International Association of Scientific Innovation and Research (IASIR)
(An Association Unifying the Sciences, Engineering, and Applied Research)

ISSN (Print): 2279-0047
ISSN (Online): 2279-0055

International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Analysis of Virtualization: Vulnerabilities and Attacks over the Virtualized Cloud Computing

[1]Kanika, [2]Navjot Sidhu
[1]M. Tech. Research Scholar, [2]Assistant Professor
Centre for Computer Science and Technology
Central University of Punjab
Bathinda, India

Abstract: *Cloud computing is the fastest growing technology in the IT world. The technology offers reduced IT costs and provides on the demand services to the individual users as well as organizations over the internet. The means of cloud computing is obtained by the virtualization of the resources such as hardware, platform, operating system and storages devices. Virtualization permits multiple operating systems to run on the same physical machine. Multiple tenants are unaware of the presence of the other tenant with whom they are sharing the resources. The co-existence of multiple virtual machines can be exploited to gain the access over other tenant's data or attack to deny of services. The significant concern is insuring the security and providing isolation between multiple operating systems. The paper explores various kinds of vulnerabilities and attacks associated with the virtualization.*

Keywords: *Cloud computing, Virtualization, Multi-tenancy, Network-security, Hypervisor.*

I. Introduction

Cloud computing is the Internet-based computing, where sharing of resources, software and platforms are provided to the users on demand an in distributed computing environment. Cloud computing is the growing trend for storing and processing data in a resource sharing environment. To use the full potential of cloud computing, data is transferred, processed, retrieved and stored by external cloud providers. The term cloud in the cloud computing specifies storage space, hardware, networks combination to deliver computing services. Cloud services include delivery of software, platform to develop applications and providing a complete infrastructure over the internet.

Cloud computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud computing creates exciting opportunities like reduced costs and flexibility to the users.

A. Cloud Computing Service Models

Cloud service providers offer services that are separated into three categories as [1], [9]:

1) Software as a Service (SaaS): In the model, softwares are offered as a service on demand to the customers. Multiple tenants are serviced via running single instance of the service. Customers are billed on the basis of usage and there is no need for investment in servers or software licenses. For the providers, the costs are also lowered, as there is need of single application to host and maintain.

2) Platform as a Service (Paas): PaaS provides complete platform required to develop user specific applications and services over the Internet. Platform as a service offers combination of operating system and application servers, such as Linux, Apache, MySql and PHP etc.

3) Infrastructure as a Service (Iaas): IaaS offers complete infrastructure such as servers, basic storage systems, networking equipments. Here multiple tenant shares a virtualized environment. Tenants are coupled with Managed Services for OS and application support.

B. Deployment models in cloud computing

Cloud computing services can be deployed in four different ways depending upon the structure of the organization. The deployment models can be used with any service models (SaaS, PaaS, or IaaS) as [5], [9]:

1) Private cloud: The cloud infrastructure is provisioned to be used by a single organization comprising multiple consumers and managed by an organization or a third party.

2) Community cloud: In community cloud, organizations having similar requirements share a common cloud. The cloud is managed by the organizations in the cloud, a third party.

3) Public cloud: In the public model, services are provided to customers by the cloud service provider over the Internet. The services can be providing storage space or infrastructure over the internet. The services can be free of cost or on the basis of a pay-per-use. Gmail, skydrives are the common public clouds.

4) Hybrid cloud: A hybrid cloud service is implemented by combining the services of different cloud computing systems say combining private, public cloud. A hybrid cloud is created to fulfil the specific demands of the organisations.

C. Essential Characteristics

Cloud computing provides services to the customers over the internet with reduced cost and reliability. Here are the five characteristics of the cloud which represents its services [9], [18]:

1) On-demand self-service: A consumer can automatic provision computing resources, as they needed without requiring interaction with cloud service provider.

2) Broad network access: Cloud services are provisioned over the network and can be accessed via multiple devices such as mobile phones, laptops, PDA, etc.

3) Resource pooling: The cloud service provider's resources are pooled in a multi tenant environment; resources are dynamically allocated to the tenants according to their demand. The tenant don't know the exact location of the resources. The shared resources include storage, processing, memory, etc.

4) Rapid elasticity: Cloud services can be automatically scaled at any time and at any quantity depending upon the customer's demand.

