Secure Live VM Migration model for Virtualized Cloud environment

S Ramamoorthy[1], S Rajalakshmi[2]

[1]Assistant professor, Department of Computer Science & Engineering, SCSVMV University, Tamilnadu, India
[2]Professor, Department of Computer Science & Engineering, SCSVMV University, Tamilnadu, India.

---***---

Abstract - *Cloud Virtual Infrastructure management is the emerging technology in the IT industry today. Most of the IT business process demanding on the virtual infrastructure as a service from the cloud service providers including compute, network and storage etc., The dynamic adoption of computing resource and elimination of major investment cost to setup the physical infrastructure attracted the IT industry towards cloud infrastructure. Live VM Migration techniques allows more frequently move the virtual machines from one physical location to another to avoid the situations like load balancing, Fault tolerance, edge computing, virtual migration etc., The major challenge which found on this process security issues on the VM live migration. The proposed model trying to eliminate the security challenges in the pre-copy migration strategy by introducing the network addressing level hashing technique to avoid the critical part of migration process. The dirty VM memory pages are released to the destination server only after the authenticated network process.*

Key Words: **Cloud computing, VM Live Migration, Hashing, Pre-Copy, Memory pages, Network Addressing.**

1.INTRODUCTION TO CLOUD COMPUTING

Cloud Computing Data Center model will provide the facility to operate the IT business services by offering its infrastructure like Compute, Storage, Network etc., Number of physical Servers are massively utilized to perform many number of applications with the hypervisor support on the physical Environment. Every Hypervisor creates multiple number of Virtual machines to perform the host level operations. Virtual Machines are nothing but the set of files which will inherit the abstract behavior of the physical machine. There are number of Virtual machine migration operations performed on the same cloud environment for continuity of uninterrupted Service offered by the cloud to its customers.

Cloud Computing is a Internet based Technology offers computing resources as a services to its end users support various IT business process. The computing resources are physical infrastructure as a service including compute ,network and storage etc., The Cloud computing services are offered to the customers in the different models like Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

Cloud Deployment models selected by the customers based on their specific business needs. If the customer is more concern about the data and less concern about the cost they opted to go for the private cloud model in the home location. If the customer is less concern about the data security but more concern about the hiring cost then they will go for an public cloud model for their organization.

1.1 Virtual Infrastructure

The third model will provide the intermediate level facility to the customers by offering hybrid infrastructure for their business process.

Virtual Infrastructure is the backbone of the cloud computing business model, this will eliminate the need for setting up the physical infrastructure by customers. Instead of these customers can hire the computing resources as pay as you go model structure.

Virtual machine Manager (Hypervisor) abstract the physical infrastructure to the Virtual Machines running on the Hypervisor. This model allows the Multiple VM's to run multiple guest operation system on the same physical server. Many application's can be deployed using this flexibility of the physical infrastructure. Automated Live VM migration is the one of the technique which is frequently handled by the hypervisor to move the Virtual machine into different physical servers depends on the requirement of the resource availability.

1.2 VM Level Attacks:

VM level attacks like monitoring and capturing the traffic between the virtual network will lead to the different level of issues on the Co located VMs. VM level challenges like Multitenancy, Co-located VM attack must be Addressed in a Effective way in order to reduce the risk associated with infrastructure level threats in the cloud environment. As an example Cloud Platform like Amazon EC2 , Microsoft Azure running multiple number of VMs on the same Environment can lead multiple number of Security issues at the host level. Predominant usage of internet services in the process of Connection establishment between Cloud data center and the Client machine will reflect the untrusted channel communication in public cloud environment. Untrusted Network operations, Untrusted Port group, protocols and interconnecting devices will require maximum attention while setting up the Cloud Environment for running multiple number of VM on the same physical Machine.

Remote Level machine authentication is also part of this data center activity which needs to prove itself as a authorized user to access the Virtual Machine created on the cloud Environment.

2 Characteristics of VM Operations:-

Virtual machine is the set of files which inherit the abstract concept from the physical machine and creates the Virtual environment as a mirror image of physical machine. Hypervisor is the software layer which allows the multiple number of OS's run simultaneously by sharing the common resource among themselves from the underlying physical machine.

There are two types of Hypervisor namely a)Bare metal Hypervisor b) Hosted Hypervisor that is a software layer which allows the VM level interaction between physical hardware and Virtual Machine created on the same hypervisor.

