A Survey on Virtualization and Attacks on Virtual Machine Monitor (VMM)

Kolla Ranga Dinakar[1]

[1]*GMR Institute of Technology, Andhra pradesh, India*

Abstract:- *Cloud computing is a technology which increases the potential of the application in terms of working, elastic resource management and collaborative execution approach. Virtualization is the central part of the cloud computing which allows the dynamic allocation of resources to an industry or to an IT infrastructure. The virtualized system included a software ie, (VMM). Virtual Machine Monitor job is to access the underlying physical host platforms resources. Virtualization or any other technologies have some threats and attacks. This paper surveys types of virtualization, attacks on a hypervisor and some threats.*

Key Words: **Cloud computing, Virtualization, Virtual machine monitor(VMM), Attacks on the cloud, Attacks on virtualization**

1. INTRODUCTION:

Cloud computing is a technology that offers online services to the consumer on demand that reduces various software program and hardware maintenances for person level. Virtualization allows a couple of instances of an operating to run concurrently on a single computer. It is an abstraction over physical resources to make them shareable among a couple of physical users. For sources to be shareable by means of a range of physical user it allocates a logical name to a bodily aid and enables a pointer to that physical resource on demand.

2. VIRTUALIZATION:

Virtualization is a method of how to separate a carrier from the underlying physical shipping of that service. It is the technique of growing a digital model of something like pc hardware. It was once, in the beginning, developed all through the mainframe era. It includes using specialized software to create a virtual or software-created version of a computing resource as a substitute than the genuine version of the equal resource. With the assist of Virtualization, multiple working structures and purposes can run on equal Machine and its identical hardware at the equal time increasing the utilization of hardware.

In other words, one of the most important fee effective, hardware reducing, energy saving techniques used by means of cloud vendors is virtualization. Virtualization is a technique, which permits to share a single bodily instance of a resource or a software amongst more than one clients and businesses at one time. It does via assigning a logical identity to bodily storage and imparting a pointer to that physical useful resource on demand. The term virtualization is often synonymous with hardware virtualization, which performs a critical position incorrectly delivering Infrastructure-as-a-Service (IaaS) solutions for cloud computing. Moreover, virtualization applied sciences provide a digital environment for not only executing purposes but also for storage, memory, and networking.

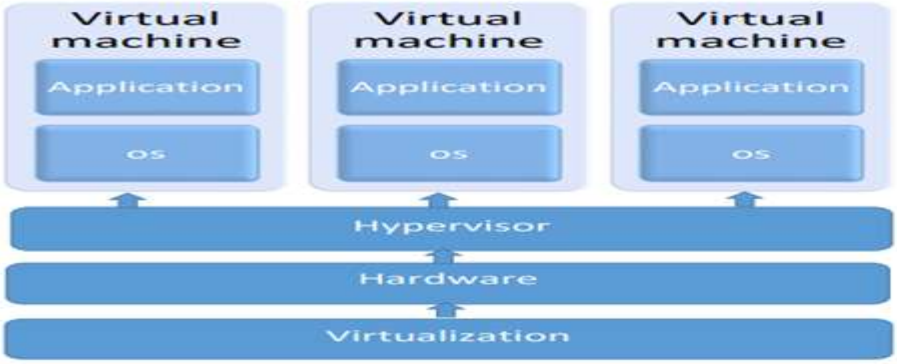

Figure 1: Architecture of Virtualization

2.1 Types of Virtualization:

Application virtualization: This is a manner where functions are virtualized and delivered from a server to the give up user's device, such as laptops, smartphones, and tablets. So as a substitute of logging into their computers at work, users will be capable to gain get admission to the software right from their device, supplied an Internet connection is available. This is mainly famous for agencies that require the use of their purposes on the go.

Desktop virtualization: Desktop virtualization is the notion of keeping apart a logical operating system (OS) instance from the patron that is used to get admission to it. Computing device virtualization separates the computing device surroundings from the bodily system and configured as a "virtual laptop infrastructure" (VDI). One of the biggest benefits of laptop virtualization is that users are able to access all their private documents and functions on any PC, meaning they can work from anywhere without the want to deliver their work computer. It also lowers the fee of software licensing and updates. Maintenance and patch administration is simple, seeing that all of the digital pcs are hosted at an identical location.

