SECURITY ANALYSIS OF VIRTUALIZATION IN CLOUD COMPUTING

Deepika Saxena[1], Dr. Navneet Sharma[2] & Geetika Malik[3]
[1]*Computer Science, ICG, The IIS University, Jaipur, India*
[2]*Computer Science, IIS University, Jaipur, India*
[3]*Computer Science, Jaganath University, Jaipur, India*

Abstract

Cloud computing is a technology that enables organizations to share various services in a seamless and cost-effective manner by providing required resources, applications, software, hardware, computing infrastructure, business process to control collaboration. Today clouds with virtualization are transforming IT. Security problems square measure the part considerations of virtualization technology once there's information communicate and application attain from such virtual machine to a different because it is an incontrovertible threat for potency. Virtualization is that the base of cloud computing, it's doomed to possess a lot of development to steal attacks, intrusions and system failures. This technology permits the introduction of logical instances and figures them to run at the same time by having totally different operative systems by all of the compatible applications every place existing physical resources. Here we have a tendency to introduce an approach to permit the safety of the Virtual machines and their needed resources by permitting them to trade usually certainly. In this paper, we studied performance and security issues with respect to efficiency, integrity and cost in cloud computing.

Keywords*: Cloud computing, Hypervisor, virtualization, Privacy, Virtual Machine, Container.*

Introduction

Cloud computing is that the production of a "cloud of computing", in line with that programs are put up and produce the results of function in a standard web browser window on a local PC, reciprocally all applications and their information binding for operation placed on an isolated server on the internet[1]. If we have a tendency to discuss concerning the (virtualization) virtual machine, therefore we are able to say virtual machine could be a machine that helps to enhance the potency of cloud computing, with the assistance of virtualization we are able to work on multiple software system and application at the same time over a similar server.

Virtualization

Virtualization involves technologies designed to point out a layer of repression between constituent systems and therefore the computer code running on them [2]. Virtualization methodology to compose a virtual version of a tool or resource, comparable to a server, storage analogy, is part of or eventually a software system wherever the context divides the resource into such or ideally execution environments [3]. Virtualization is generally defined as a technology that introduces a software abstraction layer between the hardware and the operating system and applications running on transcend of it. This abstraction layer is called virtual machine recognize (VMM) or hypervisor and generally hides the temporal resources of the computing route from the operating system (OS). Since the hardware resources are now controlled every VMM and not aside OS. It's possible to run multiple (possibly different) OSs in simulating on the connected hardware.

As a confirm the hardware platform is divided into such or a lot of agreeable units referred to as virtual machines (VMs).

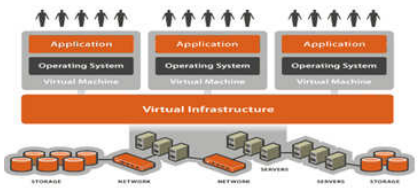
Before Virtualization

- One OS image on one machine
- Software and hardware are tightly coupled
- Attempt to run more than one application on same time machine often creates conflict
- Not so flexible and even costly infrastructure

After Virtualization

- Independence of operating system and application from under layering hardware
- A Virtual machine can easily provide to any system.
- OS and application can easily be managed as one complete entity by wrapping up them into a virtual machine.

Virtualization Infrastructure

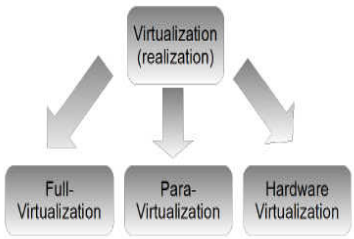


Virtualization

Classification

Virtualization permits abstraction and isolation of lower level functionalities and underlying hardware. This permits movableness of upper- level functions and sharing and/or aggregation of the physical resources. The various virtualization approaches may be categorized into:

Full Virtualization – In this, the particular hardware is totally simulated, takes place to permit software to run an unmodified guest OS. Guest computer software doesn't need any modification to run.



- Para -Virtualization software unmodified runs on modified OS as a separate system.
- Partial Virtualization – the hardware is not simulated. The guest software runs their own isolated domains.

