Bohar Singh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 1, January- 2018, pg. 17-22 **ISSN: 2321-8363**
Impact Factor: 5.515

A STUDY ON VIRTUALIZATION AND HYPERVISOR IN CLOUD COMPUTING

Bohar Singh[1], Gursewak Singh[2]
[1] *Computer Science and Application, bohar2@gmail.com*
[2]*Computer Science and Application, mgursewak@gmail.com*

Abstract

Cloud computing is growing trend in internet technology that enable on demand network access to a shared pool of configurable resources. The virtualization is a core part of cloud computing which enables physical resources to partition into virtual resources so that they can be shared among individual virtual machines. This sharing of virtualized resources can reduce wastage of storage, server and physical machines. The virtualized environment in cloud computing consists of the underlying hardware, hypervisor and virtual machines (VMs) which enables intellectual IT resources on demand dynamic allocation of resources such as network, storage, application, server and client. Virtualization using hypervisor becomes significant as a way to develop system security, provide greater flexibility and reliability. Currently, there is an increased desire to use virtualized systems in enterprise in order to reduce cost and more efficiently utilize resources. This paper describes different types of hypervisor and virtualization techniques, how it helps to expand elasticity of the resources in cloud computing environment.

***Keywords**:* Virtualization, Virtual Machine(VM), Guest OS, Hypervisor

1. Introduction

Virtualization is gaining popularity in enterprise cloud computing environments because of realized cost savings and better management that result from resource sharing and server consolidation. In an effort to improve virtualized systems, researchers look to modeling and simulation techniques in order to pinpoint performance bottlenecks and resource contention. Many challenges unfold in the development of accurate performance models, as virtualized environments add levels of complexity beyond models suitable for single physical machines.

2. Virtualization

Virtualization is a vital technology of Cloud Computing which offers two important features abstraction and encapsulation [2]. It is about creating an abstract layer between hardware and software. Usually, the virtualization layer is set above the physical layer of the Cloud's architecture. Virtualization technology is used widely in Cloud Computing data centres owing to the benefits offered, such as utilizing resources, lowering costs, easier management of servers, server consolidation, and live migration of virtual machines [18]. Through virtualisation, the number of hardware resources used in Clouds can be reduced to minimize the capital cost as well as the cost of power consumption and cooling systems. For instance, through server consolidation, multiple (virtual) servers can be allowed to run simultaneously on a single physical server. Also, live migration of the virtual machine to the not fully utilized physical servers would allow more and more physical servers to be turned off, which would lead to better achievement of energy efficiency for data centres. Furthermore, virtualization in Cloud Computing can offer dynamic configurations for different applications' resource requirements, and aggregate these resources for different needs. Additionally, it can improve responsiveness by monitoring, maintaining and provisioning resources automatically. Therefore, all these features offered by Virtualization are used in Clouds in order to meet the criterion of the business requirements of SLAs.

Furthermore, there are several types of Virtualization [17], some of which are

- full virtualisation,
- hardware assisted virtualisation,
- partial virtualisation,
- para virtualisation,
- Hybrid virtualization and operation system-level virtualisation.

Virtualization allows for the partitioning of physical resources into virtualized containers. These containers, more commonly referred to as virtual machines, are functionally nothing more than sets of files that represent virtual hardware, executing in the context of a hypervisor. This virtual hardware provides a platform on which an operating system and applications can be installed and can be configured to provide almost any service that a physical server typically provides. These services include email, database, hosting, file and print, monitoring, management, and more. The virtualized environment consists of the underlying hardware, the hypervisor, the Virtual Machine Monitor (VMM), the virtual machines (VMs), and the operating systems and applications installed on these virtual machines.

