IJCSC 0973-7391 Volume 6 • Number 1 Sep - Mar 2015 pp.62-66 available online at www.csjournalss.com

Live Migration in Cloud and its Security Concerns: A Survey

[1]Tanvi Pandya, [2]Madhuri Bhavsar
[1]Department of Comp. Sc. and Engg, Nirma University, Ahmedabad, Gujarat, India
[2]Sr. Associate professor, Deptt of Comp. Sc. and Engg, Nirma University, Gujarat, India
Tnv.pandya@gmail.com

ABSTRACT: Cloud computing is a service which allows users to access the storage and resources on the subscription basis .One of the powerful concept of the cloud computing technique is Virtualization .The main reason behind the hosting of VM (Virtual Machine) in servers is to provide optimality to user's request.
Live migration is a process in which an application running on one system can be moved to another physical machine without disconnecting the application.
There are various reasons for performing live migration in Cloud Data centre but it is still in an early stage of implementation and its security is yet to be evaluated. The main concern of IT companies behind live migration are its security issues as there are many attacks possible ,which can leads to compromise of security in cloud environment.
Unfortunately the disclosed vulnerabilities with the live migration pose significant security risks. Because of these security risks the industry is hesitant to adapt the technology for sensitive applications. This report gives a complete study, analysis and design of the live migration and its security concerns.
Keywords: Live migration, security, virtualization, Cloud

1. INTRODUCTION

Cloud computing is one of the technology that has seen a tremendous growth in past several years. Cloud computing is a paradigm where Infrastructure, platform and software can be accessed as a Service and the user have to pay only for service they use.[1]
Virtualization is one of the important feature of cloud computing. Virtualization allows to create more than one virtual environments, which can be used to run different operating systems and application on a single physical machine. For example, with Virtualization you can have Linux Based OS on one Virtual Machine (VM) and Microsoft windows OS on other Virtual Machine (VM) running over same physical machine. This rapid development of cloud computing leads to lower operational and investment cost.
The most important part of Virtualization is hypervisor. Hypervisor acts as a layer between virtualized operating System and the real hardware. There are mainly two types of hypervisor, Type 1 and Type 2. Type 1 runs directly on the host hardware and type 2 run on host operating system. The type 1 hypervisors are preferred over type 2 hypervisor because type 1 hypervisor deal directly with the hardware and hence provide better performance efficiency, availability and security.[1][3]

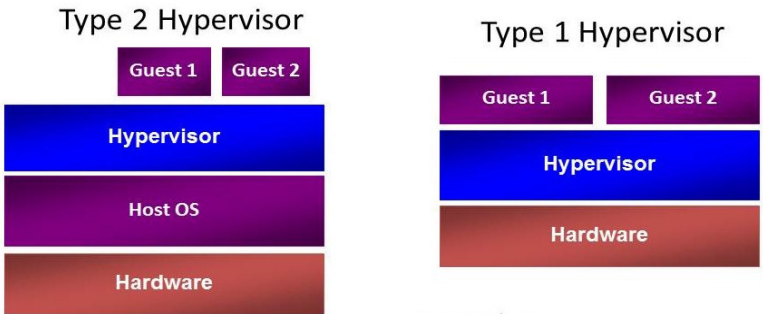

Figure: Type1 and Type 2 hypervisor

Using Virtualization, multiple Virtual machines can be created on a single physical machine along with the necessary isolation for each VM. This isolation ensures the security of each virtual machine. Live Migration is a process of migrating Virtual machine from one physical host to another without disrupting the service running on the source Machine with a little or no downtime. Live migration can be done in order to achieve energy

efficiency, load balancing and high availability of physical server in cloud data centre. However live migration is associated with few disadvantages as well such as new security and privacy problems.
The major vulnerabilities and threats that should be considered in cloud are 1) VM Poaching 2) VM jumping 3) Unsecured live migration.[4]

Advantages of virtualization
Virtualization helps in lowering the cost of space, hardware and power requirements by running multiple operating systems on a single hardware. In case of fault tolerance Virtualization also helps in migrating the resources.

2.POPULAR HYPERVISORS

Hypervisors are basically used to create the virtual machines. There are three major areas where they are used, at server i.e server virtualization, at storage i.e storage virtualization and at network i.e network virtualization. All the above listed type of virtualization requires hypervisor. The only difference is in the details and the load that the hypervisor is expected to carry in managing each Virtual machine[3]

XEN

- It is the oldest available open source virtualization technology used from approximately 5 years.
- Xen uses para-virtualization and hence it runs efficiently without the need of emulation.
- But Xen is very complex in nature so it is very hard to integrate with the Linux Kernel

KVM (Kernel based Virtual Machine)

- It resides in Linux kernel itself.
- Virtual machine can be created by just loading a module in the kernel.
- It has strengths such as security, Memory management, Live Migration, Performance, Scalability, and guest support.
- KVM support is pre-built into fedora Linux kernel for fedora 7 and above release.
- To fully utilize KVM following additional packages are required
- Qemu-KVM
- Virt-Manager
- Virt-Viewer
- Python-virtnist