Advantages of virtualization in cloud computing

Virtualization technology makes cloud computing environment easier to manage the resources. It abstracts and isolates the underlying hardware and networking resources in a single hosting environment. It increases the security of cloud computing by protecting both the integrity of a guest virtual machine and cloud components virtualized machines can be scaled up or down on demand and can provide reliability. It provides resource sharing, high utilization of pooled resources, rapid provisioning and workload isolation. The recent trends in virtualization are a consolidation of data centres thus reducing the managing cost. Apart from its benefits it has some drawbacks like managing virtual resources is critical and migrating services of these resources are difficult in achieving high availability. If one server fails VM will be restarted on the other virtualized server in resource pool restoring the required services with minimum service interruption. Virtual resources are critical for managing and data monitoring. Running applications with high utilization and availability is a challenging issue. Hypervisor: A

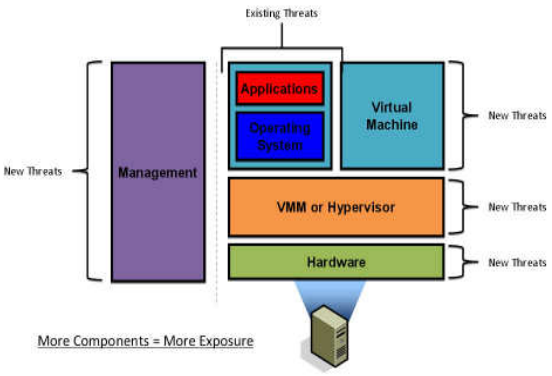
hypervisor is a software, hardware or a firmware that provides virtual partitioning capabilities which run directly on hardware. It is defined as the virtual machine manager which allows multiple operating systems to run on a system at a time providing resources to each OS without any interaction. Hypervisor controls all the guest systems. As the operating system number increases managing is difficult these leads to security issues. If a hacker gets control over the hypervisor he can control the guest systems by knowing the behaviour of the system which causes data processing damage. The advanced protection system is to be developed to monitor the activities of the guest Virtual machine [17].

VM Services

Virtualization provides some tools to facilitate and help in the administration, and provide some services. One of the services is migration that allows VM to be transferred between physical machines, in case one physical machine became down, this will allow the work on the VM to continue without waiting for the physical machine. Using virtualization, new VMs can easily be created via images file format, which is a package template. A useful feature of virtualization is clipboard that permits data transfer between guest and host machines. Great care should be taken when using these tools and services, that they don't impose security vulnerability.

VM Security and Threats

There are at least two levels of virtualization such as VMs and the hypervisor. Virtualization is not a new technology as a cloud but in it, there are several security issues that now migrated to cloud technology. Also, there are other vulnerabilities and security issues which unique in a cloud environment or may have a more critical role in cloud. In the hypervisor, all the users see their systems as self-contained computers isolated from other users, even though every user is served by the same machine. In this context, a VM is an operating system that is managed by an underlying control program.



There are various threats and attacks on this level that major issues mentioned below:

VM level attacks:

Potential vulnerabilities are the hypervisor or VM technology used by cloud vendors are a potential problem in multi-tenant architecture [18]. These technologies involve "VMs" remote versions of traditional on-site computer systems, including the hardware and operating system. The number of these VMs can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies [19]

- **Cloud provider vulnerabilities**:

These could be platform-level, such as a SQL-injection or cross-site scripting vulnerability that exist in cloud service layer which causes insecure environment.

- **Expanded network attack surface**:

Cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases [19].

- **Authentication and Authorization:**

The enterprise authentication and authorization framework do not naturally extend into the cloud Enterprises have to merge cloud security policies with their own security metrics and policies.

- **Lock-in:**

It seems to be a lot of angst about lock-in in cloud computing. The cloud provider can encrypt user data in particular format and if a user decides to migrate to another vendor or something like [9].

- **Data control in a cloud:**

For midsize businesses used to having complete visibility and control over their entire IT portfolio, moving even some components into the Cloud can create operational "blind spots", with a little advance warning of degraded or interrupted service [6].