5) Measured service: Customer usage of the provider's services is automatically monitored and reported providing transparency for both the customer and provider.

II. Multi-Tenancy

In a multi-tenant environment, tenants have their own private space to save private data as well as global space shared among all tenants. By sharing resources and creating standard offerings, multi-tenancy offers reduced cost and optimum use of resources in a shared environment.

The idea of sharing resources between multiple tenants is fundamental to cloud computing. With SaaS, data of multiple tenants is stored on the same database and may share the some tables. In IaaS, multiple tenants share infrastructure resources such as hardware, servers and storage devices.

Resources shared among multiple –tenants can be:

- Basic storage space.
- CPU processing.
- Memory.
- Network bandwidth.

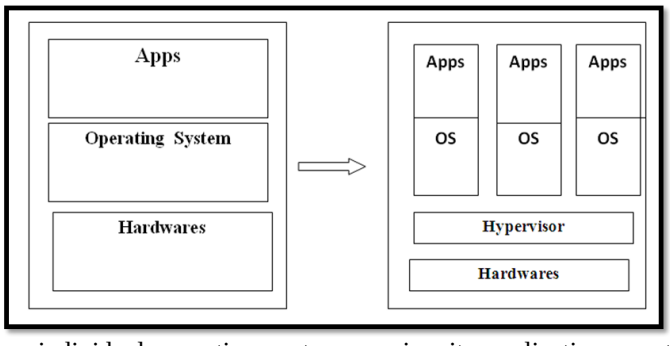
III. Virtualization

Multi-tenancy is obtained by the use of virtualization. It allows multiple operating systems to run on a single machine simultaneously. In cloud computing virtualization used to serve several end users by creating virtual version of storage space, operating system, hardware platform [1].

Virtualization divides a physical computer to several virtual machines known as guest machines. Multiple virtual machines run on a host computer, each having its own OS and applications [4].

Virtualization gives an illusion to the users that they are running their processes on a physical computer independently, but in reality they are sharing the resources of a single host machine. The software which permits multiple operating systems to use the resources a physical machine is called a hypervisor. The hypervisors resides between the operating system of the host machine and the virtual environment.

Fig 1. Physical Machine to Virtualuzed Machine



The figure shows how an individual operating system running its applications on the independent physical hardware can be placed in a virtual machine.

All the OS shares the same physical system with other virtual machines.
As the tenant sharing the same physical host with unknowns, there are various kinds of risks associated with the multi-tenancy environment in the cloud computing. So it is important aspect to isolate the multiple users on same physical. The system can be virtualized in tow different ways as [13] [14]:

A. Para Virtualization

Para- is an English affix of Greek origin that means "beside" or "alongside". Para virtualization is a server virtualization technique in which the guest operating systems are aware of being executed in a virtual environment. Hypervisor runs just above the physical hardware (Ring 0) so that guest OSs run in higher levels. It involves the modification of the operating system Kernel to replace non virtualizable instructions with "hypercalls" that communicates directly with the hypervisor. The advantage is that it has low virtualization overhead. Xen , and Hyper-V support para virtualization.

B. Full Virtualization

Full Virtualization is used to abstract the physical hardware resources to make a complete virtual system where the Guest OS could be executed. Here guest operating systems are not aware of being executed in the virtualized environment. With the ease of virtualization, the applications and software could be easily streamlined between different virtual machines. VMware's virtualization products and Microsoft Virtual Server are examples of full virtualization.

IV. Hypervisor

The hypervisor, a software layer which manages the virtualization, allows virtual machines to execute simultaneously on a single machine. This provides hardware abstraction to the running Guest OSs and efficiently manages underlying hardware resources. There are numerous hypervisors ranging from open-source such as KVM, Xen and virtual box, to commercial hypervisors such as VMware vSphere and Microsoft Hyper-V etc. [10].

A. Type 1 Hypervisor

The hypervisor also known as "Bare metal" is a piece of software that runs directly on the hardware and responsible for coordinating access to resources as well as hosting and managing VMs. Type 1 hypervisor's are completely independent from the OS. VMWare ESXi, xen are Type 1 hypervisors [17].

B. Type 2 Hypervisor

The hypervisor also known as "hosted" runs as an application on an existing operating system. Type-2 hypervisor sits on top of an operating system. The hypervisor emulates the resources required by each guest machine. Type-2 hypervisor are dependent on the operating system. It cannot boot until the operating system is booted. VMware Workstation, VirtualBox, KVM are examples of Type 2 hypervisors [10], [17].