3. Hypervisor/Virtual Machine Monitor (VMM)

The components of the virtualized environment include the hypervisor and the VMM. Most resources agree that the VMM is involved with the scheduling of virtual resources on their underlying physical counterparts, however in some cases the VMM is referred to as the hypervisor itself while in others this is merely a component of a hypervisor in a broader context. To avoid confusion, the VMM will not be a specific point of focus in this paper, since its meaning would change based on context. A hypervisor, also known as the virtual machine monitor (VMM), is the host layer of software that enables multiple virtual machines or operating systems to operate on a single physical server [24].

In general hypervisors are directly responsible for hosting and managing virtual machines on the host or server. The host is another name for the physical server and hypervisor. The virtual machines that run on the host are called guest VM or guest operating system [12]. Furthermore, a hypervisor provides a uniform view of the underlying hardware, which means that it can operate on hardware of different vendors. Hence, virtual machines can run on any available and supported computers, since the hypervisor isolates software from hardware. System administrators, who maintain and operate a computer system and network, are also able to view their hardware as a pool of resources, which allows new functionalities that are described in figure 1. It shows number of guest operating system (window, linux and Mac) are installed on hypervisor.

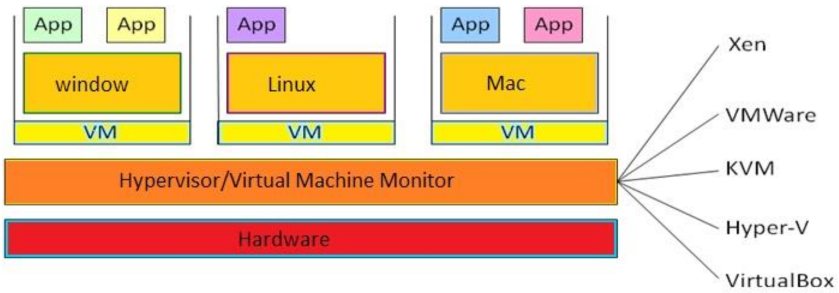

Figure 1 Hypervisor(VMM)

There are two types of hypervisors called “Type 1” and “Type 2”.
This paper specifically focuses on Type 1(bare-metal hypervisors) which are installed directly onto physical hardware. Secondly class of hypervisor (Type 2), known as hosted architectures, requires an underlying operating system such as Windows, Linux, or Mac OS in order to function.

Bohar Singh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.6 Issue. 1, January- 2018, pg. 17-22 ISSN: 2321-8363
Impact Factor: 5.515

3.1 Types of hypervisor

A. Type 1(Bare-metal hypervisor)

Type 1 is a hypervisor that is installed directly on the hardware and is also called a "bare-metal" hypervisor. The hypervisor in figure 2 is a "bare metal" hypervisor. Type 1 hypervisors are dominantly used on the server market.

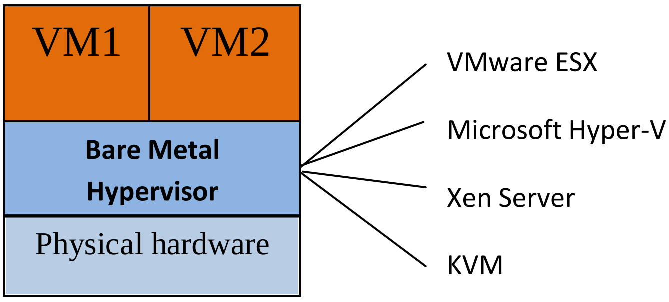

Figure 2: Bare Metal Hypervisor

Hypervisors are an important component of virtualized environments. Hypervisors are programs that allow multiple operating systems(as shown in figure 2), known as guests, to run in virtual machines in an isolated fashion, and thus share a single physical machine, or host. Many different hypervisors have been developed, a few of which are listed in the following table:

Table 1: Bare-Metal Hypervisors

x86 Hypervisors	Vendor	Type of virtualization	Licensing
XenServer	Citrix	Para, Full	Open Source
ESXi	VMware	Para, Full	Proprietary
Hyper-V	Microsoft	Full	Proprietary
KVM	RedHat	Full	Open Source