Hardware virtualization: Hardware virtualization, which is also acknowledged as server virtualization or virtually virtualization, is the abstraction of computing assets from the software program that uses these resources. In a usual physical computing environment, a software program such as an operating system (OS) or business enterprise software has direct get admission to the underlying pc hardware and components, such as the processor, memory, storage, certain chipsets, and OS driver versions. This posed foremost headaches for software program configuration and made it difficult to move or reinstall software on unique hardware, such as restoring backups after a fault or disaster.

Network virtualization: Network virtualization gathers all physical networking equipment into a single, software-based resource. It also divides available bandwidth into multiple, unbiased channels, every of which can be assigned to servers and systems in real time. Businesses that would gain from community virtualization are ones that have a massive number of customers and need to keep their structures up and running at all times. With the disbursed channels, your network pace will expand dramatically, allowing you to supply services and applications quicker than ever before.

Storage virtualization: This kind of virtualization is very convenient and inexpensive to implement because it includes compiling your bodily hard drives into a single cluster. Storage virtualization is available when it comes to planning for disaster recovery, due to the fact that the statistics saved on your virtual storage can be replicated and transferred to every other location. By consolidating your storage into a centralized system, you can cast off the hassles and costs of handling multiple storage devices.

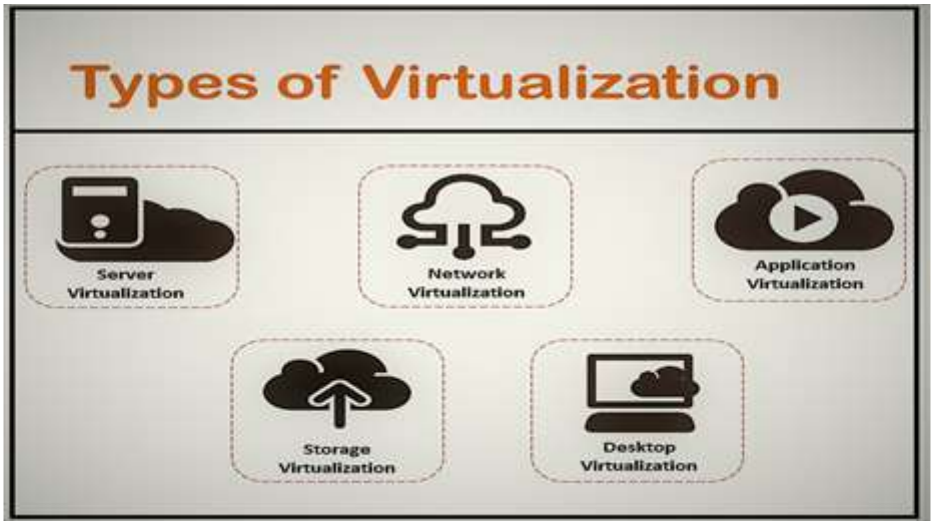

Figure 2: Types of virtualization

3. HYPERVISOR:

A Hypervisor is also known as a virtual machine monitor(VMM). It is a piece of code which runs several virtual machines(VMs). A system on which a hypervisor runs one or more virtual machines is known as a host machine, and each virtual machine is known as a visitor machine or guest machine. A system supports several guest virtual machines for sharing of resources like storage, processing. In well-known hypervisors are without delay accountable for web hosting and managing virtual machines on the host or server. The host is another identity for the physical server and hypervisor. The virtual machines that run on the host are called visitor VM or visitor working system. Furthermore, a hypervisor affords a uniform view of the underlying hardware, which capability that it can operate on the hardware of exclusive vendors. Hence, virtual machines can run on any available and supported computers, for the reason that the hypervisor isolates software from hardware. System administrators, who maintain and operate a computer machine and network, are also in a position to view their hardware as a pool of resources, which approves new functionalities that are described in the parent. It shows a number of visitor working system (window, Linux and Mac) are installed on the hypervisor.