V. Security in Multi-Tenant Environment

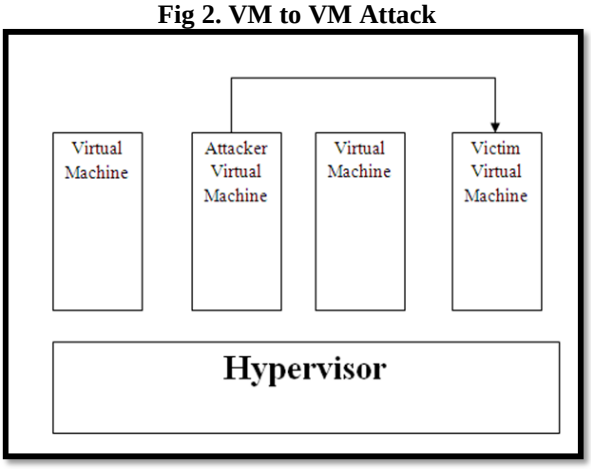
As the tenant sharing the same physical host with unknowns, there are various kinds of risks associated with the multi-tenancy environment in the cloud computing. So it is important aspect to isolate the multiple users on same physical.
It is very difficult to secure the VMs because of the upcoming techniques on how-to-attack a VM or gain control over the Hypervisor. VMs are mobile so they could be easily located on different hypervisors as per the availability of the resources. The most risk of being attacked is while are the VMs are moved. So the question here which arises is should the VMs status be off or suspended while moving. The security policies for such mobile VMs should be very secure which needs to be assured with the other hypervisor's security policy. If the security policy doesn't accompany then the VM becomes vulnerable. Current security measures don't provide complete security as the measures have become very basic [18], [22].
So there is need to think above the cloud to provide security and ensure the cloud is secure and safe. The cloud service provider organizations which provide services must educate the people, network and server administrators regarding the security threats and the preventive measures that can be taken.
The VM threats, attacks or vulnerabilities can pose a great impact on the OS. An attacker if able to gain access over the Hypervisor, then the whole Server could be at risk. All the VMs running over the hypervisor would be compromised. Following are the possible attacks that could compromise the other VM or the hypervisor itself [5], [10].

VI. VM to VM attacks

The co-existence of multiple VMs on a single piece of hardware presents malicious VM owners to glean potentially sensitive information from victim VMs sharing the same hardware resources. An attacker may use guest OS (Virtual Machine) try to communicate and compromise other Virtual Machines on the same physical host, therefore breaking the isolation characteristic of VMs [12].

The attacker VM tries to attack over other VM exiting in the virtualized environment as the vulnerabilities in the LAN.

Fig 2. VM to VM Attack



A. Sniffing Attack:

All the Virtual machines share a common network on a host machine. There is a possibility of traffic sniffing when the VMs communicate with each other. The hypervisors offer virtual network to link VMs using virtual bridge and route.

In virtualized environments, virtual Hubs are created to share the same network in the bride mode. If these hubs are not properly configured, malicious attacker can try to sniff traffic to its own VM that is directed to other VM on the network. The malicious VM can use sniffing tools like "wireshark" to sniff the virtual network traffic. By using these tools attacker can sniff IP address of the other VM that is available neighbor to it. The attacker can perform packet sniffing attack over the victim. As a result, isolation is easy to be broken [20].

B. Spoofing Attack

In the route mode, virtual switches are used to connect the virtual machines to the host machine. The virtual switches need a dedicated interface to connect each VM. Media access control (MAC) address is assigned to each virtual machine. As address resolution protocol (ARP) is necessary to implement to redirect VMs' traffic over the network. The routing table is maintained by sending an ARP command to each VM in boot time. A common vulnerability of ARP is ARP spoofing attack because ARP does not require proof-of origin. It is possible for the attacker to claim any MAC address by issuing ARP reply message with his IP. Hence the attacker can use ARP spoofing attack to redirect all the traffic of a victim VM to his VM [18], [20].

C. Denial of Service (DoS)

In the virtualized environment all the virtual machines are sharing common resources such as storage space, network bandwidth, CPU usage. The denial of service attack is aimed to exhaust the common resources in order deny the services over the other guest virtual machines [3].