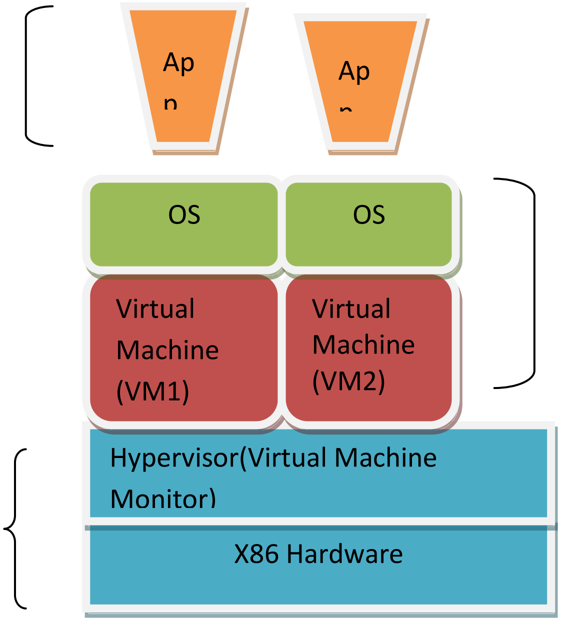

Fig -1: Hosted Hypervisor

From the above diagram it is clear that various level of security enforcement are required on the cloud Infrastructure at Infrastructure level (IaaS), Platform level (PaaS) and Application level (SaaS).

3 Live VM Migration Process:-

Live VM Migration is the process of migrating the VM from one physical server to another physical server to different location. VM contents like CPU state, Memory pages, VM configuration data etc., migrated to the destination server while VM still in running state.

Two types of Migration strategies are followed in the process of Live Migrations

1. Pre copy Migration
2. Post copy Migration

In the Pre copy migration process the Running VM contents are copied at a time and all the memory pages of the VM are migrated to destination host, this process was done without disturbing the running application.

In Stop and Copy migration process the currently running VM was stopped for the specific point of time in the source, in subsequent iteration the modified memory pages (Dirty pages) are copied to the destination server, after that VM will be resumed at the destination server.

4 Challenges Related to Co located VM's:

Primary threat for a Virtual machine is due to running multiple VMs on the Same Hypervisor. The attack surface will be very high among the VMs even the malicious VMs can also the part of this Surface. Efficient sharing of resources among the number of VMs will also lead to different issues on this environment. Live Migration of Failed VM from one hypervisor to another hypervisor will carry the sensitive information to the untrusted environment which could have the possibility to attack the target VM and extract the confidential information about the target.

The major challenge in the Live VM migration is the Security issues related to the VM content migration. Secure transfer of VM memory pages must be protected from the unauthorized modification. The VM's are still running state while transferred between different physical servers. There is a possibility of masquerade VM contents into another. Strong Cryptographic Techniques are need to be deployed to avoid this kind of memory modification but key management is the another overhead for this kind of security mechanism. The proposed model trying to eliminate this critical situation by introducing the network level Hashing technique to authenticate the memory page migrations. Types of Operations on Cloud Virtual Machine given as follows:

Table – 4.1 VM level Operations

S.No	Type of VM Operation	Function
1.	VMLive Migration	Moving the Live VM from one hypervisor to Another hypervisor
2.	VM Copy	Copy the Contents of VRAM disk into another
3.	VM Move	Movement of VM from one hypervisor to another physical server
4.	VM Clone	Performing Cloning operation to take multiple copies of VM
5.	VM Template	Taking the contents of VM in the form of Template to produce multiple copies

5. Proposed Methodology:

Proposed model try to achieve the required level of security by implementing following security polices at VM level.

- Self Destructive nature of VM when there is an unauthorized effect made on the VM.
- Authenticated move or Copy of VM operations at hypervisor level.
- For every VM operation required to prove itself as a authenticated operation on a VM.
- Identification of unauthorized move can be monitored based on the level of traffic flow between two VM's and Virtual Switch.
- If the traffic flow exceed the preset Limit then it will become concluded as a unauthorized move of VM and it will destroy by itself.

