International Journal of Engineering & Technology, 7 (2.33) (2018) 678-682

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Implementation levels of virtualization and security issues in cloud computing

A. Banushri [1] *, Dr. R. A. Karthika [1]

[1] Department of Computer Science & Engineering, Vels Institute of Science, Technology and Advanced Studies(VISTAS), Chennai
**Corresponding author E-mail: banushrics.scs@velsuniv.ac.in*

Abstract

Cloud is the buzz word in the industry. The initiation of virtualization technology in the infrastructure domain gives us the options to procure the benefits of the cloud deployments. Virtualization is a fast-growing infrastructure in the IT industry. Technology providers and user communities have introduced a new set of terms to describe the technologies and their features for virtualization. Virtualization characterizes the logical vision of data representation. The authority to compute in virtualized environment, storing the data at dissimilar geographies and diverse computing resources. Virtualization technology allows the creation of the virtual versions of hardware, networking resources, Operating systems and storage devices. It supports multiple OS run on single physical machine called host machine and multiple guest application run on single server called host server. Hypervisors assistance in virtualization of hardware. That is, the software interrelates with the physical system, providing virtualized environment to maintain multiple operating system running parallel using one physical server. This paper provides the information about the implementation levels of virtualization, the benefits and security problems of Virtualization in virtualized hardware environment.

Keywords: *Virtualization; Cloud Computing; Architecture; Security; Hypervisor.*

1. Introduction

Virtualization technology separates theprimary functions of computer, that is, computing and technology implementation, from the physical infrastructure and the hardware resources with the help of technology called virtual machine monitor (VMM). Virtualization changes the way, businesses make their outlays for using certain services, while risks associated with costs and payments for business are also well handled by it. It helps organizations save by removing the physical infrastructure to a huge extent, taking care of capital costs that need to be invested in availing and maintaining the infrastructure[6]. Moreover, other costs, such as maintenance and support, are adjusted into on-demand service based payments. Thus, it cuts much of the cost for businesses. The cloud providers use the virtualization technology, for computing resources through the network infrastructures, mainly the internet andmultiple virtual machines that are presented on the same physical server. Based on virtualization, the cloud computing model permits workloads to be systematized and provided quickly through the fast provisioning of virtual machine. A cloud computing platform supports greatly scalable programming forms that allow workloads to recover from necessary hardware or software failures. Customers do not pay for resources such as storage or infrastructure, but they only pay for what they use [7]. A virtual utilization discharges some of the distinguished management issues because; most of the software updates, maintenance, configuration and other management tasks are automated and integrated at the data center by the cloud provider. Virtualization techniques also experiences security issues for the network such as cloud [8].

2. components for virtualization

In cloud computing, Virtualization is one of most important features. Virtualization is a technology that helps IT societies to increase their application presentation in a cost-effective manner. However, it can also present application delivery challenges that make some security difficulties. The Latest interest in virtualization orbits around virtual servers because virtualizing servers can result in substantial cost savings. The virtual machine refers to a software computer that runs an operating system and applications, like a physical computer. An OS on virtual machine is called as guest operating system. There is a management layer called as virtual machine monitor manager (VMM) that directs and creates all virtual machines in virtual environment [9].

A hypervisor is one of various virtualization techniques that allow multiple operating systems, called guests, to run instantaneously on a host computer and this feature is called hardware virtualization. It is so called because it is theoretically one level higher than a supervisor is. The hypervisor presents a virtual operating platform, to the guest operating systems, and monitors the performance of the guest OS. Multiple occurrences of a variety of operating Systems can share the virtualized hardware resources. Hypervisor is mounted on server hardware whose job is to run guest operating systems [3].

A typical virtualization structure is shown in figure.1 where APP is the Application and VM is the Virtual Machine. The technology of virtualization separates the primary functions of the computers. That is the computing and the technology implementation from physical infrastructure and hardware resources, with the help of Virtual Machine Monitor. It helps the organizations to save the capital cost that is needed for investing and maintaining infrastruc-

Copyright © 2018 A. Banushri, Dr. R. A. Karthika. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

ture, by removing physical infrastructure to a greater extent. Moreover, the other costs such as support and maintenance are adjusted by on-demand service based payment [5].