Some x86 hypervisors can support both fully virtualized and para-virtualized operating systems. Fully virtualized systems are unaware they are running in a virtualized environment, and no modifications to the core operating system are required in order for them to function. Para-virtualized systems, on the other hand, are specifically modified to work in concert with the hypervisor. Prior to recent advances in CPU virtualization technologies, para-virtualized systems enabled performance improvements because the hypervisor could grant a para-virtualized system direct access to the underlying hardware resources on the host. However, para-virtualized operating systems cannot readily be migrated across different hosts in a heterogeneous environment. Recent advances in CPU hardware acceleration have exceeded performance gains garnered by para-virtualized systems, and as such, some vendors are phasing out support for them in their product stack. Another form of para-virtualization is device-based para-virtualization, in which a fully virtualized operating system is configured with special para-virtualized device drivers. These device drivers improve performance for specific devices, such as virtual network cards or virtual storage controllers, without sacrificing mobility. This form of para-virtualization is expected to prove beneficial for the foreseeable future.

Advantage of Type 1 hypervisor

- Enhance security
- Allows higher density hardware
- Hypervisor has direct access to HW

Disadvantage

- Need particular HW component
- Strict HW requirement
- More costly

B. Type2 (Hosted hypervisor)

Hypervisor, which runs on host operating system that provides virtualization services such as I/O and memory management. This is also known as a hosted approach Hypervisor. In other words Type 2 hypervisors are positioned between the hardware and virtual machines that is installed on top of an operating system. In contrast to type 1, the hypervisor is placed above the operating system and not below the operating system or virtual machines. This allows for an additional operating system to be run in a virtual environment on top of an existing operating system.

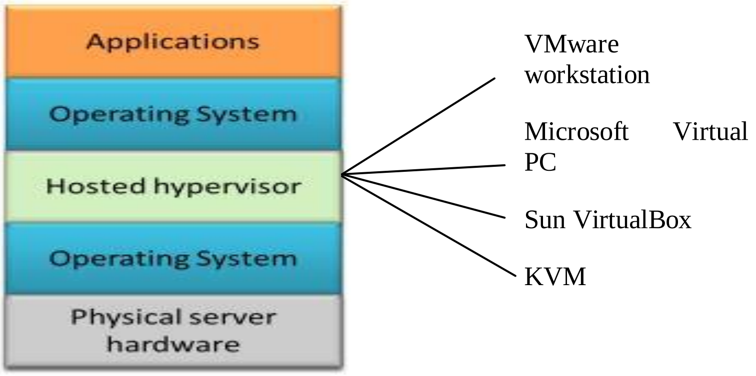

Figure 3:Hosted Hypervisor

Hosted hypervisors can be used to run a different type of operating system on top of another operating system. For example, if a user with a Linux OS wants to run an application that is designed for Windows, he or she can run a Windows OS in a virtual environment on top of the Linux OS and vice versa. Table 2 shows some common Type 2 hypervisor used in virtualization in cloud computing.

Table 2: Hosted Hypervisor

x86 Hypervisors	Vendor	Type of virtualization	Licensing
VirtualBox	Oracle(Sun)	Para	Open Source
VMware workstation	VMware	Para, Full	Proprietary
Virtual PC	Microsoft	Full	Proprietary
KVM(Kernel Based virtual machine)	RedHat	Full	Open Source

Advantages of Type 2 hypervisor

- Host OS Controls HW access
- Ease of access
- Allows for multiple operating systems

Disadvantages

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

4. Conclusion

Virtualization has become more attractive in recent years as cost controlling measures are sought out in enterprise environments to reduce IT costs and effective utilization of cloud resources. This paper explored the virtualization in cloud computing and various type of hypervisor used for resource management in virtualized environments. In this paper Type 1 and Type 2 Hypervisors are described and each hypervisor has its own merits and demerits. In an effort to improve performance of these virtualized systems, accurate performance measures, modeling and simulation are needed.