In Denial of service attack one victim virtual machine receives more request than its capacity and other end users requests cannot be served. In the cloud environment, DoS attack is more dangerous than unclouded environment because of VMs are sharing their resources with other virtual machines over the same physical machine. One virtual machine can perform denial of service attack to another virtual machine in the virtualized environment.

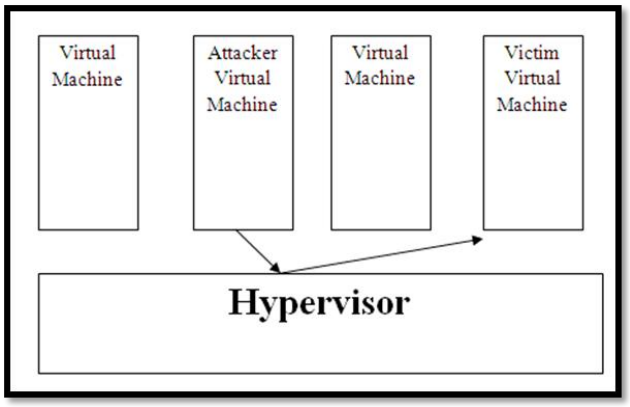
The Transmission Control Protocol (TCP) provides reliable delivery of data over the internet. TCP can be exploited to perform denial of service attack known as TCP SYN flood attack. As a TCP connection is established a by 3-way handshake and the attacker takes advantage of this. An attacker overloads the victim with so many TCP connection requests that it will not be able to respond the legitimate requests. This is done through sending too many TCP SYN packets to the victim virtual machine. The victim allocates buffers for each new TCP connection and transmits a SYN-ACK in response to the connection request. The attacker does not reply to the SYN-ACK packets. Flooding based attacks can also exhaust other resources of the system [19].

An attacker tries to identify the vulnerabilities in the hypervisor so that he can potentially access to the host OS and shared hardwares [14], [16].

VII. Vm To Hypervisor Attacks

As the hypervisor is responsible for managing a virtualized cloud, the attackers target it to access the Guest VMs and the physical hardwares that are shared among virtual machines. As the hypervisor resides between VMs and hardware, so the attack on the hypervisor can damage the VMs and hardwares. It is identified that security of VMs is compromised.

Fig 3. VM to Hypervisor Attack



A. VM Hopping

VM hopping is the process of hopping from one VM to another VM. An attacker being on one VM can gain access over the other VM. This can be achieved if both the VMs are running on the same host. An attacker on VM can gain access over the other VM2 on the same host by just knowing the IP address of the other VM or gaining access over the host itself. Once a VM is attacked, the attacker can monitor the traffic going over the VM and change the flow of traffic or manipulate it. This attack can create issue of Denial of Service (DOS) which is actually an attempt to make a computer resource unavailable to its intended users; Also the attacker can change the files of the VM by changing the configuration file. If VM is running since a long time, an attacker can modify the configuration file such that the VM2 goes to off state. Therefore the ongoing communication could be stopped. Also it can abruptly stop, so the communication is incomplete. When the connection is resumed, the VM needs to restart the entire communication [4], [16].

B. VM Escape:

VM escape is a vulnerability in the virtualization that enables a guest-level VM to attack on its host OS. An attacker runs a code on a VM that allows break out of the virtual machine and interact directly with the hypervisor.VM Escape means gaining access over the Hypervisor layer and attacking rest of the other VMs. If an attacker able to gain access to the host running multiple VMs, the attacker can access the resources which are shared by the other VMs. The host OS monitors the memory being allocated and the CPU utilization. An attacker can bring down these resources and turn off the hypervisor. If the hypervisor fails, all the other VMs turn off eventually [4], [18].

C. Mobility:

VMs are portable; they can be moved from one host to the other. Since VMs are not inherently present on the physical machine, the threat for an attack increases. The contents of the VM are stored in a file on the hypervisor. If the VM is moved to another machine, then the virtual disk is also recreated and hence an attacker can then modify the source configuration file and alter the VMs activities. The VM could be compromised if the VM is offline. An attacker can modify the configuration file off the VM. Gaining access to the virtual disk, attacker has sufficient time to break in all the security measure such as important credentials, passwords etc. Since this VM is a copy of the actual VM, it is difficult to trace the attacker with this threat [17].