- **Communication in virtualization level:**

VMs have to communicate and also share data with each other. If these communications didn't meet significant security parameters then they have a potential of becoming attacks target. As mentioned before, virtualization is the main element in today's cloud computing. It separates the physical hardware from the guest operating system (OS). This separation allows the guest operating system to migrate from one physical server to another.

There are two types of VM migrations: non-live migration or live migration.

In non-live migration, all applications running on the VM will be stopped during the VM migration, while in live migration, all applications continue running without any interruption. Moreover, there are several objectives of VM migration, such as power management, load balancing, and system maintenance [10]. Power management will power off VMs in underutilized servers in order to ensure power saving. Moreover, load balancing will help to avoid overlap by migrating VMs from a host with a heavy load to another host with a lesser load. Additionally, system maintenance will improve the reliability and availability of the system.

A lack of security in this scenario may allow an attacker to exploit live migration operation in different ways:

Denial-of-service attack:

the attacker will create many VMs on the host OS for no reason other than to make the host OS overloaded, which will make the host OS not accepting of any migrated VM.

Unnecessary migration of VM:

In this situation, the attacker will overload the host OS by unneeded VMs. This will run the dynamic load balancing feature. This feature will migrate some VMs from a loaded host to another unloaded host.

Disrupt the regular operations of the VM:

An attacker may migrate a VM from one host to another host without any goal except to interrupt the operations of the VM.

An attack on VMM and VM:

In this kind of attack the predator will migrate a VM that has a malicious code to a host server that has the target VM. This code will exchange information with the VMM and the target VM through a covert-channel. This channel will compromise the confidentiality of the host server by leaking target VMs' information. Control of incoming migration: The attacker may migrate the target VM from one host server to the attacker host server, which results in getting full control of the target VM. Advertising for false resource: This occurs when the attacker advertises false resource availability for the target VM. Attack the VMM by itself after identifying a way to enter the system

Tenants of cloud systems commonly assume that if their data is encrypted before outsourcing it to the cloud, it is secure enough. Although encryption is to provide solid confidentiality against attack from a cloud provider, it does not protect that data from corruption caused by configuration errors and software bugs [11]. There are two traditional ways of proving the integrity of data outsourced to a remote server. Checking the integrity of data can be by a client or by a third party. The first one is downloading the file and then checking the hash value[12]. The second one is to compute that hash value in the cloud by using a hash tree [13]. In this technique, the hash tree is built from bottom to top where the leaves are the data and parents are also hashed together until the root is reached[14]. The owner of data only stores the root. When the owner needs to check his data, he asks for just root value and compares it with the one he has[15]. This is also to some extent is not practical because computing the hash value of a huge number of values consumes more computation. Sometimes, when the provided service is just storage without computation[16]. It is possible to achieve cost reductions by consolidation smaller servers into more powerful servers. Cost reductions stem from hardware cost reductions (economies of scale seen in faster servers), operations cost reductions in terms of personnel, floor space, and software licenses.

Conclusion

In summary, using virtualization technology can enable running two or more operating systems on a single computer reducing the potential cost. The paper has presented some of the flaws in the virtual machine environment. In storage compared with virtual machines. A new kind of application platform doesn't come along very often. But when a successful platform innovation does appear, it has an enormous impact. Think of the way consistent type of application environment no matter which type of operating system the application is hosted on. If we use containers to host a micro services application, we can link security problems to specific micro services. This makes it easier to find and resolve vulnerabilities without disrupting the entire application. If we host applications on a virtual server, we have to secure the bare-metal host server, the virtual server and the application itself. With containers, we only need to secure the host, the Docker daemon (which is much smaller than a virtual operating system) and the application running inside the container. For this reason, containers give us a smaller attack surface to protect.containers are lightweight with regard to storage size. In case of performance containers increase performance (throughput) because they do not emulate the underlying hardware in place of virtual machine. In real-time applications containers provide more consistent timing than virtual machines. VMs take up a lot of system resources.

Each VM runs not just a full copy of an operating system, but a virtual copy of all the hardware that the operating system needs to run. This quickly adds up to a lot of RAM and CPU cycles. In contrast, all that a container requires is enough of an operating system, supporting programs and libraries, and system resources to run a specific program. In this paper we have studied various performance issues of virtualization & Containers, containers can give better performance, can enable to handle with more application into a single physical server than a virtual machine (VM).

