ISSN: 2277-9655
Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

CLOUD RESOURCE VIRTUALIZATION TOWARDS SECURITY

Shambhu Prasad Sah*, Sanjeev Kumar Panjiyar, Purushottam Das, Ankur Singh Bist
* Assistant Professor, Deptt. of CSE, Graphics Era Hill University, Nainital, Uttarkhand, India
M.Tech Student, Dept of CSE, JNTU Hyderabad, India
Assistant Professor, Deptt. of CSE, Graphics Era Hill University, Nainital, Uttarkhand, India
Assistant Professor , KIET Ghaziabad

DOI: 10.5281/zenodo.51427

ABSTRACT

Cloud computing is an advanced technology or engineering that increase IT technologies potentialities in terms of usage ,running, elastic resource(storage, computing power, servers, bandwidth etc) management and collaborative execution approach. The most critical aspect of cloud computing is cloud resource virtualization which is equally important for cloud providers and their subscribers. The resources comes in various forms such as client, applications, storage, server, network etc.. This paper focus as on how virtualization helps to improve security by protecting the integrity of virtual machines and cloud components and elasticity of the resources, in cloud computing surroundings. This paper also provides an add-on on hardware support for virtualization and open source virtualization methods, challenges and future research direction.

KEYWORDS: Cloud computing, virtualization, elasticity, hypervisor, virtual machines.

INTRODUCTION

Internet is on the edge of another revolution, where resources are globally networked and can be easily shared. Cloud computing is all about utilizing technology as a service. This form of computing is the main component of this paradigm shift that pictures the Internet as a large repository where the computing resources are available to everyone as services.

National Institute of Standards and Technology (NIST) has given a definition [1] for Cloud computing which says that ―Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (eg., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Five essential traits of cloud computing named by NIST are on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

According to the NIST reference model [11] in Figure 1. the entities involved in cloud computing are the service consumer, the entity that maintains a business relationship with and uses service from service providers; the *service* provider, the entity responsible for making a service available to service consumers; the carrier, the intermediary that provides connectivity and transport of cloud services between providers and consumers; the *broker*, an entity that manages the use, performance, and delivery of cloud services and negotiates relationships between providers and consumers; and the auditor, a party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.

An audit is a systematic evaluation of a cloud system that measures how well it conforms to a set of established criteria.[8] For example, a security audit evaluates cloud security, a privacy-impact audit evaluates cloud privacy assurance, and a performance audit evaluates cloud performance

ISSN: 2277-9655
Impact Factor: 3.785

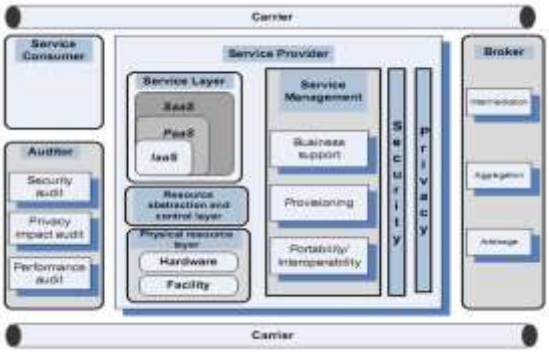

Fig1: NIST reference model

CLOUD VIRTUALIZATION

Virtualization [12] fig 2 abstracts or hook the implicit resources and simplifies their use, separates users from one another, and supports replication, which ,in turn, enhances the elasticity of the system. Virtualization is a central aspect of cloud computing, equally important to the providers and consumers of cloud services, and plays significant role in:

- System security because it allows isolation of services running on the same hardware.
- Performance and reliability because it allows applications to migrate from one platform to another.
- The development and management of services offered by a provider.
- Performance isolation.
- Virtualization models[12] the interface to a physical object by any one of four means:

1. **Multiplexing**. Multiple virtual objects are created from one instance of a physical object. For instance, multiplexing of a processor among number of processes or threads.
2. **Aggregation**. In this single virtual object is created from multiple physical object. For example, a RAID disk is aggregated from a number of Physical disks .
3. **Emulation**. In this a virtual object is created from different types of physical object. For example, a physical Disk emulates a random access memory.
4. Multiplexing and emulation. For instance: Virtual memory with paging multiplexes real memory and disk, and a Virtual address emulates a real address; TCP emulates a reliable bit pipe and multiplexes A physical communication channel and a processor

