# Understanding Threats of Multitenancy and Comparative Performance Analysis of Virtualization Technologies

Zinnia Sultana
Assistant Professor
Department Of Computer
Science & Engineering
International Islamic
University Chittagong

## ABSTRACT
With the rapid growth of cloud computing, computing resources are provisioned as metered on demand services over networks and can be easily allocated and released with minimal management effort which increases the security risks. This paper aims to provide an understanding of the different threats created by multi-tenancy and virtualization in a public IaaS cloud. This paper further analyze the performance of Xen hypervisor using Apache benchmark which is chosen as it gives a good idea how the hypervisor is able to handle increasing I/O stress in terms of CPU and memory storage as the number of virtual machines increases, ultimately giving an figurative approach on solving threats created by multi-tenancy and virtualization in a public IaaS cloud.

## Keywords
Cloud, Computing, threats, multi-tenancy, hypervisors, virtualization, benchmark.

## 1. INTRODUCTION
Security is the key for any computing. Many Surveys show [7][8], security in the cloud is the main concern. Few years back, all the organizations were on their private infrastructure and though it was possible to outsource services, it was usually non –critical data or applications on private infrastructures. With the introduction of cloud computing, the story has changed. The computing is no more traditional, and organizations feel they have lost control over data [9]. New attack vectors are introduced and the benefit of being available and accessible from anywhere becomes a major threat.

Cloud computing arrived with the solution to reduce costs in organizations and at the same time to provide on-demand resources and computation without requiring to create an IT infrastructure. Services, such as Amazon Web Services or Microsoft Azure, provide a means for organizations to instantly provision and de-provision virtual machines (VM) depending on their needs, just paying for what they use.

In order to make necessary environment, cloud service providers (CSP) make use of virtualization technologies to maximize the value of their systems. Servers have always needed to run alone in physical machines to avoid their services to interface with them; but the downside of this was the waste of resources. Virtualization enables the use of all the resources in a physical host by sharing them between operating system.

Many organizations have already deployed private clouds on their own infrastructures or through third parties. However, public Clouds provide an additional advantage that makes it extremely attractive, cost savings. The resources for a cloud consumer seem to be unlimited by sharing all the host machines between organizations. At the same time, the CSPs can easily maximize the use of each physical machine.

## 2. LITERATURE REVIEW
The concept of virtualization technologies came long before the cloud computing in the IT world. Marshal et al.[1] and Haletky [2] explore the requirements of virtualization and provide a deep view of the VMware ESX server also provides a clear definition of virtualization and explores the necessary steps to deploy a secure virtualization using VM ware ESX server.

Velte et al.[3] and Reese[4], include an overview of virtualization technology and its security issues focused on virtualization in cloud environments.

Almond et al. [5] presented a document which is used as a reference. The CSA [6] and ENISA [7] provide material related to the security concerns of the multitenant architecture used in the cloud, especially in public clouds.

Institute of Standards and technology (NIST) [8] provides a great definition for cloud computing [9] including its services models, deployments models and characteristics.

Cloud Security Alliance (CSA) [10] has got a lot of frame and attention due to its remarkable contribution to the cloud. Supporting NIST's definition the document for security guidance [11]

Amazon Elastic Compute Cloud (EC2)[12], Ristenpart et al. [13] explored the different steps to perform an attack on aVM.

An overview of the typical threats to a hypervisor from a malicious VM is provided by the Burton Group. Ormandy [14] explores the security explores of host machines in virtualized environments.

Kortchinsky[15] researches a PoC of a VM escape in IBM's Cloudburst[IBM]. Kato [16] research discovered vulnerability on VMware that allows the ise of a backdoor to perform a VM escape.

## 3. CLOUD COMPUTING
### 3.1 Defining Cloud Computing
NIST [9] defines, "Clod computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction."

### 3.1.1 Cloud Computing Security

The challenges regarding security in cloud computing worth a book at least, so it is not possible to define all in this piece of work. However, an overview and understanding of the issues and how the cloud infrastructure affects the information security risks in each service model is given.

The CSA provides twelve domains of concern [11] for cloud computing to address the strategic and tactical security problems. These areas are divided into two broad categories: governance and operational.

The measures required for security controls in cloud environments are not that different from the traditional ones but differ are the new risks created by the technologies, services and deployment models used that were not present before. For example, in cloud environment firewalls will still be needed, what will change is how they are configured and deployed to cope with the communications between VMs on the same host machine where there is no physical network involved, or how to deal with multiple tenants with different levels of security located in the same physical server.

Delineation of responsibility where the above red line tenants or users are responsible for the security management and below the red line vendor or provider is responsible for all the security issues in three different service model of cloud computing.