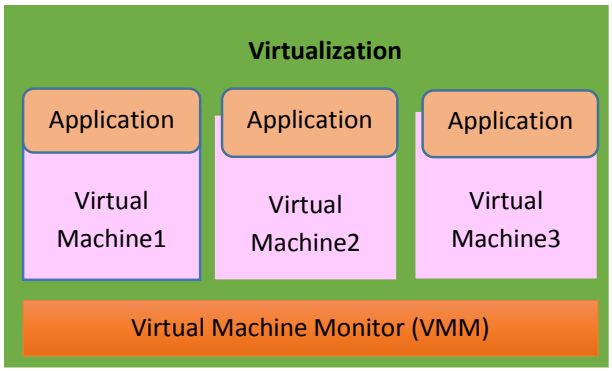


Fig. 1: Virtualization Structure.

3. Implementation levels of virtualization

Virtualization is implemented at different levels by resembling specific structures into analogous software that appears to work as the same way as physical structure. The levels upon which virtualization is implemented is shown in figure 2[15].

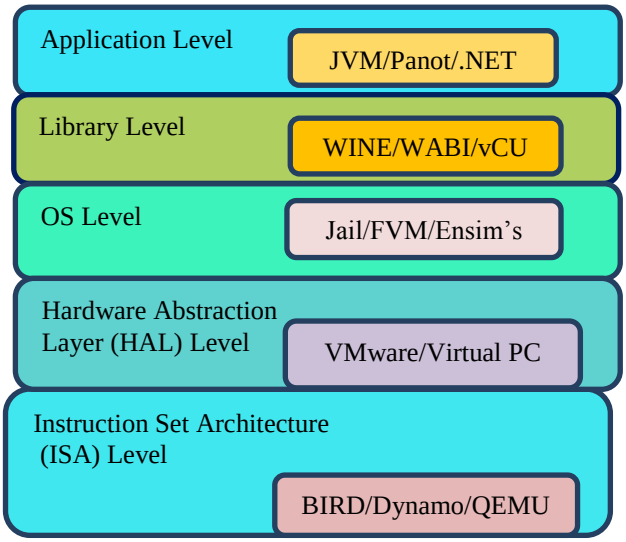


Fig. 2: Implementation Levels of Virtualization.

3.1. Virtualization at ISA (instruction set architecture) level

Virtualization is implemented at ISA (Instruction Set Architecture) level by transforming physical architecture of system's instruction set into software completely. The host machine is a physical platform containing various components, such as process, memory, Input/output (I/O) devices, and buses. The VMM installs the guest systems on this machine. The emulator gets the instructions from the guest systems to process and execute. The emulator transforms those instructions into native instruction set, which are run on host machine's hardware. The instructions include both the I/O-specific ones and the processor-oriented instructions. For an emulator to be efficacious, it has to imitate all tasks that a real computer could perform.

- Advantages:

It is a simple and strong method of conversion into virtual architecture. On a single physical structure, this architecture makes simple to implement multiple systems on single physical structure. The instructions given by the guest system is translated into instructions of the host system .This architecture makes the host system to adjust to the changes in architecture of the guest system. The binding between the guest system and the host is not rigid, but making it very flexible. The infrastructure of this kind could be used for creating virtual machines on platform, for example: X86 on any platform such as Sparc, X86, Alpha, etc.

- Disadvantage:

The instructions should be interpreted before being executed. And therefore the system with ISA level of virtualization shows poor performance.

