International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 7, July - 2014

Design and Implementation of Techniques for Secure Virtualization in Cloud Environment

Apurva R. Pisalkar
PG Scholar
St. Vincent Pallotti College of Engg & Tech, .
Nagpur, Maharashtra.

Prof. M. V. Bramhe
Associate professor
St. Vincent Pallotti College of Engg & Tech,
Nagpur, Maharashtra

Abstract--Virtualization is important feature of cloud computing. With virtualization efficiency of computing services can be increased. We can create virtual environment on any machine with any operating system. The virtual environment is vulnerable many different security attacks. In this paper we are focusing on cross vm side channel attack which is type of virtual machine attack.

In our system we have developed a security program called monitoring program. This monitoring program continuously monitors the virtual environment and reports the malicious activities done by any virtual machine. Thus using this monitoring program we can monitor the activities of all the virtual machines on our system and we can easily detect the malicious activities done by any virtual machine. Then depending on reports given by monitoring program the service provider can take action against the malicious virtual machine.

Keywords: VM, VMWare, monitoring program.

1. INTRODUCTION

Virtualization plays key role in cloud computing. In Virtualization virtual version of a device or resources, such as server, storage device, network or operating system can be created. Virtualization is a powerful technology to increase the efficiency of computing services provided to private and business users in terms of performance, maintenance, and cost.

In virtual environment more than one operating system can work simultaneously on same host machine. With virtualization resources can be utilized more efficiently, and users can decrease their expenditures on computing services significantly.

Virtualization is a technique for hiding the physical characteristics of computing resources from the way in which other systems, applications, or end users interact with those resources. This includes making a single physical resource, such as a server, an Operating system, an application, or storage device appear to function as multiple logical resources; or it can include making multiple physical resources, such as storage devices or servers appear as a single logical resource.

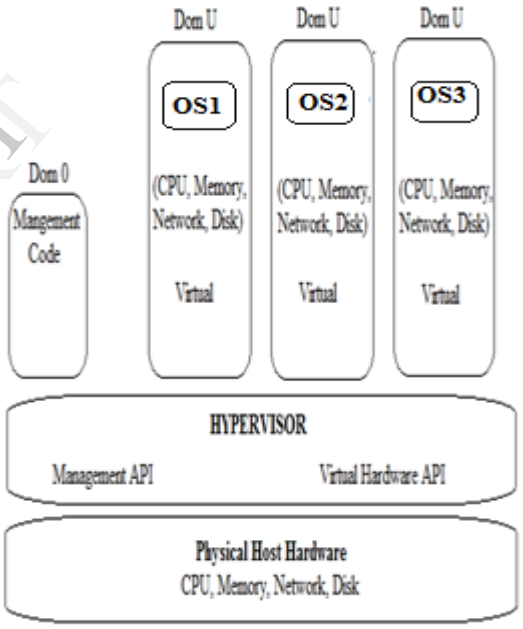

Fig: Block Diagram of Virtualization

1.1 Advantages of Virtualization:

Some advantages of virtualization are as follows:

1. Lower number of physical servers are required and because of this the hardware maintenance cost can be reduced because of lower number of physical servers.
2. By having each application within its own virtual server one application can be prevented from impacting other function when changes are made.
3. A standard virtual server can be developed that can be easily duplicated, which will speed up server deployment.
4. Multiple operating system technologies can be deployed on a single hardware platform.

1.2 Problems in Virtual Environment:

Use of virtualization in cloud environment has added number problems. These problems in virtual environment are as follows:

(a)Multi-tenancy: Multi-tenancy is an architecture in which a single instance of a software application serves multiple customers. Each customer is called a tenant. Tenants may be given the ability to modify some parts of the application, such as colour of the user interface, but they cannot modify application's code.

(b)Loss of control: The users of cloud are not aware of the location of their data and services and the cloud providers run VMs and they are not aware of their contents.

(c)Network topology: The architecture of cloud is very dynamic and the existing workload on cloud changes over time, because of creating and removing VMs. In addition, the mobile nature of the VMs that allows VMs to migrate from one server to another leads to non-predefined network topology.

