A Study on hypervisor virtualization in cloud computing

Ramakrishna Subbareddy*, Dr. B. Firdaus Begam

Abstract— Virtualization is the key factor in todays' world of cloud computer technology. Virtualization is used to create abundant ardent resources from a single physical server/entity. Hypervisor is a software tool that isolates the physical infrastructure to create and sperate the resources to work in a cloud environment. Different types of operating systems can be hosted and managed by a single physical server. Virtualization by using hypervisor is significant to progress on system security, deliver greater flexibility and reliability. Currently, there is a bigger desire to use virtualized systems in corporate enterprises which enable to reduce cost and more proficiently use resources. In this paper, I discuss different types of the hypervisors and virtualization methods and how it benefits in expansion of resources in cloud computing.

Key Words— Cloud, Hypervisor, Virtualization, Virtual Machine

1. INTRODUCTION:

Cloud computing is a network-based environment focused on computer and resource sharing. Clearly, cloud computing is defined as a pool of embedded computer resources. Typically, cloud providers use visibility technology to integrate the computer capabilities of network services and network infrastructure, particularly the internet and multiple internet devices hosted on the same virtual server. From an operational point of view, the cloud computing paradigm allows the load to be used and deployed quickly with the rapid delivery of virtual machines. The cloud computing platform supports modest, highly efficient duplicate models that allow workloads to recover from hardware and software failures. Therefore, in the cloud, consumers only pay for what they use and do not pay for local services such as storage or infrastructure. The actual application uses some very manageable management issues because many backups, software updates, configurations and other administrative tasks are performed automatically and hosted by one of the cloud providers responsible for them. Getting power capabilities is no more a new technology and it lacks enough security capabilities in a large cloud-like network. Virtualization by using hypervisors is growing in popularity in the cloud computing industry especially in the cloud computing business. Mainly, due to its realized cost saving and better management that is achieved from sharing the resources and server optimization. Simulation and modelling techniques are being used by researchers to point out performance bottlenecks and resources contention. As virtualized environments add multiple levels of complexity to outreach models suitable for single physical hardware infrastructure, it faces many challenges in developing performance models which are more accurate.

- *Ramakrishna Subbareddy is currently Research Scholar, Dept of CS, Karpagam Academy of Higher Education, Coimbatore, TamilNadu, INDIA. PH: +91 9731277137 E-Mail: Ramki.blr@gmail.com*
- *Assistant Professor, Dept of CS, CA&IT, Karpagam Academy of Higher Education, Coimbatore, TamilNadu, INDIA. PH: +91 9442179700 E-mail: firdhz.2002@gmail.com*

2. VIRTUALIZATION AND IT'S TYPES:

Encapsulation and abstraction are the two important features of virtualization [2]. An abstract layer is created between hardware and software. Virtualization is broadly used in the huge data centers due to its benefits such as utilization of multiple resources at a time, cost optimization, easy management of servers, optimization and live migration of VMs [3]. Also, multiple virtual server can be run on a single physical server which reduces the Power consumption in the data center when compared to multiple physical server which also add up to the cost. Apparently,

the virtualization in cloud computing could offer dynamic configurations of the resource requirement and applications which is used for different purposes. As an add-on, it surely improves responsiveness maintaining, monitoring and resource provisioning dynamically.

Moreover, there are several types of Virtualization [4]:

- Full virtualization
- Hardware assisted virtualization
- Partial virtualization
- Para virtualization
- Hybrid virtualization
- OS- level virtualization

Virtualization enables partitioning of physical servers, resources into virtual containers which are commonly call as virtual machines. Hypervisor will be playing here by executing the set of the files which denotes virtual hardware. An operating system and application can be installed on this virtual hardware just like any other physical server. Hypervisor, virtual machine monitor and VMs are the core components of virtualized environment. Also, an operating system installed on this VMs

3. HYPERVISOR AND IT'S TYPES:

Hypervisor is one of the components of virtualized environment which is also called a VMM (Virtual Machine Monitor. It is the host which enables various VMs (Virtual Machines) and operating systems on a single physical server [5].

Generally, hypervisors are typically responsible for hosting and managing the VMs on the server. Hypervisors offer even view of the underlying hardware, implying it works on the different hardware of different vendors. Therefore, the VMs can run on any given supported computers since hypervisor separate the software from hardware. VMs that run on the host are Guest VMs or Guest Operating Systems Administrators can view hardware as the pool of resources which also show the operating systems such as Linux, windows and Mac.