VIII. Conclusion

Security of the virtual network is the most significant concern in the cloud platform. The use of the virtualization is to isolate all the co-resident VMs under the hypervisor. But there are various kinds of security breaches in the virtualization which violates the isolation between various VMs.

This research paper focused on the various kinds of attacks and vulnerabilities associated with virtualization in the cloud computing. The paper demonstrates the possible ways how a malicious VM can impact over other VM's data. There is a need to develop and design powerful security techniques to reduce the effect of attacks that can be caused due to process virtualization. However, the work related to some of these threats is in progress but do not insure complete isolation. Future research will aim to understand the sensitivity of virtualization in the cloud and measures to secure it from attacks. This research may help to strengthen virtualization and reduce the risks of cloud computing.

IX. Acknowledgment

I would like to thank my supervisor for his most support and encouragement. I also want to thank my parents and friends, for all their support.

X. References

[1] Awoud D. et al., "Inrrastructure as a service security: Challenges and solutions," *in 7th International Conference on Informatics and Systems (lNFOS)*, pp. 1-8, 2010.

[2] Brohi Sarfraz Nawaz et al., "Identifying and Analyzing Security Threats to Virtualized Cloud Computing Infrastructures," *in International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM)*, pp. 151-155, 2012.

[3] Choi, Y.S. et al., "Integrated DDoS attack defense infrastructure for effective attack," in 2nd International Conference on Information Technology Convergence and Services (ITCS), pp. 1-6, 2010.

[4] Jasti Amarnath et al., "Security in Multi-Tenancy Cloud," *IEEE communication magazine*, 2010.

[5] Jansen W., G rance, I., "Guidelines on Security and Privacy in Public Cloud Computing," National Institute of Standards and Technology Special Publication 800-144, 2011.

[6] Kalagiakos Panagiotis, Bora Margarita, "Cloud Security Tactics: Virtualization and the VMM," *IEEE communication magazine*, 2012.

[7] K. K. Fletcher, "Cloud Security requirements analysis and security policy development using a high-order object-oriented modeling," M.S. thesis, Dept. Computer Science, Missouri Univ. of Science and Technology, Rolla, MS, 2010.

[8] Mervat Adib Bamiahet al., "Seven Deadly Threats and Vulnerabilities in Cloud Computing," *in International Journal of Advanced Engineering Sciences And Technologies*, Vol No. 9, Issue No. 1, pp. 87 – 90, 2011.

[9] Mell Peter, Grance Timothy, "The NIST Definition of Cloud Computing," NIST Special publication, September 2011.

[10] Reuben Jenni Susan, "A Survey on Virtual Machine Security," *Seminar on Network Security*, 2007.

[11] Ros, Jacobo, "Security in the Cloud: The threat of coexist with an unknown tenant on a public environment," MSc.Thesis, Royal Holloway University of London, 2011.

[12] S., Brohi, M., Bamiah, "Challenges and Benefits for Adopting the Paradigm of Cloud Computing," in *International Journal of Advanced Engineering Sciences and Technologies* (IJAEST), vol. 8, pp. 286 - 290, 2011.

[13] Sabahi F., "Security of Virtualization Level in Cloud Computing," *in Proc. 4th Intl. Conf. on Computer Science and Information Technology, Chengdu*, pp. 197-201, 2011.

[14] Sabahi Farzad, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology," *in International Journal of Machine Learning and Computing, Vol. 2, No. 1*, 2012.

[15] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, *Cloud Security Alliance*, 2009.

[16] "Securing Multi-Tenancy and Cloud Computing," Juniper Networks, White Paper,2012.

[17] Szefe Jakub, Lee Ruby B., "A Case for Hardware Protection of Guest VMs from Compromised Hypervisors in Cloud Computing", *in Proceedings of the Second International Workshop on Security and Privacy in Cloud Computing (SPCC 2011)*, 2011.

[18] Velte A. T. et al., "Cloud Computing: A Practical Approach," McGraw-Hill, pp 210-440, 2010.

[19] Zhuang Wei et al. , "TCP DDOS Attack Detection on the Host in the KVM Virtual Machine Environment," *in 11th International Conference on Computer and Information Science*, 2012.

[20] Hanqian Wu et al. "Network Security for Virtual Machine in Cloud Computing," *in International Conference on Computer Sciences and Convergence Information Technology*, pp. 18 – 21,2010.