Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 5, Issue. 8, August 2016, pg.274 – 281

ANALYSIS OF SECURITY ISSUES IN VIRTUALIZATION CLOUD COMPUTING

Motukuri Prashanthi
Assistant Professor, CSE Dept., CMR Engineering College, Hyderabad

Abstract: Cloud Computing has become a well-known buzzword nowadays due to its ability to reduce cost while increasing scalability, performance and flexibility for various processes. In today's world it is discussed topic, as the complete software industry is entering in the development of cloud services at a faster pace. Cloud computing provides an easy access to high performance computing and storage infrastructure through web services. This paper discusses an overview about the cloud computing, cloud service models, typical cloud architecture with respect to virtualization, Virtualization impact on cloud security and security threats related to virtualization

Introduction: Cloud computing is a model for enabling ubiquitous, appropriate, on-demand network access to share various computing resources such as services, networks, applications, servers, storage etc that provides with minimal effort for the customer. The cloud model is basically composed of five essential characteristics, three service models and four deployment models. The section II defines Essential Characteristics of Cloud Computing, Section III describes Service models of cloud computing, Section IV describes four Deployment models

in cloud, Section V describes introduction to virtualization and section VI describes Why Virtualization, Section VII defines various security Threats and problems in virtualization cloud computing and section VIII defines Conclusion and our future research work.

Essential Characteristics:

On-Demand self service: The end user can easily access various computing capabilities, such as server time and network storage, as needed without service provider in each service.

Broad Network Access: The end user's over the network can access various standard mechanisms through various thin and thick client platforms. (ex: mobiles, laptops, Desktops and workstations)

Resource Pooling: The service provider can provide various services and resources such as storage, processing, memory and network bandwidth using a multi-tenant model.

Rapid Elasticity: Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured Service: Cloud computing provide, control and optimize resource by leveraging a measure at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth and active user accounts). Resources can be monitored, controlled and reported transparency for both the provider and consumer of the utilized service.

Service Model:

Infrastructure as a Service (IaaS): This model allows user to rent processing, storage, networks and other resources. The user can deploy a new user as a guest OS and applications. The user does not manage the complete cloud infrastructure but has the control over OS, storage, deployed applications and various network components. Some providers are Amazon EC2, GoGrid etc.

Platform as a Service (Paas): This model provides the user to deploy user built applications onto the cloud infrastructure that are built using programming languages and software tools supported by the provider. The user does not manage underlying cloud infrastructure. Some providers are Google App Engine, Microsoft Azure etc.

Software as a Service (SaaS): It is browser initiated application software over thousands of cloud customers. In cloud, the customer need not invest in servers or software licensing. Some examples are salesforce, workstreams etc.

Deployment Models:

Private cloud: The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud: The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud: The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud: The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

Virtualization:

Virtualization is the creation of a virtual (rather than actual) version of something, such as an operating system, a storage device, an application, or network resources. From an enterprise perspective, virtualization offers data center consolidation and

Improved IT operational efficiency. Today, enterprises have deployed virtualization technology within data centers in various forms, including OS virtualization (VMware, Xen), storage virtualization (NAS, SAN), database virtualization, and application or software virtualization (Apache Tomcat, JBoss, Oracle App Server, Web Sphere). IaaS providers including Amazon (EC2) and Sun Cloud employ OS virtualization, which enables customers to run instances of various operating system flavors in a public cloud. In addition to OS and storage virtualization, Saas and PaaS service providers are known to have implemented software and database resources. For example, Salesforce.com is known to have virtualized both the software and the database stack