(d)Single point of access: Virtualized servers have a limited number of access points available to all VMs. This represents a critical security vulnerability where compromising these access points compromise the VMs, hypervisor or the vSwitch.

2. CLOUD COMPUTING

According to definition given by NIST:

"Cloud 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." The cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

The primary types of cloud deployment models are as follows:

- Private Cloud
- Public Cloud
- Community cloud
- Hybrid Cloud

Some essential characteristics of cloud are:

- Broad network access
- Rapid elasticity
- Resource pooling
- measured services

Cloud computing have three types of service models:

- Cloud Software as a Service (SaaS)
- Cloud Platform as a Service (PaaS)
- Cloud Infrastructure as a Service (IaaS)

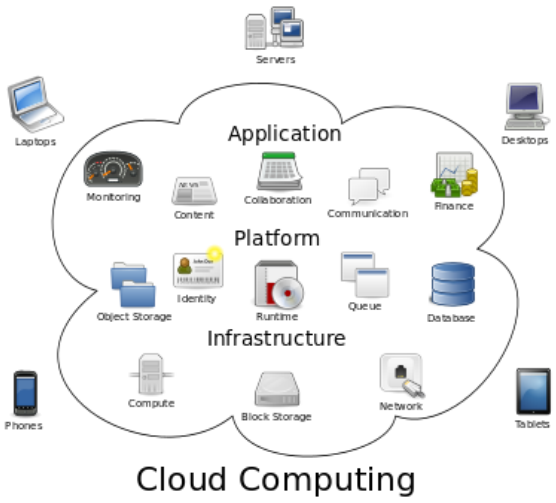

Fig: Basic Diagram of Cloud Environment

2.1 Security Attacks on Cloud Virtual

Infrastructure:

The virtual cloud infrastructure is vulnerable to various security attacks. Different security attacks on cloud virtual infrastructure can be categorised into following categories:

2.1.1 Hypervisor Attacks:

Hackers consider the hypervisor as target because of the greater control afforded by lower layers in the system. Compromising the hypervisor enables gaining control over the installed VMs, the physical system and hosted applications. These VM-Based Root kits are capable of inserting a malicious hypervisor on the fly or modifying the installed hypervisor to gain control over the host workload.

2.2 vSwitch Attack:

The vSwitch is vulnerable to a wide range of layer-2 attacks like a physical switch. These attacks include vSwitch configurations, VLANs and trust zones, and ARP tables.

2.3 Virtual Machine Attacks:

Cloud servers contain tens of VMs, these VMs may be active or offline, and in both states they are vulnerable to various attacks. Active VMs are vulnerable to all traditional attacks that can affect physical servers. Once a VM is compromised, this gives the VMs on the same physical server a possibility of being able to attack each other, because the VMs share the same hardware and software resources e.g. memory, device drivers, storage, hypervisor software. Collocation of multiple VMs in a single server and sharing the same resources increases the attack surface. When a VM becomes offline, it is still available as VM image files that are susceptible to malware infections and patching.

Some examples of virtual machine attacks are as follows:

2.3.1 Virtual Code Injection Attack:

In virtual code injection attack, malicious code is injected in program to change the course of execution of program. This type of attack exploits poor handling of untrusted data. These types of attacks are usually made possible due to a lack of proper input/output data validation, for example, allowed characters, data formats, amount of expected data etc.

2.3.2 VM Escape Attack:

Normally virtual machines are encapsulated. The operating systems running inside the virtual machine doesn't know that they are virtualized. These virtual machines cannot directly interact with the hypervisor. The process of breaking out and interacting with the hypervisor is called a "VM escape."

Since the hypervisor controls the execution of all of the virtual machines running on the host then the attacker that can gain access to the hypervisor can gain control over every other virtual machine running on the host.