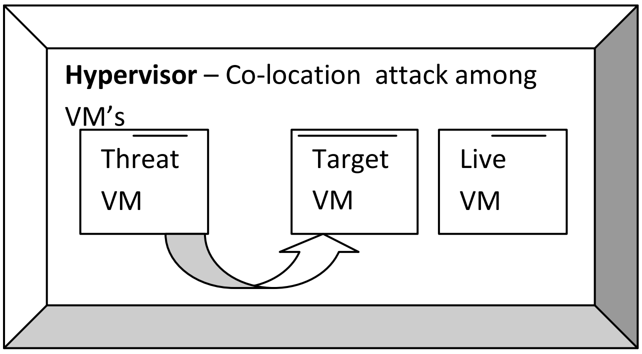

Fig-5.1 Co-Located VM surface Attack

Abnormal traffic rate identified between VM's are enforced to apply some set of security policy given below:

Behavior of VM **Security Policy Rule**

Traffic rate HIGH- Destroy the VM fail to provide Signature Identity

Traffic Rate=MEDIUM-Signature Identity Check

Traffic Rate= LOW – Continue its normal operation.

5.1. Vsignature – Authentication Process:-

Every clustered hypervisor's group generated some hash value signature when it was created as the part of cluster group for the Authentication purpose. This hash based signature used to identify the hypervisor while moving the Live VM's between one Hypervisor to another in the same cluster group.

This Signature Authentication will provide sufficient security to prevent the Virtual Machine hosted in a attackers hypervisor in unauthorized manner.

Every time the Virtual machine will update the new MAC Address by throwing back to its router where its previously hosted network. The Signature Verification module will now recomputed the hash value based on the MAC address which is thrown by the hypervisor.

6. Implementation & Result Analysis:-

The above work is simulated using Cloudsim by setting up the two different data center along with multiple number of Virtual machines running on the same hypervisor cloudlet. It is allowed to move a virtual machine from one hypervisor to another hypervisor and the data transfer rates are monitored at the VM and VSwitch level.

$$\text{Capacity of Cloudlet} = \sum_{i=0}^{n} C(i)/Nvm$$

By setting pre Limit condition to the data traffic rate between two VMs and Vswitch identifies the unauthorized behavior of the Virtual machine.

Mathematical Evaluation:

Tmr = Tc+ Tsd ------→ (1)

T service downtime = Tmr – Tcycles - (2)

Tsd > Est. Th value ----→ (3)

Concluded as a abnormal behaviour VM.

RTT / ICMP Packet: (Vswitch)

Total Data transfer = Total no. Of RTT peak@/CPU cycles +Data Transfer +Total down time

$$RTT \rightarrow \frac{\text{mean time between Time at first packet sent}}{\text{Time at response}}$$

Let the size of the virtual machine RAM is 'V' the peak rate at which packet's sent 'P' and the network bandwidth available be 'B'.

For an instance, Xen virtualization environment.

The Threshold limit, on the number of RTT peaks / CPU cycles limited to 5.

If RTT > Peaks > 5VM – abnormal

If the maximum amount of data transfers, set to 3 times of Vm RAM.
(1)If amount of data transfer > 3 times VRAM Forcefully stop VM and directed signature authentication
Then, set Th memory page = 50 (Or)
> 50 memory pages

(2)If VM migration amount is < X then, downtime > Th value Then destroy VM & migration.

→ Data migration during its nth cycle will always less than (or) equal to size of VRAM – V.

$$V * \begin{bmatrix} P \\ B \end{bmatrix} n\text{-}1 < V; \quad n >= 1 \dashrightarrow (4)$$

The RTT peak rate always less than network bandwidth available.

RTTP < B → B

Tc = V/B

Tc = [V/RTTP] ------→ (5)

Total Data migrated during the down time,

$$V \begin{bmatrix} P \\ B \end{bmatrix} n < \psi V \dashrightarrow (6)$$

ψ - Limit data transfer.

6.1 Results Analysis:-

Table -6.1 Report analysis

S.No	Preset Transfer rate (IOPS)	Starting Time (ms)	Completion Time (ms)	Actual Transfer Rate (IOPS)
1.	3000	4.03 ms	5.08ms	2800
2.	4000	5.09	6.05	3000
3.	4200	6.15 ms	7.10	7000
4.	3500	7.12ms	8.10ms	8000

Variation in the IOPS from the above statistical analysis clearly shows that unexpected data traffic between the VM's and Vswitch will lead to an unauthorized move of Virtual machine from the known Hypervisor to target attack surface in the cloud environment.From the estimated values above graph shows a sudden rise of the curve when there is high volume of data transfer at specific point of time.