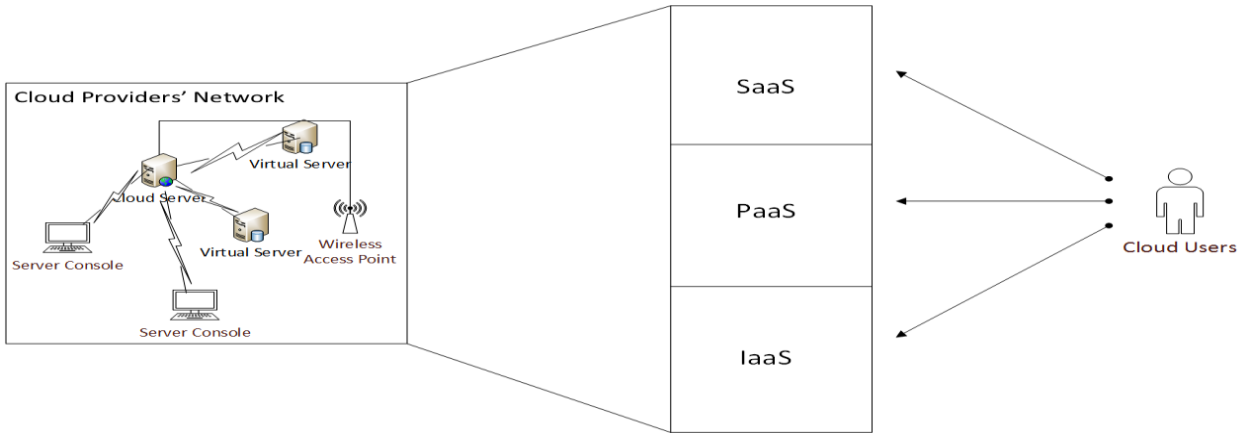


Figure 1: Cloud service Hierarchy

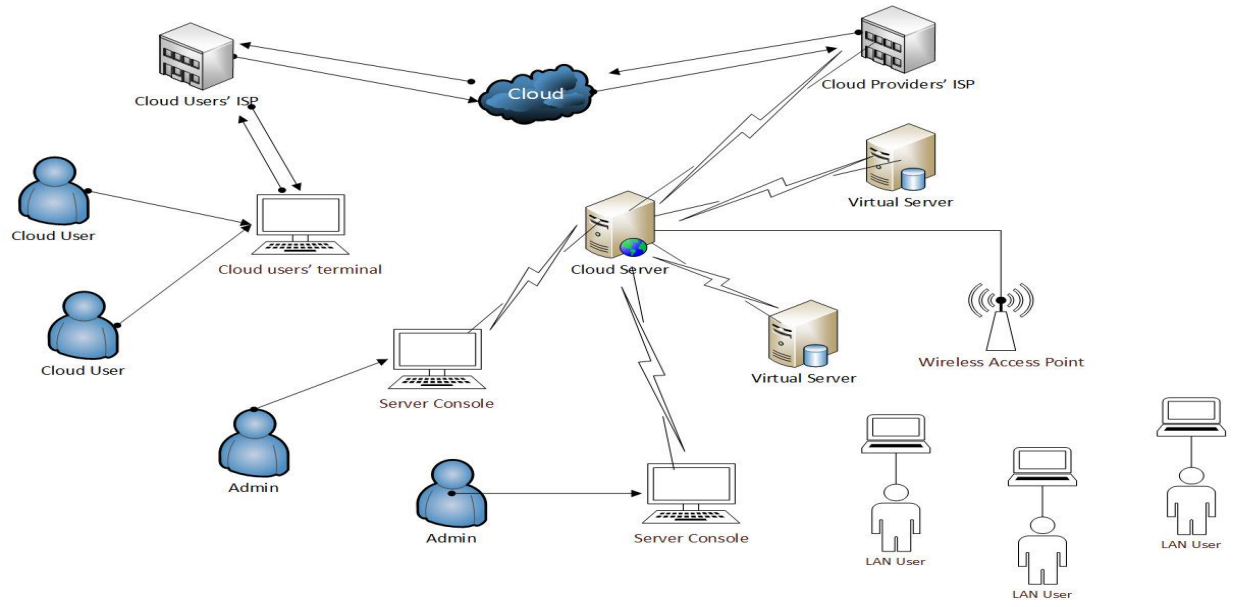


Figure2: A Typical Cloud Architecture

Figure 1 and 2 explains how a cloud uses the concept of virtualization in order to share resources, services and operations among various service providers and users.

Why virtualization:

There are many reasons why we need to virtualize resources. The five most common reasons are:

Sharing: When a resource is too big for a single user, it is best to divide it into multiple virtual pieces, as is the case with today's multi-core processors. Each processor can run multiple virtual machines (VMs), and each machine can be used by a different user. The same applies to high-speed links and large-capacity disks.

Isolation: Multiple users sharing a resource may not trust each other, so it is important to provide isolation among users. Users using one virtual component should not be able to monitor the activities or interfere with the activities of other users. This may apply even if different users belong to the same organization since different departments of the organization (e.g., finance and engineering) may have data that is confidential to the department.

Aggregation: If the resource is too small, it is possible to construct a large virtual Resource that behaves like a large resource. This is the case with storage, where a large number of inexpensive unreliable disks can be used to make up large reliable storage.

Dynamics: Often resource requirements change fast due to user mobility, and a way to reallocate the resource quickly is required. This is easier with virtual resources than with physical resources.

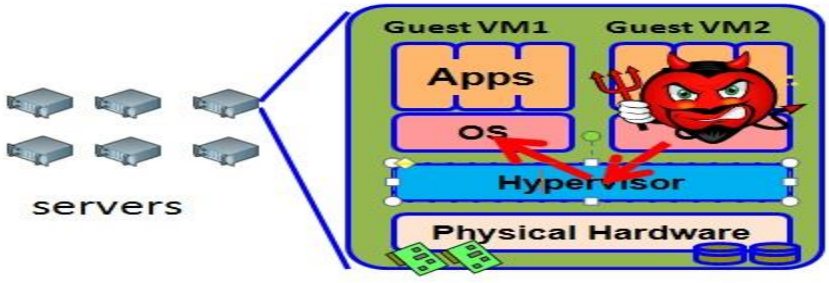
Ease of management: Last but probably the most important reason for virtualization is the ease of management. Virtual devices are easier to manage because they are software-based and expose a uniform interface through standard abstractions.

