Review on Security Of Cloud Computing

Mohammad Ishfaq Khan1, Sameer Pandey2, C.K.Raina3
Student CSE Department ,AIT Chandigarh,Punjab, India
Under the supervision of C.K.Raina(HOD Cse Department)

ABSTRACT:

With the development of cloud computing data security becomes more and more important in cloud computing.This paper analysis the basic problems of cloud computing data security.

Security is the key for cloud success. Data in the cloud is typically in a shared environment alongside the data from the customers. Encryption is effective but isn't cure all. There are two technologies multi-tenancy,virtualization which provides security about cloud computing. If there is no security with

Virtualization ,then there will also no security issues with cloud computing.

Keyword: Virtualization and Multi-tenancy.

Introduction

Cloud computing presents a new way to supplement the current consumption & delivery model for IT services based on internet.Infrastructure as a services are largely scale on virtualization technology.This techniques provides security and isolation which customers wants multi-tenancy and virtualization

enable on efficient computing model. Multi-tenancy provides isolation environment for each customers & allows multiple tenants to co-exist in same physical machine sharing its resources (CPU, memory,network). Virtualization is the means used to obtain multi-tenancy. Virtualization allows multiple operating systems to run on the same physical device at the same time. This allows several users

to executetheir applications on the same environment but isolated from each other.This paper will summarize in the area of cloud computing security, with a focus on Virtualization Security.

VIRTUALIZATION

Virtualization has been in the IIT world for a long time IBM was the first that indrouced the idea in the early of 1960's with the name 'Time Sharing'. Virtualization of operating system is also known as Server Virtualization.This technology are already established in IT sectors. Server virtulization is defines as a way of making a physical computer function as if it were two or more computers where each non-physical or virtualized.Virtualization technology therefore allows the installation of an operating system on hardware that does not really exist. Virtualization, resources can be divided or shared through multiple environments, where those environments may be aware of not of the others. These environments are known as virtual machines (VMs), and usually host an OS.

There are two virtualization types that concern cloud computing:

□ **Full Virtualization:**

In this type of virtualization, a complete installation of one machine is run on another.

□ **Paravirtualization:**

This type of virtualization allows multiple modified OSs to run on a single hardware device at the same time by more efficiently using system resources.

The main difference between them is that in full virtualization the entire system needs to be emulated (BIOS, drive...); but in paravirtualization, the OSs has been modified to work more efficiently with the hypervisor. The use of paravirtualization reduces flexibility since OSs need to be properly modified to run, which means that probably new OSs will need some time before being available on this type of virtualization. Also, there is an increased security impact since the modified OSs have more control over the underlying hardware which can impact on the other virtualized systems and the host OS.

Virtual Machine

A **virtual machine** (VM) is a virtualized representation of a physical machine operated and maintained by the virtualization software. VM is a self-contained operation environment.This machine separate computer, emulating the processor, memory, network adapter, removable drives and peripheral devices. VMs provide some benefits over physical machines. VMs are usually compromised by a single or group of files that are read and executed by the virtualization platform. This means that they can be easily migrated from one system to another, copied, or backed up.

Virtual Appliances

A virtual appliance (VA) is described as “a pre-packaged software image designed to run inside a virtual machine” Examples of VAs are the virtualized forms of physical network devices such as routers, or switches. Special type of VAs called virtual security appliance (VSA). Examples of VSAs are firewalls, anti-virus, or IDS/IPS.

Virtualization Security-

Virtualization has the revolutionized the data center and is one of the key foundational technologies underlying cloud computing. Many companies deploying virtualization solutions both in their private and public clouds, assuming the risks are similar to deploying physical servers.

However, protecting virtual assests can be more difficult than protecting physicals server; ultimately,**there is no virtualization technology that can equal the protection of physical separation.**

A list of security challenges of virtualization in the Cloud that summarize almost all the problems:

□ **Inter-VM Attacks:** The new communication channel created between VMs cannot be monitored using traditional network security controls.

□ **Instant-on gaps:** Provide up-to-date security to dormant VMs becomes a difficult task. A compromised image of a VM could potentially create a security breach when instanced.

□ **Mixed Trust level VMs:** Several VMs with different security levels could potentially be placed on the same host machine. This is especially concerning when coexisting with unknown tenants.

□ **Resource contention:** Accidental or unauthorized use of shared resources can potentially lead to a denial of service.

□ **Complexity of management:** Management of the VMs becomes harder than before, requiring more complex patching and configuration policies.

□ **Multi-tenancy**: VMs now coexist with other unknown and potentially malicious VMs.

□ **Lack of audit trail:** The process of monitoring and log VMs activities becomes more difficult on virtualization environments.

Several issues arise from virtualization in cloud environments, but this can actually become an advantage for organisations. The absence of a security perimeter and the highly volatile nature of VMs will force organisations to adopt robust security processes which can result in a high-security computing infrastructure according to Reese. This thesis will focus on the threats exposed by a malicious tenant coexisting in the same host system with other tenants in a public IaaS Cloud. More precisely the following threats will be analyzed:

□ Virtual machine to virtual machine attacks (VM-to-VM).

□ Virtual machine to hypervisor attacks (VM-to-Hypervisor).