3.1Types of Hypervisors:

Type 1: (bare metal hypervisor) Type 1 is a hypervisor that is installed at once on the hardware and is also referred to as a "bare-metal" hypervisor. Type 1 hypervisors are basically used on the server market. It is a device that installs without delay on the server hardware layer. These structures are alleviated so as to "focus" on the administration of visitor working structures is to say, those used by using the virtual machines they contain. This releases the best feasible sources for digital machines. However, it is viable to execute only one hypervisor on both the servers.

Among type 1 hypervisors there are hypervisors like Xen, VMware ESX and Proxmox.

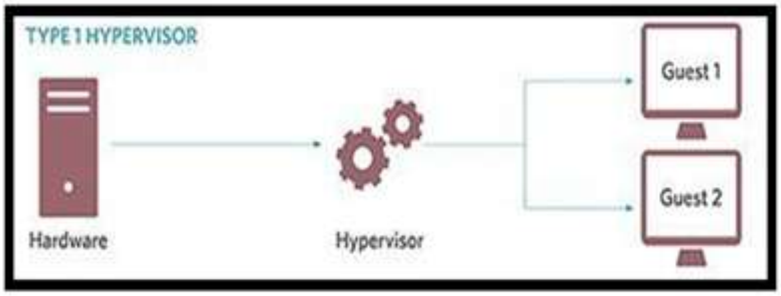

Figure 3: Type 1 Hypervisor

Advantages of Type 1 hypervisor:

- Enhance safety
- Allows greater density hardware two
- The hypervisor has direct get admission to the HW

Disadvantage of Type 1 hypervisor:

- Need precise HW
- aspect Strict HW
- requirement two More high priced

Type 2: (Hosted hypervisor) A hypervisor, which runs on a host working gadget that gives virtualization services such as I/O and reminiscence management. This is also recognized as a hosted method Hypervisor. In other phrases, Type 2 hypervisors are positioned between the hardware and virtual machines that are installed on the pinnacle of a running system. In contrast to kind 1, the hypervisor is placed above the running system and not under the operating gadget or digital machines. This allows for an extra running system to be run in virtual surroundings on the pinnacle of an existing operating system.

Among the type 2 hypervisor, we locate VMware Player, VMware Workstation and VirtualBox Virtual PC.

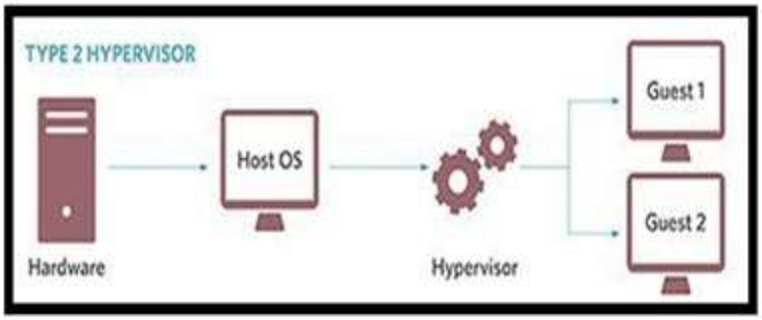

Figure 4:Type 2 Hypervisor

Advantages of Type 2 hypervisor:

- Host OS Controls HW access
- Ease of access
- Allows for more than one running systems

Disadvantages of Type 2 hypervisor:

- Decreased security
- Lower VM density
- Needs a host OS first

4. ATTACKS ON CLOUD INFRASTRUCTURE:

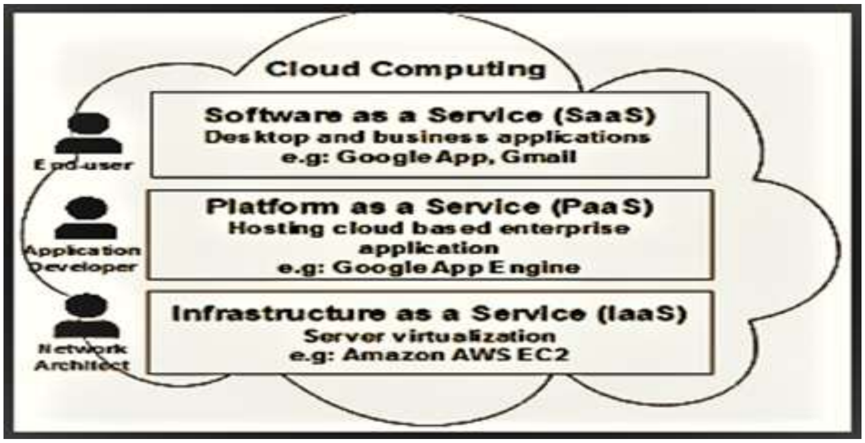
Cloud Computing
Software as a Service (SaaS)
Desktop and business applications
e.g: Google App, Gmail
End-user
Platform as a Service (PaaS)
Hosting cloud based enterprise application
e.g: Google App Engine
Application Developer
Infrastructure as a Service (IaaS)
Server virtualization
e.g: Amazon AWS EC2
Network Architect