CSA: Cloud Security Alliance is an organization led by a group of corporate and associations such as Dell, HP, Ebay etc. The CSA defines various features, specifications and well known standards that are related to security framework in cloud. The CSA uses widely adopted frameworks in order to achieve standardization of policies and best practices based on already accepted security principles. CSA usually provides trust in delivery and operations in cloud.

Cloud Computing Security:

By the CSA guidance, ENISA's security assessment and NIST mission to advance the standards and technology. An Emphasis is given to the distinction between services in the form of Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS). In order to concentrate and organize information related to cloud security and for future studies, in this section CSA has identified various problems and they are categorized into seven categories. In this paper we mainly discuss some of the problems caused by virtualization:

1. **Isolation:** First, virtualization provides isolation. Isolation is key for many applications and comes in several flavors.
   a. **Fault Isolation:** If one virtual machine contains a buggy operating system, that OS can start scribbling all over physical memory. These wild rights must be contained within the VM boundaries.
   b. **Performance Isolation**: Ideally VMs performance would be independent of the activity going-on on the hardware. This must be accomplished by smart scheduling and resource allocation policies in the monitor.
   c. **Software Isolation:** Most of the issues with computers today are complex software configurations. DLL hell on PCs, operating system and library versions, viruses, and other security threats. VMs are naturally isolated for each other by running in separate software environments.
2. **Hypervisor Vulnerabilities:** Malicious software can run on the same server:
   - Attack hypervisor
   - Access/Obstruct other VMs



3. **Multi-Tenancy -** Different users within a cloud share the same applications and the physical hardware to run their VMs. This sharing can enable information leakage exploitation and increases the attack surface and the risk of VM-to-VM or VM-to hypervisor compromise.
4. **Workload Complexity -** Server aggregation duplicate the amount of workload and network traffic that runs inside the cloud physical servers, which increase the complexity of managing the cloud workload.
5. **Loss of Control** - users are not aware of the location of their data and services and the cloud providers run VMs they are not aware of their contents.
6. **Network Topology -** The cloud architecture is very dynamic and the existing workload change over time, because of creating and removing VMs. In addition, the mobile nature of the VMs that allows VMs to migrate from one server to another leads to non-predefined network topology.
7. **No Physical Endpoints -** Due to server and network virtualization, the number of physical endpoints (e.g. switches, servers, NICs) is reduced. These physical endpoints are traditionally used in defining, managing and protecting IT assets.
8. **Single Point of Access** - virtualized servers have a limited number of access points (NICs) available to all VMs. This represents a critical security vulnerability where compromising these access points opens the door to compromise the VCI including VMs, hypervisor or the vSwitch.

Conclusion: There are security challenges in the cloud, and a secure cloud is impossible unless the virtual environment is secure. Traditional security solutions do not map well to the virtualized environments, because of the complex and ever-dynamic nature of the cloud computing. New virtualization-aware security solutions should be provided to ensure the preemptive security to the overall system. These security solutions should have the intelligence to be self-defending and have the ability to provide real-time detection and prevention of known and unknown threats. Our research is focusing on developing a new virtualization-aware security solution that can meet our research challenges and have the ability to defend the cloud virtual infrastructure different layers (including VMs, vSwitch and Hypervisor) against zero-day threats.

References

[1] Alexander Lenk, Markus Klems, Jens Nimis, Stefan Tai, and Thomas Sandholm, "What's inside the Cloud? An architectural map of the Cloud landscape," in *Proceedings of the 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing*, 2009, pp. 23-31.

[2] Luis Vaquero, Luis Rodero-Merino, Juan Caceres, et al, "A break in the clouds: towards a cloud definition," *ACM SIGCOMM Computer Communication Review*, vol. 39, pp. 50-55, 2009.

[3] Wesam Dawoud, Ibrahim Takouna and Christoph Meinel, "Infrastructure as a service security: Challenges and solutions," in *2010 The 7th International Conference on Informatics and Systems*, 2010, pp. 1-8.

[4] Kevin Skapinetz, "Virtualization as a Black hat Tool," in *Network Security, Elsevier.*, 2007, pp. 4-7.

[5] W. Dawoud, , Takouna, I., Meinel, C., "Infrastructure as a service security: Challenges and solutions," in *the 7th International Conference on Informatics and Systems*, Cairo, May 2010.

[6] Kai Hwang, Sameer Kulkareni, Yue Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Management," Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, 2009, pp.717-722.

[7] Bernd Grobauer, Tobias Walloschek and Elmar Stöcker, "Understanding Cloud-Computing Vulnerabilities," IEEE Security and Privacy, 10 Jun. 2010. IEEE computer Society Digital Library. IEEE Computer Society, pp.1-8.

[8] Martim Carbone, Diego Zamboni, Wenke Lee, "Taming Virtualization," IEEE Security and Privacy, 2008, vol. 6, pp. 65-67.

