International Journal of Trend in Research and Development, Volume 3(2), ISSN: 2394-9333
www.ijtrd.com

Understanding Cloud Computing Service Model and Security Issues in IaaS

Baljit Saini,
Lecturer, Computer Department, K.D.Polytechnic Patan,Gujrat

Abstract: Cloud computing becoming trend in these days. IT organizations are transforming in cloud computing. Cloud computing reduces cost .Users can access resources and data while they are sitting far away. Privacy, Confidentiality, Authenticity are main security issues in cloud computing. In this paper we will discuss various components of IaaS and its security issues.

Keywords: *Cloud computing, SLA, Virtual Machine, API*

I. INTRODUCTION

Cloud computing refers [1] to applications and services that run on a distributed network using virtualized resources and accessed by common Internet protocols and networking standards. The use of the word cloud makes reference to the two essential concepts:

- **Abstraction:** Cloud computing abstracts the details of system implementation from users and developers. Users are not aware about the physical location of the system where application and software runs and also they do not know physical location of data centre where data actually store.
- **Virtualization:** Cloud computing works on the concept of virtualized systems..in this system user pay as per the resources he used. Users also pay for space which he utilized.

Basically there are two different [2] classes of Cloud Deployment model and service model. Deployment model tells location and purpose of cloud. Public, Private, Hybrid clouds are deployment model. Service model tells type of service cloud provides. Software as a Service, Platform as a Service, and Infrastructure as a Service are service models.

Cloud Computing is a growing field. Information Technology companies started to adopt it as a important unit. Safety is main concern as more and more information on individuals and companies are placed in the cloud. Consumers declined to use cloud due to security reasons. Privacy and data security are main hurdles in the success of cloud computing.

II. SERVICE MODEL

In service model cloud provide service to users. Basically there are three types of services:

A. IaaS

Infrastructure as a Service model uses various hardware components to provide services to users. Hardware resources can be machines, storage, infrastructure, and other hardware resources which work virtually for the clients. Service provider handles whole environment and the services which are given to the users. Customers use those services virtually at their end.

B. PaaS

Platform as a Service model uses machines, operating systems, applications, services, development frameworks, transactions, and control structures virtually. User can install its applications on the cloud infrastructure or use applications that were programmed using programming languages languages that are supported by the service provider. The service provider handles the cloud infrastructure, the operating systems, and the software. User installs and manages the application that he is using.

C. SaaS

Software as a Service is a model which uses applications, operating environment and user interfaces. Thin client interface is used in this model to provide services to users. User is responsible to manage his data. These three different service models combination is known as the Service Platform Interface (SPI) model of cloud computing.

III. IaaS COMPONENTS

IaaS [10] delivery model is a combination of several components that have been developed through past years nevertheless, combining all those components together in a shared and outsourced environment is challenging tasks. Main hurdles in cloud computing adoption are Security and Privacy. Security violation in any component effect on the security of other components.

A. Service Level Agreement (SLA)

A Service Level Agreement (SLA) is [3] the contract for performance negotiated between user and a service provider. SLAs usually specify these parameters: Availability of the service (uptime), Response times or latency, Reliability of the service components, Responsibilities of each party, Warranties, SLA includes SLA contract definition, SLA negotiation, SLA monitoring, and SLA enforcement. SLA contract definition and negotiation stage is important to determine the benefits and responsibilities of each party, any misunderstanding will affect the systems security and leave the client exposure to vulnerabilities. The SLA specifies thresholds and financial penalties associated with violations of these thresholds. Well-designed SLAs can significantly contribute to avoiding conflict and can facilitate the resolution of an issue before it escalates into a dispute.

Most public cloud infrastructure services are available only through non-negotiable standard contracts which strictly limit the provider's liability. As a result, the remedies offered in case of non-compliance do not match the cost to the customer of the potential service disruptions. Furthermore, most IaaS providers put the burden of SLA violation notification and credit request on their customers.

B. Utility Computing

Utility [9] computing is an important part of cloud computing. in utility computing services and hardware resources are given to users for their requirements. Resources can be hardware, storage device, bandwidth etc.User pay as per their usage. Complexity of cloud computing is one of the hurdles of utility computing. Attacker attack utility computing offenly to use services of utility computing without paying charges.

C. Cloud Software

Cloud software is open source or commercial closed source. In the both the cases vendor does not ensure for vulnerabilities and bugs in available software.

D. Virtual Machine

Basic unit of computing is [4] Virtual machine. There are two basic types of virtual machines: Persistent and Non- Persistent.

- In Persistent machine if the machine is stopped data is backed up on permanent storage device. Machine will be restarted from the state where it is last stopped.
- In Non-Persistent machine if machine is stopped modified data is lost. In this case required data must be moved to some other place before machine is stopped.

Like Physical machines Virtual machines are at risk to hardware failures.