2.3.3 Cross VM Side Channel Attack:

Cloud computing provides infrastructures which is a collection of multiple computers, virtual machines and other resources to its users to store their application, files, confidential information, documents and so on. By mapping the cloud infrastructure the target virtual machine is selected. New virtual machine is placed co-resident to the target virtual machine. After successful placement of instantiate virtual machine it can successfully extract the confidential information from the targeted virtual machine. This type of attack is called cross-vm attack. Side channel attack requires two main steps: Placement and Extraction. Placement refers to the attacker arranging to place their malicious VM on the same physical machine. Extraction: After successfully placement of the malicious VM to the targeted VM extract the confidential information, file and documents on the targeted VM.

3. PROPOSED SYSTEM

Virtual environment is vulnerable to many security attacks. In our system we are focusing on cross VM Side Channel Attack which takes place in between virtual machines which are created in our virtual environment. In our system we are trying to develop a security program called as monitoring program which will monitor activities of virtual machines from out of box and will detect the malicious activities of any virtual machine.

In our system we will have two physical machines. On one machine we will show virtual environment using VMware workstation. On this system we will create 3virtual machines. On all these three virtual machines we will install different operating systems (windowsXP, windows7, windows8).

One of these machines will be a normal user, one will be attacker and one will be a victim which will be attacked by attacker. All these 3 machines will be interconnected using Wamp server.

On other physical machine we will install the monitoring program. This program will continuously monitor all the virtual machines on other system. This program will be connected to the virtual machines through LAN/Internet.

As we mentioned that one of the three virtual machines will be attacker. This attacker virtual machine will read all the functions done by the victim machine. The attacker will passively monitor the victim. Now the monitoring program installed outside the cloud will be monitoring the activities of all the virtual machines and it will find the activity done by the attacker. When monitoring program find this activity of attacker it will inform the cloud provider about this activity and will block the attacker.

As per our planned work our proposed system will be as shown in following diagram:

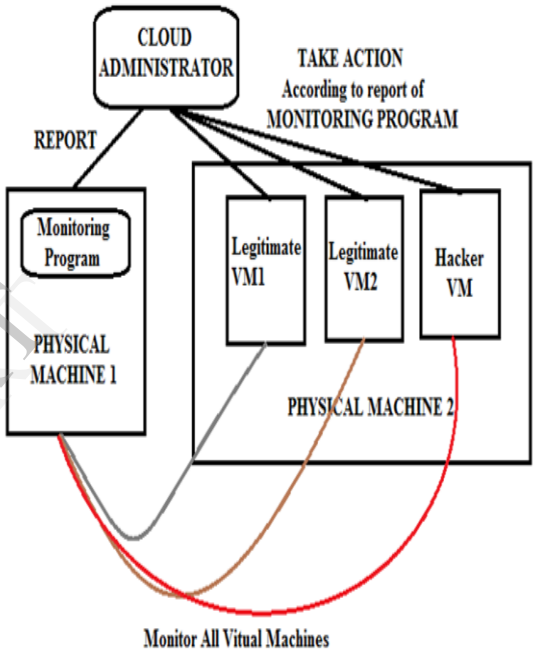

Fig: Proposed System

4. IMPLEMENTATION

Step by step implementation of our system is explained as below:

In our system we have installed VMware workstation 10 on our host computer. VMware workstation is used for creating virtual environment in our system.

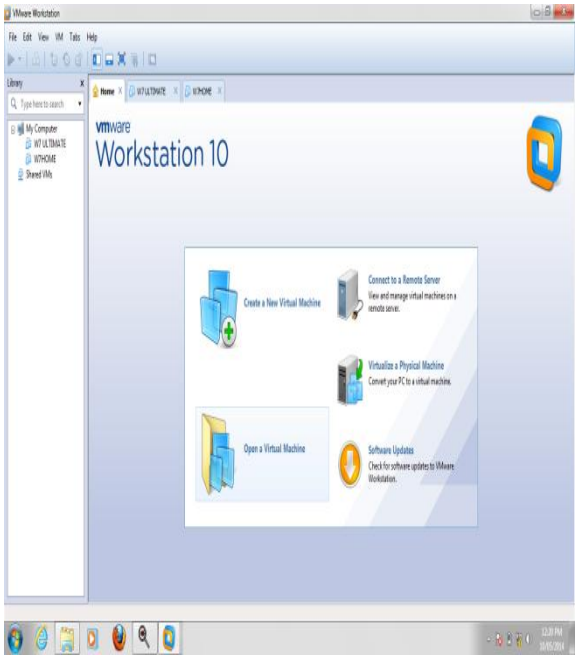

Fig: Screenshot of VMware workstation

After creating virtual environment using VMware we have created two virtual machines on our host machine. On one virtual machine we have installed Windows 7 Home and Windows 7 Ultimate on other virtual machine.