**Fig1: Delineation of responsibility**

| IaaS | PaaS | SaaS |
|---|---|---|
| Interface | Interface | Interface |
| Application | Application | Application |
| Solution Attack | Solution Attack | Solution Attack |
| Opertating System | Opertating System | Opertating System |
| Hypervisor | Hypervisor | Hypervisor |
| Compute & Storage | Compute & Storage | Compute & Storage |
| Network | Network | Network |
| Facility | Facility | Facility |

### 3.1.2 Multienancy

IBM[5] defines the term multi-tenant as the ability to provide computing services to multiple customers by using a common infrastructure and code base. In a multitenant environment, tenants have a private and a common space shared amonst all tenants.

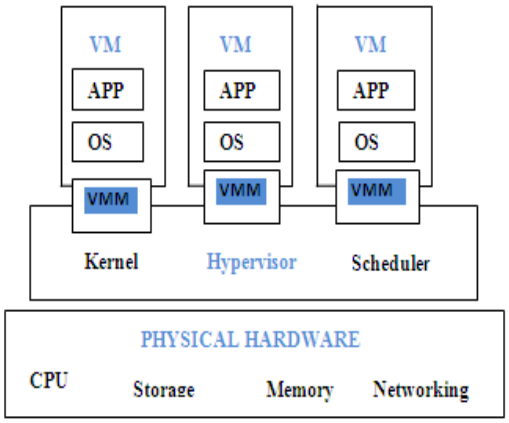


**Fig2: Components that can be shared across multiple tenants.**

## 4. THE THREATS

In order to use the infrastructure more efficiently, CSP's enable multi-tenancy allowing different tenants/VMs to coexist on the same physical host separating them with a virtual layer of isolation. VMs in the same physical host shares the resources of that physical machine and at the same time each VM will be separated from the others creating a false state of isolation. It is called false layer because full isolation of VMs are never possible.

Multitenancy introduces many risks in all the cloud service models, but especially IaaS clouds where the consumers have a lot of control. However, it needs to be considered that some CSP's are actually hosted in IaaS clouds. For example, some SaaS providers like Twitter make use of services from IaaS providers like Amazon Web Services (AWS). Thus, the risk also extends to the users of those SaaS.

Broadly speaking there are three types of attacks on VMs.

VM-to-VM: An attacker uses a VM to communicate and compromise other VM on the same physical host; therefore breaking the false isolation layer of VMs.

Denial of service (DoS): An attacker will try to exhaust the resources unavailable from a physical host in order to deny service of the other VMs in the machine. As the source of the attack is a VM and the target is the co-resident VMs, DoS will be considered as a VM-to-VM attack.

VM-to-Hypervisor: An attacker tries to penetrate the isolation created by the hypervisor in order to compromise it, which potentially gives access to the host OS and hardware.

## 5. EXPERIMENTAL RESULT

A simplest way has chosen to perform certain tests. To compare the hypervisors the system is virtualized as Processor: Intel Core i5 430M (2.26GHz, 1066MHz, 3MB) OS: Windows 8 Professional (32 bit) Memory: 4GB Dual Channel DDR3 at 1066MHz Storage. To run the system in tandem I virtualized external1Tb hard disk. Three instances of operating system is created at the top of every virtualization technology where one of them is Linux Ubuntu and the other two are Windows 7 operating system.

## 6. COMPARISONS

### 6.1 Feature Comparison

It is often difficult for users to identify which platform is best among different virtualization techniques. It is true that that none of the virtualization technique is bad but necessity

depends upon the superlative degrees. A detailed comparison chart between VMWare ESX, VirtualBox 3.2, Xen 3.1 and KVM from RHEL5 is given to show the simplification of this task.

**Table 1. Features Comparison Table**

| | Xen | KVM | VBox | VMWare |
|---|---|---|---|---|
| Para-virtualization | Yes | No | No | No |
| Full virtualization | Yes | Yes | Yes | Yes |
| Host PC | x86, x86-64, IA-64 | x86, x86-64, IA64, PPC | x86, x86-64 | x86, x86-64 |
| Guest PC | x86, x86-64, IA-64 | x86, x86-64, IA64, PPC | x86, x86-64 | x86, x86-64 |
| Host OS | Linux, UNIX | Linux | Windows, Linux, UNIX | Proprietary UNIX |
| Guest OS | Linux, Windows, UNIX | Linux, Windows, UNIX | Linux, Windows, UNIX | Linux, Windows, UNIX |
| VT-x/AMD-v | Opt | Req | Opt | Opt |
| Cores supported | 128 | 16 | 32 | 8 |
| Memory supported | 4TB | 4TB | 16GB | 64GB |
| 3DAcceleration | Xen-GL | VMGL | Open-GL | Open-GL, DiectX |
| Live Migration | Yes | Yes | Yes | Yes |
| License | GPL | GPL | GPL/proprietary | Proprietary |