Figure5: Cloud Infrastructure

Attacks in the IaaS layer: Infrastructure as a Service is the additional layer between hardware and Operating System in cloud computing. It is built to support and beef up the virtualization technology which will be used by means of the hypervisor. Moreover, virtualization science lets in the administrative operations by means of allowing the introduction of Application Programming Interface (API). The hypervisor attacks are accelerated with the growth of the number of hypervisors. This is because the exploitation of the channels and APIs to the cybercriminals additionally accelerated The VMEscape also can also affect the IaaS layer

Attacks in the PaaS layer: Platform as a Service layer is a platform and obligates to guard both the programming framework and runtime engines from the cybercriminals. Hence, the encryption method is adopted in the PaaS layer to secure the customers from any interference from the cybercriminals. Nevertheless, the multitendency assist has led to vulnerability. This is due to the truth that multi-tenancy enables numerous customers from one of a kind structures to use cloud computing at the same time. Therefore, the cybercriminals can also disrupt the execution of the PaaS.

Attacks in the SaaS layer: The SaaS layer affords offerings that extract data from more than one sources in cloud computing. The instance of the software is a web application. This has given the opportunity for the cybercriminals to create abnormal conduct of cloud computing by inserting malicious script into the webpage. One of the outstanding attacks in the SaaS layer is SQL injection. In the yr of 2012, LinkedIn was being attacked through the hacker through the SQL injection attack. The facts such as passwords had been possessed by means of the hacker and then published it into the password cracking forum. The victims have been multiplied up to 6.5 million. Therefore, LinkedIn has confronted a million lawsuit due to this problem.

5. ATTACKS ON VIRTUAL MACHINE MONITOR(VMM):

Virtualization Attacks One of the top cloud computing threats involves one of its core enabling technologies: virtualization. In virtual environments, the attacker can take control of virtual machines installed by compromising the lower layer hypervisor. It is noticeable that the Cloud Service Provider (CSP) is easily obtainable and this has benefits for both cybercriminals and malevolent users. Hence, the presence of vulnerabilities in the CSP has leveraged the malevolent attacks. Without virtualization, the multiple users to communicate and share similar physical resources are merely impossible. Through the virtualization, the cloud users able to use various applications freely by conducting several useful functions such as migrate, roll back and more in the VMs. In general, the virtualization attacks can be categorized in conventional/traditional attacks and virtualization precise attacks.

Insider Virtualization Specific Attacks: Subsequently, the virtualization of particular assaults can further be divided into insider attacks and exterior attacks. The insider assault is described as the malevolent users that equipped and misused their knowledge about the cloud device. This has circuitously influenced the confidentiality, integrity, and availability of the CSP. Moreover, the malevolent customers have triggered the severe danger to the CSP. As the malevolent customers most probable flip into cybercriminals as time passed. The overview of the insider virtualization precise attack is illustrated in the parent Besides the three wonderful insider attacks displayed in the there are other insider attacks, namely the Communication between Virtual Machines and VM Escape.

External Virtualization Specific Attacks: The external virtualization particular attacks are defined as any assaults launched by way of both malicious cloud computing users and other external users who have possessed the unauthorized accessibility from the CSP. It is observable that the strategies of three notable exterior assaults such as Breakout attack, External Modification of Virtual Machines and Hypervisor attack.