3. LIVE MIGRATION

Virtualization is one of the major features responsible for the acceptance of cloud world-wide as it leads to reduced operational and investment cost. One of the important benefit of Virtualization is Virtual Machine (VM) migration. Live Virtual machine migration technique can be defined as the process of migrating the state of a physical machine to another without the disruption of the application running on the Source VM.[4][5]. There are different Virtual Machine migration techniques, such as:

A. Energy Efficient Migration Technique
The power consumed by the Data Centre directly depends upon the number of servers and the cooling System. The maximum power consumed by any server is up to 70%, even at their highest utilization level. So the migration technique can be used to maximize the use of the servers and reduce the overall power consumption.

B. Load Balancing Migration Technique
Migration technique can be used to distribute load across the servers in order to improve the scalability of cloud environment. It helps in minimizing the resource consumption; avoid bottlenecks and over-provisioning of resources.

C. Fault tolerant Migration Technique
If any part of the system fails then the fault tolerant migration technique can be used to keep the application running. This technique transfer the application from the failed VM to other VM and it is based upon future prediction of the system.

3.1 Security Concern in migration

One of the very important factors which is needed to be considered during migration is providing security to virtual machine while their migration from source to the destination.

There are various active and passive attacks possible during migration such as

- The attacker may steal the bandwidth by taking the control of source virtual machine and migrating it to the destination virtual machine.
- The attacker may falsely advertise its resource and attract others to migrate its resources towards itself.
- Passive snooping: Attacker just accesses the data of migration using any sniffing tool that may lead to leakage of some confidential information.
- Active manipulation: Attacker may modify the data which is travelling from the source to the destination.[6]

There are various cryptographic algorithms are available which can be used to encrypt the data in order to avoid the data from the attack to some extent. Following things should be enforced on the source and the destination machine before initiating the migration process:

- The migration initiator should be authenticated.
- Trust chain should be preserved among the entities during migration
- Migration should be confidential

3.2 Live Migration security Concerns

Live Migration leads to several security threats in cloud data centre. There are several security loopholes in live migration done by using KVM, Xen and VMware hypervisor. For Example, VMware may expose the sensitive information during migration and the Xen can take advantage of vulnerability in migration module and hence can take complete control of VMM or host VM.

In regard of migration security several research papers have been published and discussed but most of the solution works better only for offline migration, live migration still require much attention. The insecure live migration raises the risk of security as it may give rise to vulnerabilities and threats which than can be exploited by the attacker.

Attacks on Live migration can be categorized in different classes:[7][8]

3.21 **Control Plane**

All the operation such as initiation and management of live migration should be provided with proper authentication to secure the migration process against spoofing attacks and replay attacks. No user other than the authenticated user could do the migration process. The other possible attacks such as denial-of-service-attack which can be done by an attacker by initiating a large number of fake migrations to the legitimate destination. The possible attacks at the control plane are:

1. Incoming Migration Control
   By initiating unauthorised migration request, the attacker may live migrate the guest machine to the attacker's machine and hence can gain access to all the information of the guest VM.

2. Outgoing Migration Control
   The attacker can initiate the migration to the legitimate VM and can make the overuse of the resources of the legitimate VM which can lead to failure of the VM.

3. False Resource advertising
   The attacker can falsely advertise its resources and hence it can influence other VM to migrate its resources.

3.22 Data Plane

Insecure data plane can lead to various active and passive attacks. As in live migration all the states including CPU state, kernel details are transferred from host VM to destination VM, so it is possible that the attacker might do passive snooping and can get the confidential information which is getting transferred during migration. The attacker can also take control of migration data and may change it. Man-in-the-middle attack is one of the examples of attacks which may occur at the data plane, various sniffing tools such as wirshark can be used to do detect such type of attack.

3.23Migration Module

Migration Module is a software utility responsible for all migration related functionality, the vulnerability in migration module may allow compromising the VMM and any guest OSes as well. For example, Xen have following vulnerability which can be used as attack:

-Stack Overflow due to integer signedness issue

-Heap overflow due to issue in memory allotment routine.

3.3 EXISTING SOLUTIONS FOR PROVIDING SECURITY

1. Isolating Migration Network

In this approach the Virtual LAN consisting of the source and the destination host is isolated from migration traffic from other Network. This will reduce the risk of exposure of migration to the whole network.

2. Network Security Engine Hypervisor (NSE-H)

This functionality provides extension to the hypervisor by providing functionality of firewall and IDS/IPS which secure the migration from external attack and can also detect the network for the intrusion and hence an alarm can be generated in case of any intrusion detection.

