deployment Models-

- *Public cloud-*

  A public cloud is design in such a way that it is always available for public to meet their service demands. Anyone can buy cloud resources from this type of cloud.
- *Private cloud-*

  A private cloud is designed for a specific organization to meet its requirements. In private cloud only the person of that organization can use private cloud and avail services available on private cloud.
- *Community cloud-*

  A community cloud is designed for a specific community such as musician, player, scholars etc.
- *Hybrid cloud-*

  A hybrid cloud is combination of two or more clouds. The participants of this cloud may private cloud, public cloud or community cloud.

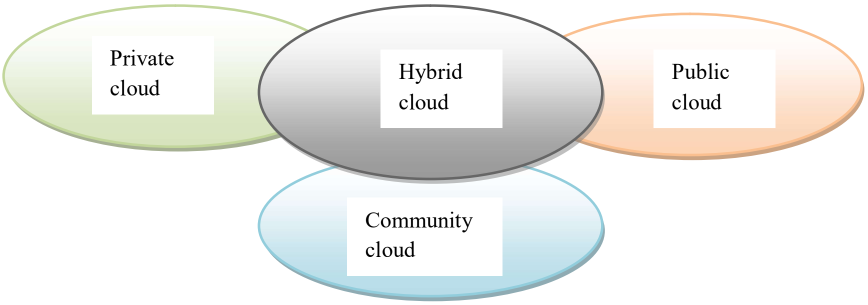

Figure 1. Cloud Deployment model

B. Cloud Service Model-

- *Software as a Service (SaaS)-*
  The application softwares are provided to the cloud user as a service in Software as a Service (SaaS). The cloud users buy the applications or softwares as per their requirements through this service model.
- *Platform as a Service (PaaS)-*
  In these types of service model, platform is provided to cloud users so that cloud users can install and run their softwares on that platform.
- *Infrastructure as a Service (IaaS)-*
  In this type of service model infrastructure is provided to the cloud users so that the cloud users can use cloud's infrastructure. The cloud infrastructure includes processing power, network, storage etc.
- Security as a Service-
  In security as a service the security management of the organization is handled by cloud service provider. The cloud service provider is responsible to tackle all the threads and security issues of the organization which buy security as a service from cloud service provider.

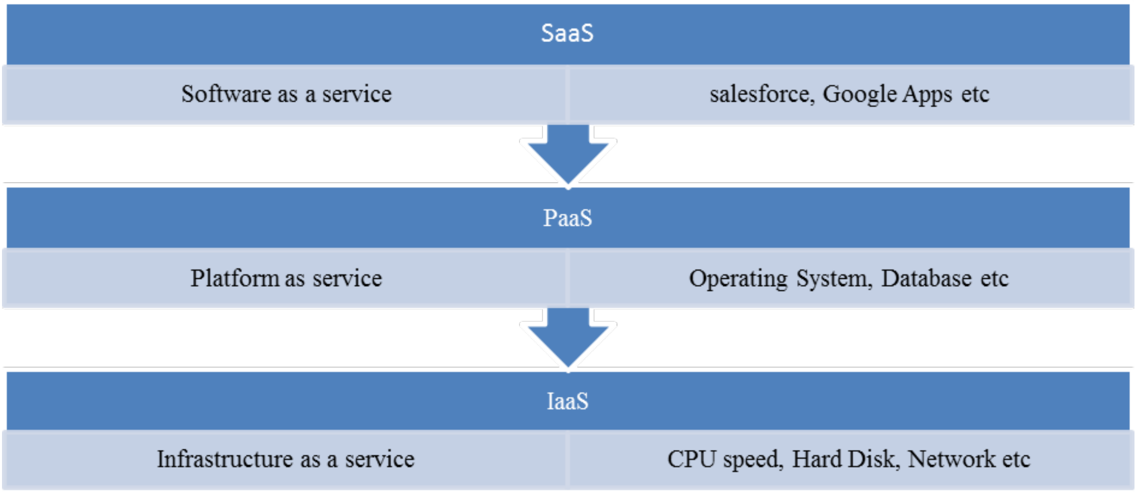
SaaS
Software as a service
salesforce, Google Apps etc
PaaS
Platform as service
Operating System, Database etc
IaaS
Infrastructure as a service
CPU speed, Hard Disk, Network etc

Figure 2. Cloud Service model

II. SECURITY ISSUES IN IAAS

Security is the main concern in cloud computing implementation. Cloud service provider must ensure that the data of cloud user will be stored safely and securely. The cloud users usually don't have knowledge the physical location of their data storage. There are usually many servers that form a cloud and each server may be located at different place. So date move from one location to another most of the times. This makes data security more challenging. Security issues vary with cloud deployment models. If it is private cloud then security threats are less for data because data is stored locally and there are limited users that can access private cloud. The security issues are as follows:

A. *Confidentiality-*

The information of cloud user should be kept safe and secure. Information store in database can not be accessed by unauthorized users intentionally or unintentionally.

B. *Integrity-*

The data stored in cloud database must not be changed accidentally or intentionally. The Integrity is the guarantee that message sent will be the message receives by destination machine.

C. *Availabily-*

The cloud resources must be available so that cloud users can access them reliably and timely.Availability garanties that cloud resources will be available when needed.

D. *Data Location-*

Data location is not visible to cloud users specially in public cloud. Data may be in motion from onle location to another. Hence extra security should be applied by cloud service provider to protect user’s data.

E. *Multi-Tenancy Risks-*

Multi tenacy arises the risk of data isolation. Many different types of users use the public cloud. So in public cloud data isolation is challenging.

F. *Data Loss or Leakage-*

The cloud service provider must ensure that user data will not be lost or theft.

G. *Maintenance-*

The cloud hardware resources should be maintaine properly and checked periodicaly so that data can not be lost due to falure of hardware resource.

III.CONCLUSION

In this paper I have discussed the main security issues in Information as a Service (IaaS) of service stack model of cloud computing. The Benefits of cloud computing are very much but lots of benefits also bring lots of challenge to implement security at IaaS level. There are many service layers on service stack of cloud and security should be implemented at each service level. Public clod and private cloud may have different type of security but security is essential part of a successful cloud implementation.

REFERENCES

[1] R. L. Krutz and R. D. Vines, “Cloud Security: A Comprehensive Guide to Secure Cloud Computing”, Wiley Publishing, 2010

[2] J. W. Rittinghouse, and J. F. Ransome,” Cloud Computing: Implementation, management and Security”, CRC Press, 2010

[3] Cloud Computing Security: A Trend Micro White Paper, May 2010

[4] W. Juang and Y. Shue. “A Secure and Privacy Protection Digital Goods Trading Scheme in Cloud Computing”, 2010

[5] F. Douglis, “Staring at Clouds”, IEEE Internet Computing, June 2009

[6] W. Jansen,And T. Grance, DRAFT: Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of

[7] Commerce, Special Edition 800-144, January 2011

[8] S. Singh and T. Jangwal, “Cost breakdown of Public Cloud Computing and Private Cloud Computing and Security Issues”

[9] International Journal of Computer Science & Information Technology (IJCSIT) Vol 4, No 2, April 2012

[10] R. Kean, et al., the Security for Cloud Computing: 10 Steps to Ensure Success, White Paper, Cloud Standards Customer Council, August 2012