3.2. Virtualization at HAL (hardware abstraction layer) level

The virtualization at the HAL (Hardware Abstraction Layer) is the most common technique, which is used in computers on x86 platforms that increases the efficiency of virtual machine to handle various tasks. This architecture becomes economical and relatively for practical use. In case, if emulator communication is required to the critical processes, the simulator undertakes the tasks and it performs the appropriate multiplexing. The working of virtualization technique wants catching the execution of privileged instructions by virtual machine, which passes these instructions to VMM to be handled properly. This is necessary because of the possible existence of multiple virtual machines, each having its own OS that could issue separate privileged instructions. Execution of privileged instructions needed complete attention of CPU.If, this is not managed properly by VMM, and it will raise an exception, which will result in system crash. Trapping and forwarding the instructions to VMM, helps in managing the system suitably, and thereby avoiding different risks. We cannot fully virtualize all platforms, with the help of this technique. Even in X86 platform, it is detected that some privileged instructions fail without being trapped, because their execution is not privileged appropriately. Such occurrences need some workaround in virtualization technique, to pass the control of such execution of fault instructions to the VMM, which would handle them properly. Code Scanning and dynamic instruction rewriting are some of examples of the techniques to enable VMM to have control of execution of fault privileged instructions.

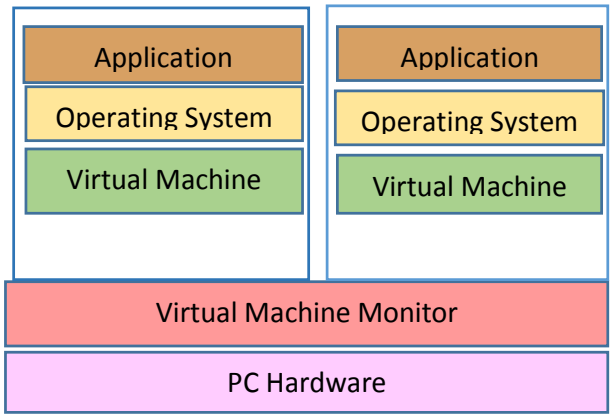


Fig. 3: Virtualization at HAL.

3.3. Virtualization at OS (operating system) level

To overcome redundancy and time consumption issues, virtualization at the operating system level is implemented. This kind of technique includes the sharing of both the OS and hardware. The physical machine is being separated from logical structure (virtual system) by separate virtualization layer, which could be compared with VMMs in functions. This layer is built on the top of the OS, which could enable the user to access to multiple machines, which is isolated from others and is running independently. The virtualization technique at the OS level, keeps the environment for running of applications properly.IT keeps the OS, the user-libraries, application-specific data structures separately. Thus, the application is not able to differentiate between the virtual environment (VE) and the real. The main idea behind OS level virtualization implementation is that the virtual environment rests indistinguish-

able from the real one. The virtualization layer imitates the operating environment, which is recognized on the physical machine, in order to provide a Virtual environment for application, thus by making partitions of each virtual system, whenever needed. An orderly managed partitioning and multiplexing permits to disseminate complete operating environments, which are separated from physical machine.

3.4. Virtualization at library level

Programming the applications in more systems needs a widespread list of Application Program Interfaces (APIs) to be disseminated by implementing several libraries at user level. These APIs are used to save users from miniature details involved with programming related to the OS and facilitate the programmers to write programs more easily. At the user level library operation, a different virtual environment is provided, in that kind of perception. This virtual environment is created above the OS layer, which could expose a different class of binary interfaces together. This type of virtualization is well-defined as an implementation of various set of ABIs (Application Binary Interfaces). The APIs are being implemented with the help of the base system and execute the function of ABI/API emulation.

3.5. Virtualization at application level

The user level programs and the operating systems are executed on applications, which behave like real machines. The memory mapped I/O processing technique or I/O mapped input/output processing is used to deal with hardware .Thus, an application might be taken simply as a block of instructions, which are being executed on a machine. The Java Virtual Machine (JVM) carried a new aspect to virtualization and it is known as application level virtualization. The main concept after this type of virtualization is to produce a virtual machine that works distinctly at the application level and functions in a way similar as a normal machine. We can run our applications on those virtual machines as if we are running our applications on physical machines. This type faces a little threat to the security of the system. However, these machines should have an operating environment delivered to the applications in the form of a separate environment or in the form of a hosted OS of their own.