## 6.2 Technical Comparison (KVM & XEN)

The comparison between KVM and XEN says that in the host operating system KVM isn't an option on older CPUs. In Sysbench simple CPU load performance there is a very dominance time which implies that the system spend the most time on syscalls or LRQ servicing routines

**Table 2. Technical Comparison (KVM & XEN)**

| | KVM | XEN |
|---|---|---|
| **Host OS** | | **Better** |
| **Market** | | **Better** |
| **OS overhead** | | **Better** |
| **Security** | | **Better** |
| **Maturity** | | **Better** |
| **Memory Page Sharing** | **Better** | |
| **Ease of Use** | **Better** | |
| **I/O Latency** | **Better** | |

## 6.3 Technical Comparison (VM ware & Vbox)

In technical comparisons between the virtualization techniques certain few points are considered though there can be many other functionality to be considered.In host operating system support, we found virtual box is better and configuring, updating and editing is easier in virtual box then that of VM-ware. VM ware is better in USB support. Virtual box supports relatively larger range of virtual hard disks. Teleportation or migration of VM in virtual box is better along with the command line options where copying and editing is very easy. In case of graphics and Ovf support it is found that VM-ware is better.

**Table 3. Technical Comparison (VMwae&Vbox)**

| | VMware | Virtual box |
|---|---|---|
| **Host OS Support** | | **Better** |
| **VM editing** | | **Better** |
| **USB support** | **Better** | |
| **Range of Virtual Hard disk** | | **Better** |
| **Remote connection** | | **Better** |
| **VM cloning** | | **Better** |
| **Graphics** | **Better** | |
| **Cmd line** | | **Better** |
| **Teleportation** | | **Better** |
| **Ovf support** | **Better** | |

## 6.4 Benchmark Performance Comparison

1. CPUspeed

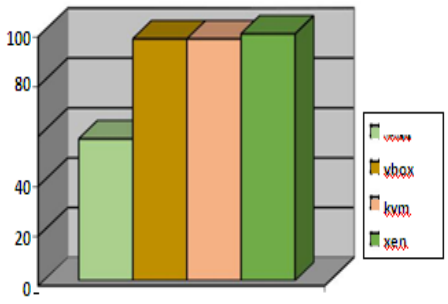


**Fig3 : CPU overhead performance**

In Sysbench simple CPU load performance we see a very dominance time which implies that the system spend the most time on syscalls or IRQ servicing routines. Comparatively XEN seems to be the winner.

2. Cache and Memory Performance

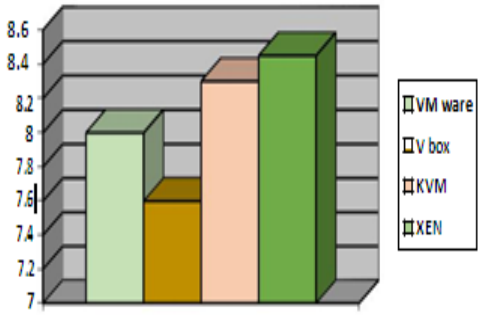


**Fig4: Cache and memory performance**

Cache and memory speed performance shows that XEN is slight faster and least Vmware and Vbox. It seems that Xen do a good use of nested page table feature.

3. Sequential read performance (GB/s)

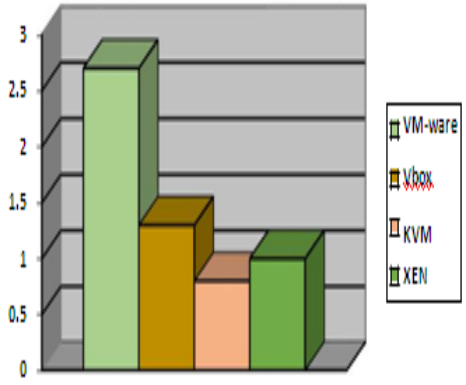


**Fig 5: Sequential read performance**

In sequential read test KVM is much slower due to very poor caching and great I/O overhead.

4. Sequential write performance

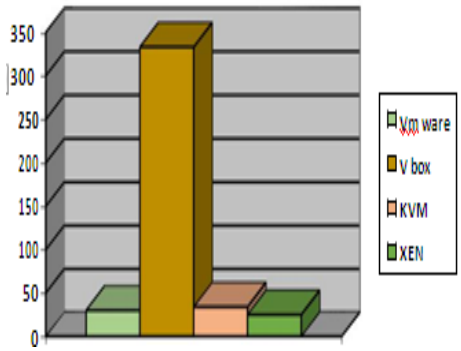


**Fig 6: Sequential write performance**

Sequential write test amazed us the faster is virtual box it seems like it use write back cache algorithm while the other use a write through policy , though greater risk of data loss in spite of speed . In this test KVM and XEN are the closer.