MULTI-TENANCY

The term “multi-tenancy” refers to a software architecture in which single instance of software runs on a server and serves multiple tenants. A tenant is a group of users who share a common acc ess with a specific privileges to software instance. “Multi-tenancy in cloud service models implies a need for policy-driven enforcement, segmentation, isolation, governance, service levels, and chargeback/billing models for different consumer constituencies”. There are some differences between a SaaS and an IaaS multi-tenant architecture. Depending on the different deployment models, a multi-tenant environment will provide different security concerns. According to IBM, the term multi-tenant means the ability to provide computing services to multiple customers by using a common infrastructure and code base. In a multi-tenant environment, tenants would have a private space and a common space shared amongst all tenants. By sharing resources and creating standard offerings, multi-tenancy reduces costs and improves efficiency of operations. Multi-tenancy makes use of virtualization technologies to increase resource utilization, load balancing, scalability, and reliability; and the use of automation reduces complexity, decrease operation costs, and increase provisioning speed. Multi-tenancy can be applied to different levels. Depending on the level, the multi-tenancy architecture will lead to different concerns. According to IBM these levels can include:

□ **Application level.** Multiple tenants use an application which provides logical separation between users, access controls, and customization.

□ **Middleware level**. Multiple applications use the same middleware which provides logical separation, access controls, and resources.

□ **Operating system** (OS) level. Multiple middleware runs under the same OS which provides access controls, logical separation, and resources to the middleware.

□ **Hardware level.** The hardware provides logical separation, access control and resources to each OS instance. In this level, each OS is considered a tenant.

The most typical components that can be shared across multiple tenants are:

□ Storage.
□ CPU processing.
□ Memory.
□ Network bandwidth
□ Management.
□ Provisioning.
□ Complexity.
□ Power Usage.
□ Billing or chargeback.

Virtualization technologies are the key to solve these problems. Virtualization provides a mean to maximize the efficiency of sharing these resources through several mechanisms.

Multi-tenancy Security

The capability of multi-tenancy to share resources is a key element for cloud computing. Virtualization is the means used to achieve multi-tenant environments, so they share many of security risks. From a high point of view the idea of sharing resources and the coexistence of different tenants that are unknown to each other, enables all the security risks. Virtualization is the means used to achieve multi-tenant environments, so they share many of security risks. From a high point of view the idea of sharing resources and the coexistence of different tenants that are unknown to each other, enables all the security risks.

~Availability:Build resilient architecture,high availability tolerance redundancy.

~Secure Seperation:Enable separation across tenants,and also increase security to access control.

~ServiceAssurance:Deliver consistent SLA across computer network storage.

CONCLUSION

It is clear that although the use of cloud computing has rapidly increased, cloud computing is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. Virtualization is the means used to achieve multi-tenant environments, so they share many of security risks. From a high point of view the idea of sharing resources and the coexistence of different tenants that are unknown to each other, enables all the security risks. Virtualization is the means used to achieve multi-tenant environments, so they share many of security risks. From a high point of view the idea of sharing resources and the coexistence of different tenants that are unknown to each other, enables all the security risks.

FUTURE WORK

For data security and privacy protection issues, the fundamental challenges are separation of sensitive data and access control. Our objective is to design a set of unified identity management and privacy protection frameworks across applications or cloud computing services. As mobility of employees in organizations is relatively large, identity management system should achieve more automatic and fast user account provisioning and de-provisioning in order to ensure no un-authorized access to organizations' cloud resources by some employees who has left the organizations. Authorization and access control mechanisms should achieve a unified, reusable and scalable access control model and meet the need of fine-grained access authorization. Accountability based privacy protection mechanisms will achieve dynamical and real-time inform, authorization and auditing for the data owners when their private data being accessed..

REFRENCES

1-Cloud Security Alliance. Security best practices for cloud computing, 2010b http://www.cloudsecurityalliance.org

[accessed on: 10 April 2010].

2-Cooper R. Verizon Business Data Breach securety blog, 2008 http://securityblog.verizonbusiness.com/2008/06/10/2008-data-breach-investigations-report/S

[accessed on: 11 February 2010].

3-IBM researcher solves longstanding cryptographic challenge. Discovers method to fully process encrypted data without knowing its content; could greatly further data privacy and strengthencloud computing security.

http://www-03.ibm.com/press/us/en/pressrelease/27840.wss

4- National Institute of Standards and Technology, The NIST Definition of Cloud Computing, Information Technology Laboratory, 2009

5- B. Lang, I. Foster, F. Siebenlist, R. Ananthakrishnan, T. Freeman, Attribute based access control for grid computing, 2008.

6- Cloud Identity Summit, Secure the cloud now, Cloud identity summit, Retrieved on 10/11/2010 from: http://www.cloudidentitysummit.com/

7- Randike Gajanayake, Renato Iannella, and Tony Sahama, "Sharing with Care An Information Accountability Perspective," Internet Computing, IEEE, vol. 15, pp. 31-38, July-Aug. 2011.

8- DoD, "National Industrial Security Program Operating Manual", 5220.22-M, February 28, 2006.

9-] Richard Kissel, Matthew Scholl, Steven Skolochenko, Xing Li, "Guidelines for Media Sanitization," NIST Special Publication 800-88, September 2006, http://csrc.nist.gov/publications/nistpubs/800- 88/NISTSP800-88_rev1.pdf.