4. A comparison between implementation levels of virtualization

Various implementation levels of virtualization have their own set of merits and demerits. For example, ISA level virtualization gives high flexibility for the applications but the performance is very poor. Likewise, the other levels such as HAL-level, OS-level, Library and Application Level also have both negatives and positives. The OS-level and the HAL-level virtualizations are the best on performance, but the implementations are complex and the applications flexibility is also not very good. The Application level implementation provides larger application isolation feature, but low flexibility, poor performance and high implementation complexity makes it less desirable. Library level virtualizations have medium performance, medium complexity, but poor isolation feature and low flexibility

Table 1: Comparison of Implementation Levels of Virtualization

Implementation Level	Performance	Implementation Complexity	Application flexibility	Application Isolation
ISA	Very poor	Medium	Excellent	Medium
HAL	Excellent	High	Medium	Very Good
OS Level	Excellent	Medium	Low	Very Poor
Application Level	Medium	Low	Low	Very Poor
Library Level	Poor	High	Low	Excellent

5. Requirements for virtualization design

The design of virtual systems becomes indistinct with OSs, which have functionalities comparable to virtual systems.So we need to have definite dissimilarities in the design of virtualized systems. The virtualized design requirements are generally viewed as follows:

5.1. Equivalence requirement

A machine which is developed through virtualization should have a logical equivalence with real machines. The emulator should match the capabilities of physical system in terms of computational performance. The emulator system should be able to execute all applications and the programs are designed to execute on real machines with certain exception of timing.

5.2. Resource control requirement

A computer is a combination of resources such as memory, processors and I/O devices. These resources must be controlled and managed effectively by VMM. The VMM must enforce isolation between virtualized systems. The virtual machines should not face any interference.

5.3. Efficiency requirement

The virtual machines must be efficient in performance as the real system. Virtualization is done with the purpose to get proficient software without physical hardware. Thus, the emulator should be capable of interpreting all the instructions that might be interpreted safely in a physical system.

6. Reliability, security and privacy issues in virtualization

There are reliability associated problems in virtualization, distant from security that can have an effect on the performance of the cloud. For example, too many virtual machines are combined onto a physical server by the providers. Performance problems can be caused by the impact factors like I/O bottlenecks or CPU cycles. These problems caused in a traditional physical server. These problems are to be expected to occur in virtualized server because of single physical server linked to multiple virtual machines so that they all battle for critical resources. Capacity planning management and performance management are vital in virtualized environment than Physical [13].This means, IT organizations must constantly observe the utilization of virtual machines and physical servers in real time. This capability makes IT organizations to avoid under-utilization and over-utilization of server resources such as memory and CPU and also allocate and reallocate resources, which is based on business requirement changes. The main challenge in virtualization is to manage the virtual machine sprawl. In virtualized environment, with VM Sprawl, the number of virtual machines running increases that are not needed for the business [4].The VM sprawl increases the overuse of infrastructure. To prevent this, VM managers have to analyze the new Virtual machines cautiously and ensure that unnecessary Virtual machines travel to other physical servers. However, it can be interesting to ensure that the travelled Virtual Machine keeps the same QoS configurations, security and needed privacy policies. It must be guaranteed that the destination maintains all the essential configurations of migrated VMs There will be two changes for the customer's data when it is stored in the cloud. First, the data would be stored away from customer's local machine and secondly, the data would be moved to a multi-tenant environment from a single-tenant. These alterations could hoist a significant concept called data leakage.DLP is the data leakage prevention to defend sensitive data. It is used to detect the unauthorized Recovery of

data [14].DLP products does not address integrity of data or availability of data but DLP is efficacy only in confidentiality. All encryption techniques depend on secure and remarkable key management constructions in cloud [1]. Several users might use their encryption methods and key management, which is another concern to address the encrypted data. In cloud-based services, the user data is stored on the third party's storage location. A service provider should implement security measures adequately to ensure data privacy. Data encryption is the main solution to guarantee the privacy of data against malicious attacks in the databases. Therefore, encryption methods have momentous routine inferences in cloud [2].