Fig: VM Created using VMWare

On the host computer and on both virtual machines we have installed WAMP server which is used for establishing communication between virtual machines and also host machine.

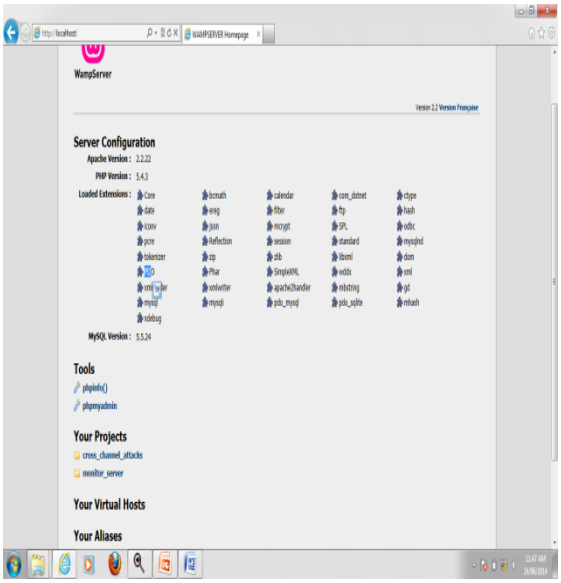

Fig: WAMP Server Home Page

On both the virtual machines we run download/upload program. This program uploads or downloads files on or from the virtual machines. With upload program we can upload any file from one virtual machine to other virtual machine. With download program we can download the uploaded file.

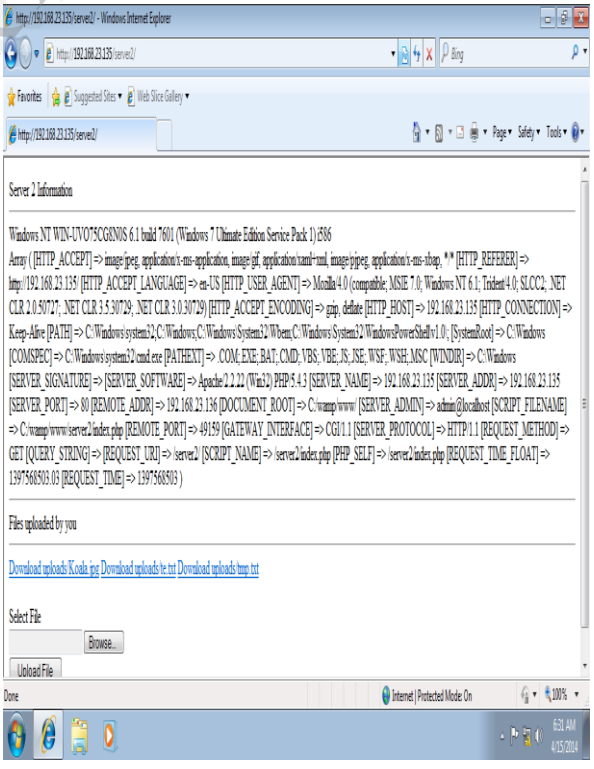

Fig: Upload/Download Program

With download/uploads program we have installed delete uploads program. With this program we can delete the uploaded files. When we delete the file then that event is reported.