Co-Residential Attacks: Co-Residential Attacks are frequently used in Virtual Machine Allocation Policies in Cloud Computing. The co-residential attack, where malicious users construct side channels and extract the data from virtual machines co-located on the identical server. The intruder is capable to extricate any personal statistics or statistics from the victim, need to co-locate the VMs with the target VMs. A virtual cloud aid allocation model is proposed. In this, the trouble of virtual cloud sources allocation is abstracted as a utility-maximization problem, making trade-offs between the utility of the data middle and the performance of the purposes into account, and maximizing the utility on the premise of meeting user's performance.

Cache-Based Side-Channel Attacks: Resource sharing in cloud computing raises a problem of Cache-Based Side Channel Attack (CSCA). It is proposed to observe and forestall visitor virtual machines from CSCA. Cache omit patterns had been analyzed in this answer to realize aspect channel attack. CSCA is divided into two types and those are time pushed cache attacks and hint driven cache attacks. It is primarily based on a cloud setting with two VMs installed on an equal physical machine using bare-metal hypervisor sharing best possible level cache.

6. Conclusion:

In conclusion, virtualization is a key enabling technology of the cloud, permitting many guest machines to share the same physical hardware. The hypervisor is supposed to be secure from assaults and efficiently isolate the VMs, yet potential security flaws are evident. VM break out is the most serious of all the assaults mentioned due to the fact the escaped VM would be free to compromise all the other co-resident VMs. Solving the VM escape problem ought to probably require a paradigm shift in the structure and sketch of hypervisors. Other assaults that focus on stealing facts via side-channels can be mitigated by adding noise to the side-channel. Solving the problem of hypervisor security is an vital step in imparting a secure cloud surroundings for agencies and buyers to utilize.

REFERENCES:

[1]M. Watson, N. Shirazi, A. Marnerides, A. Mauthe, and D. Hutchison, “Malware Detection In Cloud Computing Infrastructures”, IEEE Transactions on Dependable and Secure Computing, vol13, no. 2, pp. 192-205, 2016.

[2] S. Jin, J. Ahn, J.Seol, S. Cha, J. Huh and S. Maeng, “ H-SVM: Hardware-Assisted Secure Virtual Machines Under A Vulnerable Hypervisor”, IEEE Transactions on Computers, vol64, no. 10, pp. 2833-2846, 2015.

[3] A. Riddle, and S. Chung, “A Survey on the Security of Hypervisors in Cloud Computing”, 2015 IEEE 35th International Conference on Distributed Computing Systems Workshops, 2015.

[4] Ajay Kumara M. A and Jaidhar C. D, “Hypervisor and Virtual Machine Dependent Intrusion Detection and Prevention System for Virtualized Cloud Environment”, 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), 2015

[5] O. Agesen, A. Garthwaite, J. Sheldon, and P. Subrahmanyam. The evolution of an x86 virtual machine monitor. ACM SIGOPS Operating Systems Review, 44(4):3–18, 2010. .

[6] Secure virtualization for cloud computing".Flavio Lombardi, Roberto Di Pietro, June 2010.

[7] Shyam Patidar; Dheeraj Rane; Pritesh Jain “A Survey Paper on Cloud Computing” in a proceeding of Second International Conference on Advanced Computing & Communication Technologies, 2012

[8] T. Dillon, C. Wu, and E. Chang, “Cloud Computing: Issues and Challenges,” 2010 24th IEEE International Conference on Advanced Information Networking and Applications(AINA), pp. 27-33, DOI= 20-23 April 2010

[9] VMware (2009).History of virtualization. DOI= http:// www. Vmware.com /virtualization/ history. html.

[10] Mell, P., Grance, T., & Grance, T. (n.d.). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.

[11] Tan, S. (2010). Forecast: Understanding the Opportunities in Virtualization Consulting and Implementation Services. Gartner. Publication Date: 11 March 2010, ID Number: G00174840

[12] Ramos,S.J.C.C. 2009).Security Challenges with Virtualization. Thesis, December 2009, DOI = http: // docs. di .fc.ul. pt/jspui/bitstream / 10455/3282/1/Thesis – Jramos FCUL.pdf

[13] Chowdhury, M. K.; Boutaba, R. (2009). A survey of network virtualization. Elsevier. Computer Network 54(2010) 862-876

[14] Goldberg, R.P. (1974). Survey of virtual machine research. Computer, pages 34–45, 1974