7. Security of virtual machines

Virtualization contains several security issues and vulnerabilities which are unique to cloud. There are mainly two levels of virtualization, the hypervisor and the Virtual Machines. Virtualization comprises several security issues that now drifted to cloud technology. There are other exposures and security disputes which are unique to cloud environment or might have a more acute role in cloud [12].

7.1. Hypervisor security

There are several Virtual Machines that can have autonomous security zones which are not accessed by other virtual machines, which have their own zones. A hypervisor has its own security zone and within the virtualization host, it acts as a controlling agent. Within the same physical infrastructure, there are multiple security zones. Another major virtualization security apprehension is, evading the Virtual Machine or capability to reach hypervisor within VM level. As more Application Program Interfaces are created, that controls and disables the functionality in a Virtual Machine, which can lessen availability and performance [11].

7.1.1. Benefits of hypervisor-based system

The hypervisor, not only manages resources, but has the capability to secure the infrastructure of cloud. Hypervisor-based virtualization ability is the finest choices of applying techniques to achieve a protected cloud environment.Some of the reasons for selecting this technology are:

i) The Hypervisor controls the hardware. Hypervisor operates as a firewall and able to avert malicious users.
ii) In the cloud computing hierarchy, below the guest OS, the Hypervisor is implemented, which detects if any attack passes the security systems of guest OS.
iii) It is used as a layer of notion to segregate the virtual environment from hardware beneath.
iv) It controls all access between the shared hardware and the guest's OSs.So it is able to simplify transaction monitoring process.

7.1.2. Weakness of hypervisor-based systems

There are a few weaknesses that could affect performance of executed methods.

1) Since there is only one hypervisor, and if it collapses due to excess load or due to booming attack, all the VMs and all the systems will be exaggerated.
2) It has vulnerabilities to attacks, such as buffer overflow.

7.1.3. Security management and hypervisor-based virtualization

A hypervisor is a supervision tool and the main objective of this region is to construct a trust region around the VMs and the hardware. In security management of hypervisor, there are three levels. The first level is the Authentication, where the users must validate their account .correctly, using the suitable mechanisms. The second level is Authorization where the user must have permission to do everything they wish [3]. The third level is the Networking where the network should be designed to ensure secure connections. Networking is the essential concern in the transaction involving the hypervisor and the user. But there is a great deal in virtualization security than in normal networking. If a cloud provider depends only on the network security, then the virtual environment will be at risk. If a cloud provider spends more money on developing a robust network and disregards communication involving the hypervisor and virtual machines, then it would be waste of money [10].

7.2. Intrusion detection system in VM

If an Intrusion Detection System (IDS) is present in the hypervisor, it will be capable of detecting the attacks better than the IDS running on the guest OS. The guest Operating System cannot observe actions in cloud; it can monitor actions only within its VM. The HIDS (hypervisor IDS) has more performance than the NIDS (Network IDS). It looks NIDS might be finest solution for cloud environment, but using NIDS has severe troubles. The most important problem, when using NIDS for observing is the encrypted data [8]. Providing safe and consistent service assertion is quiet important. Various Network-based intrusion detection systems (NIDS) are used to get the packets from the cloud. It has higher false positive rate, lower detection rate and is not capable to resist the single point attack failure. Several intrusion detection systems (IDSs) are organized in each layer of cloud infrastructure for guarding each Virtual Machine (VM) against threats. It is necessary to deploy IDS sensor to monitor, separated VM at all layer that is organized by the VM management unit.