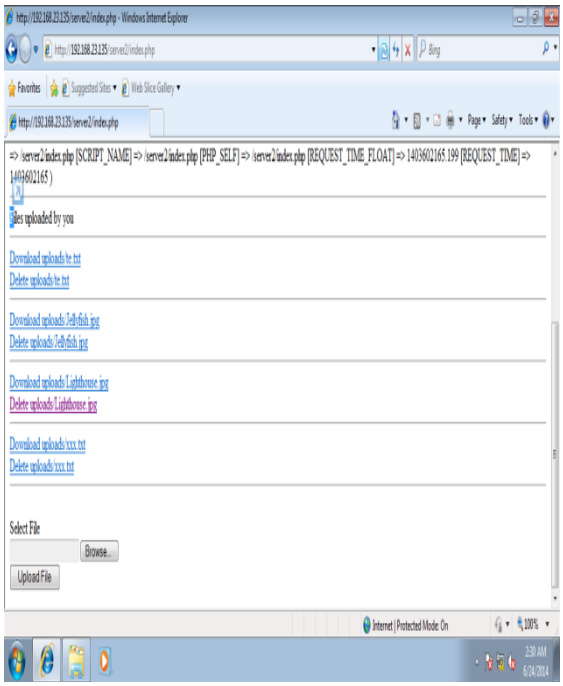

Fig: Delete Program

WAMP server provides MySql database. In this database the record of all the files uploaded on that machine is maintained.

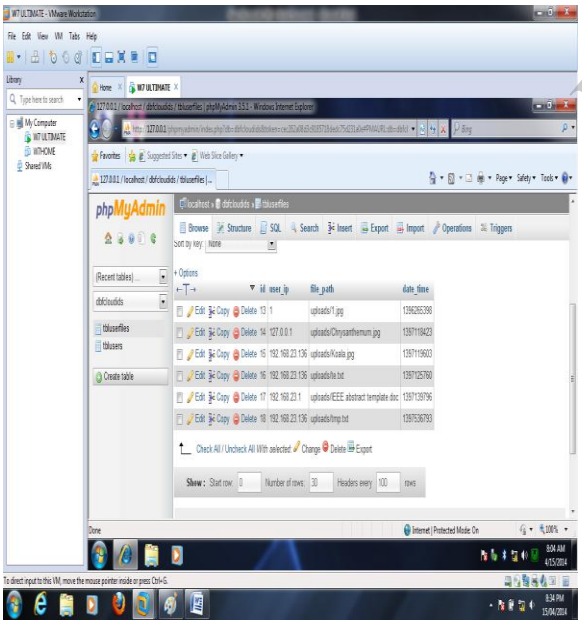

Fig: Database Created in WAMP Server

When we delete any file which is uploaded on virtual machine with upload program then that event is recorded by the monitoring program. The monitoring program is the program which we have installed on other computer and which continuously monitors the activities of the virtual machines which are installed on our host computer system. The monitoring program detects which virtual machine is doing the malicious activity of deleting data on other virtual machine.

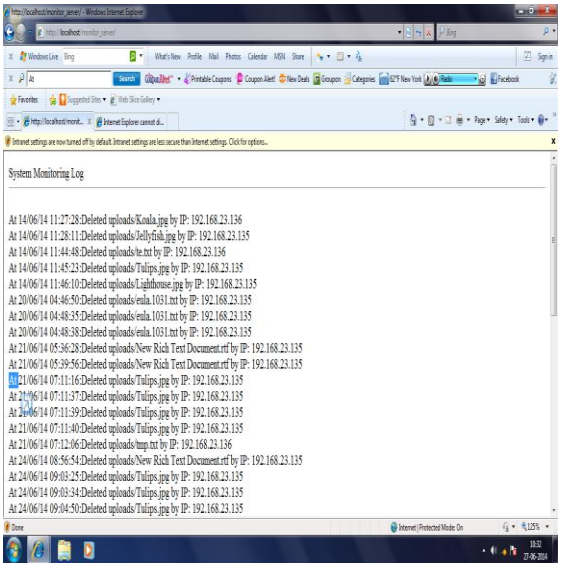

Fig: Result Given by Monitoring Program

CONCLUSION

In this paper we have explained what virtualization is, advantages of virtualization and types of possible security attacks in cloud environment. In our system we are focusing on cross vm side channel attack which is type of virtual machine attack. For providing security to system against cross vm attack either in the box approach or out of box approach is used. In our system we are using out of box approach. So we have created virtual environment in one system and installed security program another machine. Whenever any virtual machine does any malicious activity with other virtual machine then that activity is noticed by the monitoring program and it gives message which virtual machine has done the malicious activity. Thus with the monitoring program we can detect the malicious activities taking place in virtual environment. Thus we can provide security to our virtual environment.