E. Virtual Disk

A virtual disk is a storage device that is located on virtual machine. Virtual disks can handle random data usage. At a time Virtual disks can be installed on one virtual machine. Virtual disk can be installed on multiple machines throughout its life. Virtual disk exists even if its machine is shut down. Virtual disk can also have chances to fail.

F. Geographic Region

In reality Virtual machine actually installed somewhere. The geographic region is the place where the hardware resources and virtual machines actually installed. Geographic region also play an important role in clouds computing. Distance between user and the virtual machine is important in case of emergency like disaster occur in a particular zone. Geographic region size depends upon the size of the cloud. If the cloud is large the region size can be in miles and if the cloud size is small the region size can be in a building or a room.

G. Failure-insulated Zone

Failure-insulated zones are sub-divisions of the geographic regions. Failure insulated zones are divisions in geographic zones. Geographic regions are important in case of large-scale failures. Failure-insulated zones are divisions within a geographic region that are, as much as possible, isolated from expected localized failures such as disk or power supply failure. Similar to geographic regions, exactly how isolated these zones are will vary. A large public cloud may have zones that are placed in rooms separated by firewalls. A smaller private cloud may use zones as simple as two racks that can be in a room.

H. Archival Storage

Archival storage is long term permanent storage. Archival storage allows the storage and retrieval of individual blobs, but does not allow random I/O within the blobs. Archival storage is not mounted to any virtual machine, and can be accessed by multiple virtual machines at the same time. Archival storage exists outside of any specific geographic region. It is considered to be completely durable, but not always available.

IV. SECURITY ISSUES in IaaS

A. Shared resources

Resources are shared in [8] cloud computing environment with clients. Elements such as Hard disk, RAM, CPU cache and other were not typically designed with multitenant privacy requirements of cloud computing in mind. Information can be leaked when data is shared in these resources. As a result, the sharing of these resources may lead to leaked information.

B. Malicious insiders

Insider threats should be taken care in cloud computing. An employee at cloud provider side could directly access customer's data and steal or change it.

C. Denial of Service

Attackers can attack cloud resources by using all resources or by bind most of them to slow down client's computers. If a customer uses all of their cloud resources, they may degrade the service quality of other clients in the same cloud section.

D. Insecure APIs

A set of APIs are provided by cloud providers to access their services. Security issues are coming in APIs .Cloud providers are busy in improving their development. Cloud providers must have to fix security issues in APIs within time.

E. Insecure Data

As software attacks are increased, it is a challenge for cloud providers to keep user data safe and to keep their infrastructure updated. Privacy loss is also an important issue in cloud computing. Most data breach attacks that affected the cloud were directed at the web application itself or took advantage of poorly configured permissions in cloud implementations.

CONCLUSION

In this paper we discuss cloud computing service model Infrasture as Service, Platform as Service and Software as service. Infrasture as service have some basic components as SLA,Virtual Machine, Virtual Disk, Geographical Region, Archival Storage, utility computing, Computer Software. As cloud computing is a growing field it has some security issues. Security issues in Iaas are shared resources, malicious insider, denial of service, insecure data, Insecure API's etc.We discuss security issues in this paper. In the progress of cloud computing on a large scale, the proactive measures must be taken to ensure security

References

[1] Cloud Computing Bible,written byBarrie Sosinsky Published by Wiley Publishing, Inc.10475 Crosspoint BoulevardIndianapolis, IN 46256.

[2] Mell P, Grance T (2011), "The NIST definition of Cloud Computing" NIST, Special Publication 800–145, Gaithersburg, MD.
[3]] Ankush Narkhede(2013), "Cloud Security Issue and Challenges" Network and Complex Systems, ISSN 2224-610X (Paper) ISSN 2225-0603 (Online), Vol.3, No.1, 2013.
[4] https://scn.sap.com/people/eric.farrar/blog/2010/10/01/the-components-of-iaas
[5] T. Garfinkel and M. Rosenblum, "When virtual is harder than real: security challenges in virtual machine based computing environments," Proceedings of the 10th conference on Hot Topics in Operating Systems –Volume 10, 2005.
[6] M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, On Technical Security Issues in Cloud Computing. IEEE, 2009.
[7] Jensen M, Schwenk J, Gruschka N, Iacono LL (2009) on technical Security issues in Cloud Computing. In: IEEE International conference on Cloud Computing (CLOUD'09). 116, 116, pp 109–116.
[8] Keiko Hashizume1, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez(2013), " An analysis of security issues for cloud computing", Journal of Internet Services and applications, Page 4-5.
[9] P. R. Jaiswal1, A. W. Rohankar (2014), "Infrastructure as a Service: Security Issues in Cloud Computing" International Journal of Computer Science and Mobile Computing, Vol.3 Issue.3, March- 2014, pg. 707-711.
[10] Pankaj Arora,Rubal Chaudhary,Satinder Pal Ahuja(2012), " Cloud Computing Security Issues in Infrastructure as a Service "International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 1, January 2012 ISSN: 2277 128X.