There are two types of hypervisors:

A. Bare Metal Hypervisor
B. Hosted Hypervisor

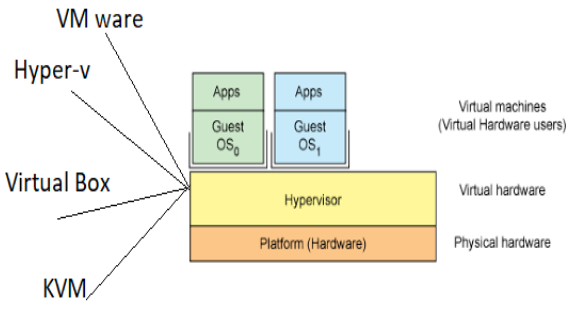

Figure 1. Hypervisor (VMM)

A. BareMetal Hypervisor (Type 1):

A hypervisor which is directly installed in a physical server is called BareMetal Hypervisor. Predominantly, its usage is on servers. Figure 2. Depicts the Bare-metal Hypervisor.

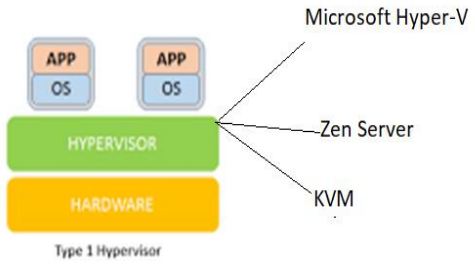

Figure 2. (Bare Metal Hypervisor)

Hypervisor is a vital component of the virtualization environment. At its core, the hypervisor is a host system or operating system.

It is programmed to allow access to the underlying hardware components, as if they had direct access to the hardware. The hypervisor enables the computer to split its operating system into its physical infrastructure. In this position, the hypervisor can provide the physical maintainer with the ability to operate multiple visible units.

It allows the opportunity to install multiple clients on the same server. Server virtualization allows multiple denser deployment at a high price with limited ability to install all computer features.

Each client will receive a copy of their dedicated server. However, virtual server resources such as CPU cycles, memory and network bandwidth are shared among all employers on the server.

The hypervisor is all about the flexibility of the skin. Hypervisors allow increased use of hardware, especially in cases where not all physical sources are used. Virtualization may work, but it does not require a basic OS. Especially when I talk about the load of datacenter related products. Datacenters that monitor hypervisors are installed on top of the bare metal server and not inside the OS. It's program that enables to run multiple operating systems (as shown in Figure 2) as guest OS. Each guest runs separately sharing a single physical Server OR host. There are many hypervisors have been developed. Below table depicts a few.

X86 Hypervisors	Type	Vendor	Licensing
Xen Server	Para, Full	Citrix	Open Source
Esxi	Para, Full	VMware	Proprietary
KVM	Full	IBM	Open Source
Hyper-V	Full	Microsoft	Proprietary

Table 1. Bare-metal Hypervisors

X86 Hypervisor can support both para and full virtualization. No modifications to the core OS are required as they are unaware of the running a virtual environment. Para virtualized Hypervisors need modification for enabling it to work. Para virtualization is good in performance tuning as it gets the direct access to the underlying hardware resources from the hypervisor. However, migration between different hosts is a challenge. In devise-based para virtualization, the devise drivers will improve the performance for some specific devises, for instance virtual network cards and not virtual storage controllers. This devise-based para virtualization futuristically beneficial in a broader sense.

Advantages of Bare-Metal Hypervisors (Type1):

- Enhanced security
- Higher density hardware
- Direct access to HW

Disadvantages of Bare-Metal Hypervisors (Type1):

- Need of specific HW component
- Stringent HW requirement
- Expensive

B. HostedHypervisor (Type 2):

Hosted Hypervisor runs on hosted operating system which also provides the I/O and memory management. The hosted hypervisors are placed between the hardware and the virtual machines. Basically, this type 2 hypervisor are placed above the operating systems and NOT below the OS or VMs which enable another VM can run on the existing virtual machine.

Hosted Hypervisors are basically managed and act as visual error correction controllers. Its built-in functionality allows to do any job. To build and

maintain a virtual environment, a separate software need not be installed on another machine. As one couldn't find any other application within the OS, then type 2 hypervisor is used. Creating summaries or modify tools, import or export, etc. can be achieved through type 2 hypervisor.

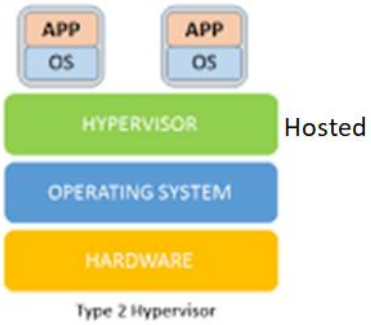

Figure 3 (Hosted Hypervisor)

Hosted Hypervisor can run more operating systems than any other OS. For example, if anyone with Window OS wants to use an application designed for Linux OS, the Linux OS in a virtual environment above Windows VM can be used. Different Types of Hosted (Type2) Hypervisors are shown in the below table 2.