References

[1] VMware. (2009). History of virtualization. DOI= http:// www. vmware.com/virtualization/history.html.
[2] Mell, P., Grance, T., & Grance, T. (n.d.). The NIST Definition of Cloud Computing Recommendations of the National Institute of Standards and Technology.
[3] Tan, S. (2010). Forecast: Understanding the Opportunities in Virtualization Consulting and Implementation Services. Gartner. Publication Date: 11 March 2010, ID Number: G00174840
[4] 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
[5] Chowdhury, M. K.; Boutaba, R. (2009). A survey of network virtualization. Elsevier. Computer Network 54(2010) 862-876
[6] Goldberg, R.P. (1974). Survey of virtual machine research. Computer, pages 34–45, 1974
[7] Ray, E.; Schultz E. (2009). Virtualization security. ACM International Conference Proceeding Series, art. no. 42
[8] Bittman, T.J. (2008). Server virtualization trends in 2008: Everything changes. Gartner. 11 March 2008
[9] Murphy, A. Virtualization defined – eight different ways.White paper. DOI=http://www.f5.com/pdf/white papers /virtualization - defined-wp.pdf
[10] Cloud Computing Use Cases Discussion Group, "Cloud Computing White Paper", 30 October 2009
[11] Devanathan Nandhagopal, Nithin Mohan, Saimanojkumaar Ravichandran, and Shilp Malpani. "VMware and Xen Hypervisor Performance Comparisons in Thick and Thin Provisioned Environments."
[12] Spruijt, R. (2010). Desktop virtualization and the power of App-V and Windows DOI= http: // www. brianmadden. com/blogs/rubenspruijt/archive/2010/02/22/desktop-virtualizationand-the-power-of-windows-7.aspx
[13] Tan, S. (2010). Forecast: Understanding the Opportunities in Virtualization Consulting and Implementation Services. Gartner. Publication Date: 11 March 2010, ID Number: G00174840
[14] MacDonald, N. (2010). Addressing the most common security risks in data center virtualization projects. Gartner. 25 Januari 2010
[15] Schumate, S. (2004). Implications of Virtualization. Technical Report 2004. DOI = www. dell. com/downloads/ global/power/ps4q04-20040152-Shumate.pdf
[16] Singh, Bohar, and Pawan Luthra. "Review of Linpack and Cloudsimon VMM."arXiv preprint arXiv:1405.6490 (2014).
[17] VMware Inc., "Understanding Full Virtualization, Paravirtualization and Hardware Assist", White paper, 2007.
[18] Mohan, A., & Shine, S. (2013). "Survey on Live VM Migration Techniques", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 2(1), pp-155.

[19] Che, J., He, Q., Gao, Q., & Huang, D., "*Performance measuring and comparing of virtual machine monitors"*. In *Embedded and Ubiquitous Computing, 2008. EUC'08. IEEE/IFIP International Conference on*(Vol. 2, pp. 381-386). IEEE, (2008, December).

[20] Groenhuis, R.; Smith, J. (2010). Transform the Management of Your Virtualized Datacenter. Presentation VMware Forum 2010 Nijkerk. VMware

[21] Padhy, Rabi Prasad, Manas Ranjan Patra, and Suresh Chandra Satapathy. "Cloud computing: security issues and research challenges." International Journal of Computer Science and Information Technology & Security (IJCSITS)1.2 (2011): 136-146.

[22] Ahmed, Mohiuddin, et al. "An advanced survey on cloud computing and state-of-the-art research issues." IJCSI International Journal of Computer Science Issues 9.1 (2012): 1694-0814.

[23] Gebhardt, Carl, and Allan Tomlinson. Security consideration for virtualization. Technical report, Department of Mathematics, Royal Holloway, University of London, 2008.

[24] Mendel Rosenblum, Tal Garfinkel, "Virtual Machine Monitors: Current Technology and Future Trends , ", IEEE Computer, Vol: 38, Issue: 5, 2005.