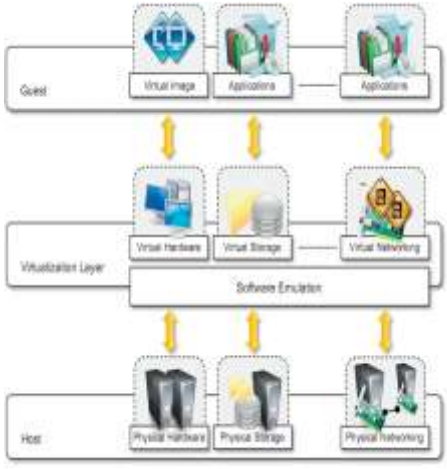

Fig 2: Virtualization Reference Model

ISSN: 2277-9655
Impact Factor: 3.785

Virtual Machine Monitor or Hypervisor: Particular software that firmly partitions the resources of a computer system into one or more virtual machines is known as VMM or hypervisor. A guest operating system is an Operating system that runs under the control of a VMM rather than directly on the hardware.[5] The VMM operates in kernel mode, where as a guest OS executes in user mode. VMMs allow multiple operating systems to run concurrently on a single physical hardware system, at the same time, VMMs impose isolation among these systems or VMs, thus enhancing protection and security.

A VMM controls[6] how the guest operating system uses the hardware resources. The consequences occurring in one VM do not affect any other VM running under the same VMM. At the same time, the VMM enables:

•sharing of single platform by multiple services.
•The shift of a virtual server or VMs from one platform to another, the so-called live migration.
• Modification of the system by maintaining backward compatibility with the original system.

Virtual machines: A virtual machine (VM*)* is an isolated environment that appears to be a whole computer but actually only has access to a portion of the computer resources. Each VM appears to be running on the bare hardware, giving the appearance of multiple instances of the same computer, though all are supported by a single physical system. There are three classes of virtual machines namely traditional, hybrid and hosted VM .

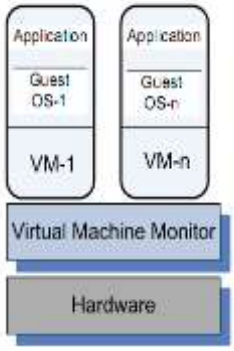

Fig (a)

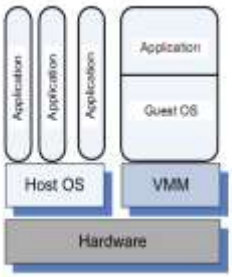

Fig (b)

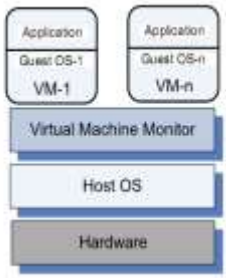

Fig (c)

[1] Traditional.VM also known as a"bare metal" VMM. A thin software layer called hypervisor that executes directly on the Host machine hardware; its main advantage is performance [see Figure (a)]. Examples: VMWare ESX, ESXi Servers, Xen, OS370, and Denali.
[2] Hybrid. The VMM shares the host machine hardware with the existing OS [see Figure (b)].Example: VMWare Workstation.
[3] Hosted. The VM runs on top of an existing OS and OS executes on top of host physical hardware [see Figure (c)].The main advantage of this Approach is that the VM is easier to build and install

ISSN: 2277-9655
Impact Factor: 3.785

PERFORMANCE AND SECURITY ISOLATION

In any shared computing environment performance isolation is a vital condition for quality-of-service guarantees. Indeed it becomes very difficult to predict the closing or completion time when the run time conduct of an applications is impacted by other application executing at the same time, and thus, is competing for CPU cycles, disk, main memory, cache and network access. Moreover the optimization[7] of the application also becomes evenly difficult. To some extent certain level of performance isolation is supported by various operating systems, like Linux/RK, SILK, QLinux etc. but the problem still persists as one has to account for all system resources used and to circulate the overhead for different system activities, including paging and context switching, often called as QoS crosstalk problem for individual users.