X86 Hypervisors	Type	Vendor	Licensing
Virtual PC	Para, Full	Microsoft	Proprietary
VM ware workstation	Para, Full	VMware	Proprietary
Virtual Box	Full	Oracle (SUN)	Open Source
KVM (kernel based Virtual Machine	Full	Red hat	Open Source

Table 2. Hosted Hypervisor (Type 2)

Advantages of Hosted Hypervisors (Type2):

- Hardware access is controlled by host OS
- Accessibility ease
- Multiple operating systems compatible

Disadvantages of Hosted Hypervisors (Type 2):

- Reduced security
- Low VM density
- Required host OS

4. SECURITY IN HYPERVISOR:

In view mode, there are virtual machines that may have privacy features that are not available on other devices with their own locations. The hypervisor has its own safety point and is the controlling provider of everything inside the monitor. The hypervisor can affect and affect all the actions of visual equipment operating within the hostel [7]. Conventionally, the security areas lie with same infrastructure. This can create a security problem when the attacker controls the hypervisor. After that the attacker completely controls all the details inside the hypervisor area. Another major concern is the safety of the "Essential Machine Escape" or access to a hypervisor within the visual equipment level. This will be a main apprehension as many APIs have been established for acquisition forums [8]. When there is more creation of APIs, the performance and availability will be reduced since controls disables virtual machine's performance inside it to a great extent.

A. Advantages and disadvantages of systems that support hypervisor

The hypervisor, in addition to its ability to manage resources, could protect cloud infrastructure. Secure cloud environment can be achieved by using methods.
Few motives are given below to choose hypervisor technology:
1. A secure infrastructure is achieved via hypervisor since hardware is controlled by it. Access is possible this way. Malicious users can be stopped from hardware infrastructure compromise, since hypervisor acts as a fire extinguisher.
2. In cloud computing area, the usage of hypervisor is under the OS Controller, hypervisor can easily detect when on host operating system, the attack on the security system exceeds.
3. The physical environment from the underground hardware can be separated by using Hypervisor

4. Hypervisor will have a great level of control of all access between under shared hardware and
visitor operating system.
Consequently, in a cloud environment testing, transaction can be simplified by using a hypervisor.

There are weaknesses of the hypervisor in addition to advantages, the performance of the installed security systems can be affected:

1. The system becomes a single point of contact since there is a single hyper visor. All the VMs and programs will be affected when a congestion attack crashes the hypervisor.
2. The hypervisor is vulnerable to few of the firm attacks as in other technologies.

B. Management of security in hypervisorbased virtualization operations

As stated earlier, hypervisor is anadministration tool and creating a reliable environment around VMs and hardware is the main purpose. Hypervisor testing is one of the techniques of VMs, which can enable trust and users can ensure security. Thestages of hypervisor safety management as defined below:

• Authentication: A proper, available, standard and appropriate means should be used to verify the user accounts.
• Authorization: The authorization should be protected by the user. Also, the user should have permission for the things they want to perform on the system.
• Network communication: Secure connection to the system should be a priority while building the network. It should be unique from a regular network connection.

In a management research, verification and validation are most significant featuressince there are numerousconducts to accomplish the drive of accounting by holding checks [9]. When it comes to interaction between hypervisors and user network communication plays very important role and security to it as well. One should understand the APIs and the basic concepts of hypervisor and visual equipment and how those management tools work. Cloud users are on their way to a comprehensive security policy while the security manager administrate the authentication, authorization and security of hypervisor, virtual hardware and security of the network [10]. The visual environment will be conceded when the cloud provider at the visual level depends solely on network security to perform these functions.

5. CONCLUSION:

Virtualization has become more eminent off-late due its cost controlling measures which major corporates enterprise environments use to optimize the IT costs and efficient utilization of their cloud computing resources. This paper emphasized on the virtualization in cloud computing and different types of Hypervisor used the environment of Virtualization. Also, Bare-metal and hosted Types of hypervisors were described. However, each has its own advantages and disadvantages. To improve these virtualized systems, there is a need of performance measures, modelling and simulation besides application of robust security.

REFERENCES

[1] Bohar Singh et. al (2018), International Journal of Computer Science and Mobile Applications, Vol.6 Issue. 1, pg. 17-22

[2] Peter Mell, Tim Grance, (2011) "The NIST Definition of Cloud Computing" Recommendations of the National Institute of Standards and Technology

[3] Anuj C Mohan and S. Shine (2013), "Survey on Live VM Migration Techniques", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(1), pp-155.

[4] VMware, (2008) "Understanding Full Virtualization, Paravirtualization and Hardware Assist", White paper.

[5] Rosenblum, M., & Garfinkel, T. (2005). Virtual machine monitors: current technology and future trends. Computer, 38(5), 39–47

[6] R. Spruijt (2010)," Desktop virtualization and the power of App-V and Windows 7"

[7] G. Texiwill (2009), Is Network Security the Major Component of Virtualization Security?

[8] D. E. Y. Sarna (2011), Taylor and Francis Group, LLC, Implementing and Developing Cloud Computing Applications

[9] T. Ristenpart and et. al (2009), "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the 16th ACM conference on Computer and communications security, Chicago, IL

[10] 2009, "Securing Virtualization in Real-World Environments," White paper.