References

1. Buyya R., Ranjan R. and Calheiros R.N. Modeling and simulation of scalable cloud computing environments and the cloudsim toolkit: challenges and opportunities, High Performance Computing & Simulation HPCS'09, 2009, pp. 1-11.
2. Aishwarya Anand "Amazon's Approach to Cloud Security" Proceedings of 4th IRF International Conference, Pune, 16th March-2014, ISBN: 978-93-82702-66-5 pp. 173-178
3. Pankaj Sareen " Cloud Computing: Types, Architecture, Applications, Concerns, Virtualization and Role of IT Governance in Cloud " International Journal of Advanced Research in Computer Science and Software EngineeringVolume 3, Issue 3, March 2013 ISSN: 2277 128Xpp. 533-538
4. L. Shi, H. Chen, J. Sun," vCUDA: GPU accelerated high performance computing in virtual machines," in: Proceedings of the IEEE International Symposium on Parallel and Distributed Processing, 2009
5. Farzad Sabahi, "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology", Int. Journal of Machine Learning and Computing, pp.39-45, vol. 2, no. 1, February, 2012
6. R. Chow, et a!., "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the CCSW'09, Chicago, Illinois, USA., 2009.
7. D. Talbot. (2009). Vulnerability Seen in Amazon's Cloud-Computing. Available:
8. http://www.technologyreview.comlprinter jriendly arti cle.aspx?id=23792
9. D. E. Y. SAR NA, Implementing and Developing Cloud Computing Applications: Taylor and Francis Group,LLC, 2011.
10. P. Sefton, "Privacy and data control in the era of cloud computing."
11. R. Ahmad, A. Gani, S. Hamid, M. Shiraz, F. Xia, and S. Madani. "Virtual machine migration in cloud data centers: a review, taxonomy, and open research issues". The Journal of Supercomputing, vol. 71., no.7, pp. 2473-2515, July 2015.
12. Shetty, A. M R and S. G, "A Survey on Techniques of Secure Live Migration of Virtual Machine". *International Journal of Computer Applications,* vol. 39, no. 12, pp.34-39, February 2012.
13. C. Xianqin, G. Xiaopeng, W. Han, W. Sumei, and L. Xiang, "Application-Transparent Live Migration for Virtual Machine on Network Security Enhanced Hypervisor". *China Communications*, vol. 8, no. 3, pp. 32-42, 2011.
14. W. Wang, Ya Zhang, B. Lin, X. Wu, and K. Miao, "Secured and reliable VM migration in personal cloud," *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, Chengdu, 2010, pp. V1-705-V1-709. doi: 10.1109/ICCET.2010.548537

15. X. Wan, X. Zhang, L. Chen, and J. Zhu, "An improved vTPM migration protocol based trusted channel," *Systems and Informatics (ICSAI), 2012 International Conference on*, Yantai, 2012, pp. 870-875. doi: 10.1109/ICSAI.2012.6223146.
16. K. Nagin et al. "Inter-cloud mobility of virtual machines," in *Proceedings of the 4th Annual International Conference on Systems and Storage (SYSTOR '11).* 2011, pp.1-12. DOI=http://dx.doi.org/10.1145/1987816.1987820
17. Y. Chen, Q. Shen, P. Sun, Y. Li, Z. Chen, and S. Qing, "Reliable Migration Module in Trusted Cloud Based on Security Level – Design and Implementation," *Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International*, Shanghai, 2012, pp. 2230-2236. doi: 10.1109/IPDPSW.2012.275s
18. http://www.cse.iitd.ernet.in/~sbansal/csl862-virt/2010/readings/software_hardware_tech_x86_virt.pdf
19. J. Kirch. Virtual machine security guidelines. *The center for Internet Security*, September 2007. http://www.cisecurity.org/tools2/vm/ CIS_VM_Benchmark_v1.0.pdf.
20. D. Rowe. (2011, The Impact of Cloud on Mid-size Businesses. Available:
21. http://www.macquarietelecom.com/hosting/blogicloudcomputing/impact-cloudcomputing-midsize-businesses