3. Secure VM-vTPM Migration protocols

Secure VM-vTPM migration protocol consists of various steps starting from authentication, attestation and data transfer stage. Firstly both the parties that is source VM and the Destination VM authenticate each other for further communication. In the next step the integrity of the source and the destination is checked, only after verifying the integrity, the source VM start transfer to the destination VM. The file send by the source VM is stopped at the vTPM which encrypts the file and transfer to the destination VM. After completion of the transfer the file at the vTPM is deleted.

4. Improved vTPM Migration protocol

This protocol is improved version of vTPM. It consists of trusted channel establishment and data transfer. The source VM and destination VM first authenticate each other to establish the trusted channel and then integrity verification is done. Both the source and the destination negotiate keys with each other using DH key exchange algorithm. After the channel is established VM and vTPM starts the transfer as usual.

5. Using SSH Tunnel

SSH tunnel is established between the proxies for secure migration. The proxy server at the source and the destination cloud communicate with each other and hides the details of the source VM and the destination VM.[9]

3.4 PROPOSED SOLUTION:

After analysing all the existing scenario about the live migration, its security concerns and solution it can be concluded that there is still a need of improvement of securing the live migration from attacks.

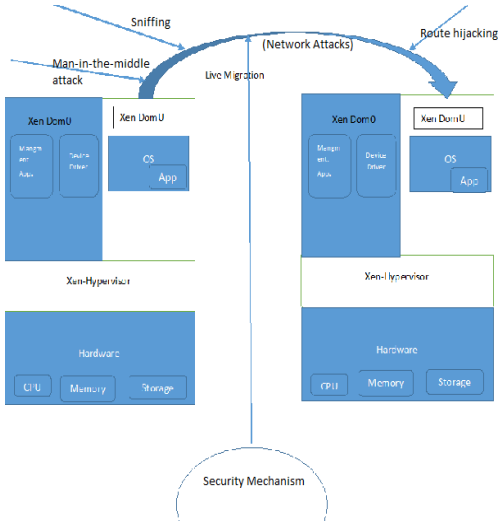

Figure: Proposed architecture

It is known that the live migration is a process started from the source VM to the destination VM.As shown in diagram there is need to apply some security mechanism between the source and destination in order to prevent from network attacks such as sniffing, route hijacking, man-in-the-middle attack. The above diagram shows how two virtual machines communicate with each other for live migration, how the network is established, which attacks are the possible during migration and where the security mechanism should be applied. The security mechanism will encrypt the data before transferring it to the network, so now as data would be encrypted over the channel there are less chances of attack and leaking of the confidential information.

3.5 CONCLUSION AND FUTURE WORK

In this paper we have discussed about the live migration and its security concerns.There are various attacks possible on the live migration .Till now a lot research have been doneand various research paper have been published with the different solutions to secure the live migration process but no solution provide the complete security.

Our proposed architecture uses the encryption at the hypervisor level which can helps in providing security in better way , there are various encryption algorithms available such as RAS, DES, AES which can be used along with the migration module.

3.6 REFERENCES

[1] Perez-Botero, Diego. "A Brief Tutorial on Live Virtual Machine Migration From a Security Perspective." University of Princeton, USA (2011).

[2] Wang, Wei, et al. "Secured and reliable vm migration in personal cloud." Computer Engineering and Technology (ICCET), 2010 2nd International Conference on. Vol. 1. IEEE, 2010.

[3] YamunaDevi, L., et al. "Security in virtual machine live migration for kvm." Process Automation, Control and Computing (PACC), 2011 International Conference on. IEEE, 2011.

[4] Ahmad, Naveed, Ayesha Kanwal, and Muhammad AwaisShibli. "Survey on secure live virtual machine (VM) migration in Cloud." 2013 2nd National Conference on Information Assurance (NCIA).

[5] Biedermann, Sebastian, Martin Zittel, and Stefan Katzenbeisser. "Improving security of virtual machines during live migrations." Privacy, Security and Trust (PST), 2013 Eleventh Annual International Conference on. IEEE, 2013.

[6] Anala, M. R., Jyoti Shetty, and G. Shobha. "A framework for secure live migration of virtual machines." Advances in Computing, Communications and Informatics (ICACCI), 2013 International Conference on. IEEE, 2013.

[7]Leelipushpam, P. GetziJeba, and J. Sharmila. "Live VM migration techniques in cloud environment—a survey." Information & Communication Technologies (ICT), 2013 IEEE Conference on. IEEE, 2013.

[8] Sulaiman, NorshazrulAzman Bin, and Hideo Masuda. "Evaluation of a Secure Live Migration of Virtual Machines Using Ipsec Implementation." Advanced Applied Informatics (IIAIAAI), 2014 IIAI 3rd International Conference on. IEEE, 2014.

[9] Wang, Wei, et al. "Secured VM Live Migration in Personal Cloud." Proceedings of ICCET, China (2010).

[10] Aiash, Mahdi, GlenfordMapp, and OrhanGemikonakli. "Secure live virtual machines migration: issues and solutions." Advanced Information Networking and Applications Workshops (WAINA), 2014 28th International Conference on. IEEE, 2014.