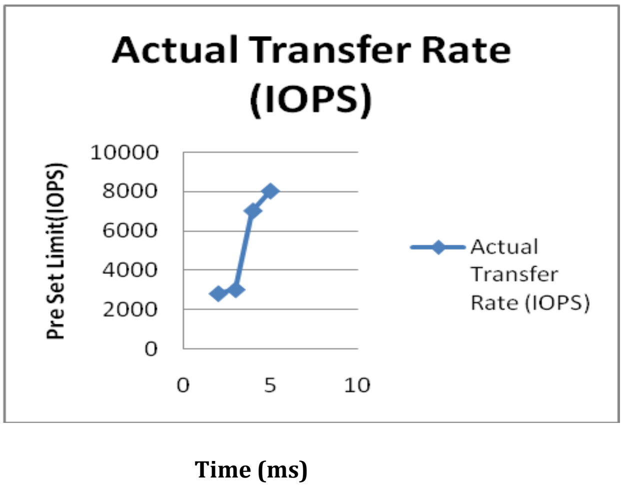

Chart -1: Transfer Rate Result Analysis

7. Conclusion

The Proposed model tries to reduce the Co- located VM attack on the same hypervisor and enforcing the security polices over the Virtual Machine, when there is an unauthorized move or Copy of Live VMs into malicious hypervisor. Monitoring preset data traffic rate between two VMs and Vswitch node helps to identify uncertainty of VMs at a specific point of time.

Simulated results also shows that proposed model will reduce the risk associated on the VM running on the suspected hypervisor in cloud.

Acknowledgement

I dedicate this research paper to my research supervisor Prof Dr.S.Rajalakshmi, Director Advanced Computing Centre,SCSVMV University for the support and guidance throughout my research work.

9.References:-

[1] Identifying and analyzing security threats to Virtualized Cloud Computing Infrastructures by Brohi, S.N., Bamiah, M.A.,Brohi, M.N., Kamran, R. in Cloud Computing Technologies IEEE 2012

[2] Improving the Resistance to Side-Channel Attacks on Cloud Storage Services **by** Heen, O., Neumann, C.,Montalvo, L.,Defrance, S in New Technologies, Mobility and Security (NTMS), IEEE 2012.

[3] Large-Scale Coordinated attacks: Impact on the Cloud Security by Riquet, D. , Grimaud, G. Hauspie, M. in Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on IEEE may-2012.

[4] Incentive Compatible Moving Target Defense against VM-Colocation Attacks in Clouds
by Yulong Zhang, Min Li, Kun Bai, Meng Yu, and Wanyu Zang in Computer Science Department, Virginia Commonwealth University ,IBM T.J. Watson Research Center, USA.

[5] On the Security of Tenant Transactions in the Cloud by Varadharajan, V.,Tupakula, U. in Cloud Computing Technology and Science (CloudCom),IEEE (Volume:1)2013.

[6] An Analysis on the Possibilities of Covert Transfers between Virtual Machines Clustered In Cloud Computing: Survey by Wilson Bakasa1, Kudakwashe Zvarevashe, Nicholas N. Karekwaivanane in International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 6, June 2014

[7] Security Games for Virtual Machine Allocation in Cloud Computing by Yi Han , Tansu Alpcan , Jeffrey Chan, Christopher Leckie in CCSW '14 Proceedings of the 6th edition of the ACM Workshop on Cloud Computing-2014

[8] Cloud Security: Attacks and Current Defenses by Gehana Booth, Andrew Soknacki, and Anil Somayaji
8th annual symposium on information assurance (ASIA'13), JUNE 4-5, 2013.

[9] Security of cloud computing, storage, and networking by Hamdi, M., Ariana, Tunisia in Collaboration Technologies and Systems (CTS), 2012 International Conference on IEEE-may-2012

[10] MUSHI: Toward Multiple Level Security cloud with strong Hardware level Isolation by Ning Zhang , Ming Li ,Wenjing Lou, Hou, Y.T. in military communications conference, IEEE 2012

[11] Cloud computing-based forensic analysis for collaborative network security management system Chen, Zhen , Han, Fuye, Cao, Junwei, Jiang, Xin more authors ,Tsinghua Science and Technology (Volume:18 , Issue: 1) 2013

[12] Mitigation of Cloud-Internal Denial of Service Attacks by Alarifi, S.,Wolthusen, S.D.,Service Oriented System Engineering (SOSE),IEEE-2014.

Author Profile:

Professor Mr.S.Ramamoorthy. B.E(CSE),M.E(CSE),(phd). He is currently pursing P.hD in SCSVMV University, India. His areas of interest Cloud Computing, BigData, Network Security, Data Mining, Mobile Communication. He has got around 6 years of teaching experience in SCSVMV University. Published various papers and journals on Cloud Computing and Network security. Currently working in the project for Education Cloud.