In multi-core systems the processor virtualization presents multiple copies of the same processor or core. The code[8] gets executed straight away by the hardware, whereas processor emulation exhibits a framework of another Hardware system in which instructions are "emulated" in software more slowly than virtualization. For instance Microsoft's Virtual-PC, which could execute on chipsets other than the x86 family. It was used on Mac hardware until Apple adopted Intel chips.

The conventional operating system multiplex multiple threads or processes, where as a VMM enabled virtualization multiplexes entire operating systems. As a result of this there exists certain level of performance penalty because OS is considerably more heavy weight than a process and the overhead of context switching is larger.

A hypervisor runs directly on the hardware a subset of frequently used machine instructions generated by the application and emulates privileged instructions, including device I/O requests. The various instructions that are executed directly by the the hardware includes branching instructions, arithmetic instructions and memory access.

The process abstraction used by operating system is not only used for resource sharing but also to support isolation..Unfortunately, this is not enough from a security perspective. It becomes very easy for an attacker to penetrate the entire system once a process is compromised. On the other hand, the software running on a virtual machine has the constraints of its own dedicated hardware; only virtual device emulated by the software can be accessed by it. This layer of software [10]has the potential to provide a level of isolation nearly equivalent to the isolation presented by two different physical systems. Thus, the virtualization can be Used to improve security in a cloud computing environment.

A VMM is a Less complicated and best defined system than a conventional operating system. For example, the Xen VMM has approximately 65,000 lines of code, whereas the Denali hypervisor has only about half that, or 30,000 lines of code. As very less privileged instructions are exposed the security vulnerability of hypervisor is substantially reduced. For example, the Xen VMM can be accessed through 26 hypercalls, where as a standard Linux allows hundreds(e.g., Linux 2.6.11 allows 289 system calls). In addition[8] to a richness of system calls, a conventional operating system supports peculiar devices(e.g., /dev/kmem) and many privileged programs from a third party(e.g., sendmail and sshd).

CONCLUSION

Virtualization layer of software has the potential to provide a level of isolation nearly equivalent to the isolation presented by two different physical systems. Thus, the virtualization can be Used to improve security in a cloud computing environment, which is essentially extremely useful for utility computing based on pay as u go model.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. H. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," University of California, Berkeley, Tech. Rep. UCB-EECS-2009-28, Feb 2009.
[2] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. Above the clouds: A berkeley view of cloud computing, Feb 2009.

[3] Ms. Shikha Joshi,Ms. Pallavi Jain," Study and Analysis of Data Sharing and Communication with Multiple Cloud Environments", International Journal of Advanced Computer Research (IJACR) .Volume-2 Number-4 Issue-6 December-2012.
[4] Jay Singh, Brajesh Kumar, Asha Khatri," Securing Storage Data in Cloud Using RC5 Algorithm", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4 Issue-6 December-2012.
[5] Mr. Sanjay Kumar Brahman, Prof. Brijesh Patel," Java Based Resource Sharing with Secure Transaction in User Cloud Environment", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-3 Issue-5 September-2012.
[6] Vineet Guha, Manish Shrivastava," Review of Information Authentication in Mobile Cloud over SaaS & PaaS Layers", International Journal of Advanced Computer Research (IJACR), Volume-3 Number-1 Issue-9 March-2013.
[7] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava," Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment", CONSEG-2012.
[8] Mr. Ajey Singh,Dr. Maneesh Shrivastava, "Overview of Security issues in Cloud Computing", International Journal of Advanced Computer Research (IJACR) Volume 2,Number 1,March 2012.
[9] Igor Ruiz-Agundez, Yoseba K. Penya and Pablo G. Bringas, "Cloud Computing Services Accounting", International Journal of Advanced Computer Research (IJACR) ,Volume 2, Number 2, June 2012.
[10] Amish Kumar Amanand Vijay Prakash," Implement Security using smart card on Cloud", International Journal of Advanced Computer Research (IJACR),Volume-3 Number-1 Issue-9 March-2013.
[11] P. Mell, T. Grance, ―The NIST Definition of Cloud Computing‖, National Institute of Standards and Technology, Information Technology Laboratory, Technical Report Version 15, 2009.
[12] FangHao,T.V.Lakshman,SaritMukherjee,HaoyuSong Secure Cloud Computing with a Virtualized Network Infrastructure.