## 7. RESULTS

In short, each supports Linux x86 64 platforms, use VT-X technology for full virtualization, and support live migration. From a CPU and memory point of view, Xen seems to pro-vide the best expandability, supporting up to 128 cpus and 4TB of addressable RAM. So as KVM's CPU limit. One of Virtualbox's greatest limitations was the 16GB maximum memory allotment for individual guest VMs, which actually limited us from giving VMs more memory for our perfor-mance benchmarks. If this can be fixed and Oracle does not move the product into the proprietary market, VirtualBox may also stand a chance for deployment in HPC environ-ments. The data compression and decompression test also is very useful to determine which virtualization technique to be choosen. In this research work we have also tried to give the reasons behind such performance of the virtualization tech-nologies.

## 8. CONCLUSION AND FUTURE WORK

Security in cloud computing must be approached cautiously. Multiple users run their systems on the same physical host machines in isolated environments and sharing the physical resources so every tenant should know and accept the fact that they are not alone and they should be cautious. This paper has provided an overview of cloud computing, including multitenant architectures and virtualization technologies. Finally it has been observed that none of the virtualization technologies can be marked as best or worst because their technologies are efficient enough in their own way of computing.

The focus of future works should aim to harden the security of virtualizations in multitenant environments, implementation strict laws and encrypting the assets can be the future work. To achieve secure virtualized environments, isolation between the different tenants is needed. Many other various performance tests can be performed even in better ways so comparing these most common hypervisors on the basis of other remarkable features can be the future work.

## 9. REFERENCES

[1] D. Marshall, S.S. Beaver, J.W.Mc Carty, VMware ESX: Essentials in the virtual Data Center, CRC press, 2009.

[2] E.L.Haletky, VMware ESX Server in the Enterprise: Planning and Securing Virtualization Servers, Prentice Hall, 2008.

[3] A.T.Velte, T.J. Velte, R. Elsenpeter, Cloud Computing: A practical Approach, McGraw-Hill,2010

[4] G. Reese, Cloud Application Architectures: Building Applications and Infrastructures in the cloud, O'Reilly , 2009 Ahmad, J., Zaidi, S.M.H and Nawaz, S.,(2004) Dynamic Routing in wavelength Convertible WDM Networks, IEEE.

[5] C. Almond, P.C. Chiquito, C.H. Fachim, S. Kim, M. Okajima & P.Ramo, Multitenant Utility Computing on IBM Power Systems Running AIX, IBM Redbooks, 2009,http://www.redbooks.ibm.com/redbooks/pdfs/sg24 7681.pdf

[6] Cloud Security Alliance, Security guidance for Critical areas of Focus in Cloud Computing V2.1, December 2009,https://cloudsecurityalliance.org/wpcontent/uploads /2011/07/csaguide.v2.1.pdf

[7] European Network and Information Security Agency, Cloud Computing benefits, risks and recommendations for information security, November 2009, http://www.enisa.europa.eu/act/rm/files/deliverables/clou d-computing-risk-assesment.

[8] National Institute of Standards and Technology(NIST), http://www.nist.gov

[9] P.Mell and T.Grance, The NIST Definition of Cloud Computing, National Institute of Standards and Technology (NIST), July 2009, http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf

[10] Cloud Security alliance (CSA), http://cloudsecurityalliance.org/

[11] Cloud Security alliance, Security Guidance for Critical Areas of Focus in Cloud Computing v2.1, December 2009, https://cloudsecurityalliance.org/wpcontent/uploads/201/ 07/csaguide.v2.1.pdf

[12] Amazon Elastic Compute Cloud(EC2), http://aws.amazon.com/en/ec2

[13] T.Ristenpart, E. Tromer, H. Shacham, and S. Savage, Hey,you,fet off my cloud: exploring information leakage in the third-party compute clouds, In proceedings of the 16th ACM conference on Computer and communications security(CCS'09), 2009

[14] T. Ormandy. An empirical study into the security exposure to hosts os hostile virtualized environments. CanSec West Applied Security Conference,2007

[15] K.Kortchinsky, Cloudburst, Presented at Black Hat USA 2009, Las Vegas, http://www. Blackhat.com/presentations/bh-usa-09/KORTCHINSKY/BHUSA09-Kortchinsky-Amstutz, S.R., (1989). Burst Switching- An update. IEEE Communication, 50-57

[16] K. Kato, VMware Backdoor I/O Port, Accessed on August2011,http://sites.google.com/site/chitchatvmback/backdoor