8. Conclusion

Virtualization is a technology which could emulate the computing resources, storage facility and networking systems in the most efficient manner. It permits cost-effective utilization of maximum resources. Virtualization is implemented at five levels. They are ISA (Instruction Set Architecture) level, HAL (Hardware Abstraction Layer) level, OS (Operating System) level, library level and application level. Cloud providers will face numerous fluctuations when their cloud becomes bigger. Decentralize applications and allowing universal access would create challenges and security problems and it should be considered before transfer of data to the cloud. So the cloud computing requires several dynamic factors and the most significant of them is security. Virtualization requires efficient, controllable emulated system as well as physical system.Xen architecture is a special hypervisor that allows hosting multiple guest machines on single storage virtual host system for efficient virtualization. Multicore processors provide efficient virtualization if they are managed well by keeping the processors free at required times, using the CPU allocation settings, and using processing of heavy loads without multi-threading.

References

[1] Ahmed Albugmi, Madini o.Alassafi, Robert Walters, Gary Wills "Data security in cloud computing" IEEE, Future Generation Communication Technologies (FGCT), October 2016.
[2] Yubin Xia, Yutao Liu, Haibing Guan, Yunji Chen, Tianshi Chen, Binyu Zang, and Haibo Chen"Secure Outsourcing of Virtual Appliance" IEEE TRANSACTIONS ON CLOUD COMPUTING, VOL. 5, NO. 3, JULY-SEPTEMBER 2017.
[3] Andrew R .Riddle, Soon M.Chung, "A Survey on the Security of Hypervisors in Cloud Computing", IEEE, ICDCSW, 2015, Pages: 100 – 104.
[4] Arpit Gupta, Vaishali chourey"Cloud computing: Security threats & control strategy using tri-mechanism"IEEE, ICCICCT, 2014.
[5] Chunxiao Li, Anand Raghunathan, Niraj K.Jha "A Trusted Virtual Machine in an Untrusted Management Environment", IEEE

Transactions on Services Computing (Volume: 5, Issue: 4, Pages: 472 - 483), 2012.

[6] T.Swathi, K.Srikanth, S. Raghunath Reddy, "VIRTUALIZATION IN CLOUD COMPUTING", IEEE, Internal Journal of Computer Science and Mobile Computing, IJCSMC, Vol.3, Issue.5 May 2014.

[7] Harshitha.K.Raj, "A Survey on Cloud Computing", International Journal of advanced Research in Computer Science and Software Engineering,Vol.4,Issue 7,July 2014.

[8] Lata Ingle, Ganesh K.Pakle, "A survey on IDS and counter-measure excerption approach for detecting VM exposures in cloud environment-based on AODV protocol", IEEE, ICICT, Vol.3, page1-5.

[9] D.Kiran Kumar, T.P.Sarachandrica, B.Rajasekhar, P.Jayasankar, "Review on Virtualization for Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 8, August 2014.

[10] Gabriel CephasObasuyi, Arif Sari, "Security Challenges of Virtualization Hypervisors in Virtualized Hardware Environment", Int. J. Communications, Network and System Sciences, 2015, 8, 260-273.

[11] Sonam Srivastava,S.P Singh, "A Survey On Virtualization and Hypervisor-based Technology in Cloud Computing Environment", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),Volume 5 ,Issue 2,February 2016.

[12] Prof. D. G. Vyawahare, Rohit B. Bende, Dheeraj N. Bhajipale, Ravindra D. Bharsakle , Amol G. Salve, "A Survey on Security Challenges and Solutions in Cloud Computing", International Journal of Innovative Research in Computer and Communication Engineering,Vol. 4, Issue 3,March 2016.

[13] Qiao Yan, F. Richard Yu, Senior Member, IEEE, Qingxiang Gong, and Jianqiang Li "Software-Defined Networking (SDN) and Distributed Denial of Service (DDoS) Attacks in Cloud Computing Environments: A Survey, Some Research Issues, and Challenges", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, and NO. 1, 2016.

[14] Preeti Sirohi, Amit Agarwal, "Cloud computing data storage security framework relating to data integrity, privacy and trust", International Conference on Next Generation Computing Technologies (NGCT), IEEE, January,2016.

[15] K C Gouda, Dines Dwivedi, Anurag Patro, Nagaraj Bhat, "Migration Management in Cloud Computing", International Journal of Engineering Trends and Technology (IJETT) – Volume 12 Issue 9- June 2014.