**Cross-VM Network Channel Attacks and Countermeasures within Cloud Computing Environments**

**ABSTRACT**

Cloud providers attempt to maintain the highest levels of isolation between Virtual Machines (VMs) and inter-user processes to keep co-located VMs and processes separate. This logical isolation creates an internal virtual network to separate VMs co-residing within a shared physical network. However, as co-residing VMs share their underlying VMM (Virtual Machine Monitor), virtual network, and hardware are susceptible to cross VM attacks. It is possible for a malicious VM to potentially access or control other VMs through network connections, shared memory, other shared resources, or by gaining the privilege level of its non-root machine. This research presents a two novel zero-day cross-VM network channel attacks. In the first attack, a malicious VM can redirect the network traffic of target VMs to a specific destination by impersonating the Virtual Network Interface Controller (VNIC). The malicious VM can extract the decrypted information from target VMs by using open source decryption tools such as Aircrack. The second contribution of this research is a privilege escalation attack in a cross VM cloud environment with Xen hypervisor. An adversary having limited privileges rights may execute Return-Oriented Programming (ROP), establish a connection with the root domain by exploiting the network channel, and acquiring the tool stack (root domain) which it is not authorized to access directly. Countermeasures against this attacks are also presented.

**EXISTING SYSTEM**

Cloud servers provides heavy computation resources and storage at cheaper cost so all users migrating their social and business data to 3rd party cloud servers. Data stored at cloud servers will be away from user control and can be misuse by cloud servers in various ways such as data tamper by internal employees or attackers who can hack VM (virtual machine) to divert traffic to different IP or send huge request to other VM to crash VM resources. In all this attack scenarios user data will be at risk.

**Disadvantages:**

1. Less Accuracy
2. More time taking process

**PROPOSED SYSTEM**

In proposed system, introducing Monitor Node which will monitor all VM’s and if any VM sending huge packet or diverting request to other VM then that monitor will detect and drop such attack request to save user data.

Following are the resources used by author to monitor VM

VM-Monitor/Controller: Responsible for executing the services of management software that are needed for functioning of cloud platform.

Compute: Compute nodes execute virtual machine instances in cloud. KVM is used as a hypervisor in this node. This node is also responsible for providing firewall services. One can deploy more than one compute node in a setup.

Network: The responsibilities of network nodes ensure the creation of virtual networks needed by the customers to create public or private networks. It connects their virtual machines with the external networks, i.e. the Internet.

**Advantages:**

1. High Accuracy
2. Takes less time

**SYSTEM REQUIREMENTS:**

**Hardware Requirments:**

* processor :   intel i3(min)
* Hard Disk  :   40 GB.
* Floppy Drive :   1.44 Mb.

**Software Requirments:**

* Operating system : Windows 10 (min)
* Coding Language  : python 3.7.0