FUTURE WORK

The system which we have explained in this paper is working with two virtual machines. We are trying to work with three virtual machines. In this system, with monitoring program we have linked only delete option. But further we can try to develop a program which access the data contained in host machine. When any virtual machine access data from the host machine this program can also be linked with the monitoring program. If
Link this program with monitoring program then we can notice the malicious activities done with host machine.

REFERENCES

[1] Lee Badger, Tim Grance, Robert Patt-Corne, Jeff Voas "DRAFT Cloud Computing Synopsis And Recommendations", Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-146 May 2011.

[2] Bhrugu Sevak "Security against Side Channel Attack in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012.

[3] Gabor Pek, Levente Buttyan, Boldisar Bencsa´ TH "A Survey of Security Issues in Hardware Virtualization" Accepted on ACM Computing Surveys, Vol. V, No. N, Article Y, Publication date: January 20XX.

[4] Amani S. Ibrahim, James Hamlyn and John Grundy "Emerging Security Challenges of Cloud Virtual Infrastructure**"** In Proceedings of APSEC 2010, Cloud Workshop, Sydney, Australia

[5] XUXIAN JIANG, XINYUAN WANG and DONGYAN XU "Stealthy Malware Detection and Monitoring through VMM-Based "Out-of-the-Box" Semantic View Reconstruction" ACM Transactions on Information and System Security,Vol. 13,No. 2, Article 12, Publication date: February 2010.

[6] Tyson T. Brooks, Carlos Caicedo, Joon S. Park "Security Vulnerability Analysis in Virtualized Computing Environments" International Journal of Intelligent Computing Research (IJICR), Volume 3, Issues 1/2, Mar/Jun 2012.

[7] Bryan D. Payne Martim Carbone Monirul Sharif Wenke Lee "Lares: An Architecture for Secure Active Monitoring Using Virtualization" IEEE 2008.

[8] Steve Mansfield-Devine "Danger in the clouds" Network Security December 2008.

[9] Kuai Xu, Feng Wang, Lin Gu "Profiling-as-a-Service in Multi-Tenant Cloud Computing Environments"

[10] M. Armbrust, A. Fox, Armando, R. Griffith, A. D. Joseph, R. Katz,Randy, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A view of cloud computing," Communications of the ACM,
vol. 53, no. 4, pp. 50–58, April 2010.

[11] S. S. L. Ertaul and G. Saldamli, "Security Challenges in Cloud Computing," in Proceedings of International Conference on Security and Management, July 2010.

[12] Y. Chen, V. Paxson, and R. Katz, "Whats New About Cloud Computing Security?" Technical Report No. UCB/EECS-2010-5, University ofCalifornia at Berkely, January 2010.

[13] Roland Schwarzkopf*, Matthias Schmidt, Christian Strack, Simon Martin and Bernd Freisleben "Increasing virtual machine security in cloud environments" Journal of Cloud Computing: Advances, Systems and Applications 2012.

[14] Jicheng Shi, Xiang Song, Haibo Chen, Binyu Zang "Limiting Cache-based Side-Channel in Multi-tenant Cloud using Dynamic Page Coloring" Dependable systems and networks workshop IEEE 41st Iternational Conference, 2011.

[15] Samuel T. King, George W. Dunlap, Peter M. Chen "Operating System Support for Virtual Machines" a white paper.

[16] Lamia Youseff, Maria Butrico, Dilma Da Silva "Toward a Unified Ontology of Cloud Computing"

[17] Hsin-Yi Tsai, Melanie Siebenhaar and André Miede, Yu-Lun Huang, Ralf Steinmetz "Threat as a service? Virtualization's impact on cloud security" IT Pro January/February 2012.