A SURVEY ON DIFFERENT CLOUD COMPUTING SECURITY AND MIGRATION TECHNIQUES

[1] Akshay Gangwani, [2] Dr.Harshal Shah,[3] Dr. Kaushal Shah
[1] M.Tech student of Computer Science, [2] professor,[3] professor,
Parul University, Waghodia, Limda, India

Abstract: In Cloud Computing, virtualization plays a major role. Virtualization in terms of CPU, Memory, Disk, and Network this all are provided by virtual machines (VM). For the development of cloud computing infrastructure, we have to use hypervisors such as VMware, KVM, and Oracle VirtualBox. There are many processes that need to follow in Cloud Computing such as live migration, load balancing, power management, network management, etc. In live migration one physical node transfers all access to another physical node or same VM of a physical system. By live migration, we have high availability and shut down or sleep unused VM to save power consumption. We are focusing on migration as well as security aspects of VM. So, we are exploring such a technique that will optimize VM's working.

Keywords **- Cloud Computing, Security, live Migration, scheduling, Virtual Machine.**

I. INTRODUCTION

Cloud computing has three models known as SAAS, PAAS, and IAAS. SAAS is known as Software as a service. There are so many examples of SAAS such as GMAIL, Online ERP Systems where user or client can use their service no need to do development, the second model is PAAS where hardware and software things are provided by cloud providers to develop such application. Lastly, the third model which is known as IAAS where all computing resources such as CPU, Ram, Disk and Network are given by Cloud Provider. VM Migration is part of Cloud Computing where VM is transferred or Migrated to another VM or another PM (Physical Machine). There are so many Security threats that are identified during VM migration where the attacker has so many techniques of doing the attack.

II. LITERATURE REVIEW

A. VM Migration

Firstly, Migration Consist of Memory transfer. This Memory transfer consists of three phases known as push phase, stop-and-copy phase, pull phase [15].

1) Push Phase

The VM keeps running at the source host computer where it's all memory pages are transferred over the network to the destination host. In this process the memory pages— that are already arrived at the destination host, but modified again at the source during this process, known as dirty pages—are sent again to the destination in order to preserve memory consistency [15].

2) Stop-and-copy phase

In this phase the VM source host is stopped, memory pages are transferred to the other host and therefore the VM starts at the destination host [15].

3) Pull phase

VM at the destination, if a page which is not been copied from the source (known as a page fault), pulls the page across the network from the source host.

B. Migration Algorithms

Migration Algorithms use combinations of memory migration phases. It uses one or two sorts of phases there are two techniques that are widely used pre-copy & post-copy [15].

1) Pre-copy

This algorithm uses an iterative push phase that follows a short stop-and-copy phase. In the push phase, all the memory pages are first copied to the destination. After that, only dirty pages are copied to the destination in iterative rounds, i.e., pages transferred to destination host during round n are the pages modified during the round n − 1. In the stop-and-copy phase, only the CPU state and any remaining dirty pages are sent to the destination which brings the destination VM to a totally consistent state. In the pre-copy algorithm, the source host handles the requests to VM services during the live migration process. Due to repetitive push-phase, a minimal number of pages are transferred throughout stop-and-copy phase part resultant downtime can be reduced. However, it might need to send a large number of pages repeatedly wasting bandwidth, if the pages are modified frequently. Both Xen hypervisor and VMware hypervisor uses the live migration pre-copy approach.

2) Post-copy

The post-copy algorithm uses a short stop-and-copy phase followed by a pull phase. In the stop-and-copy part, the VM goes offline at the source machine, VM's processor state is transferred to the destination host and resumed there. The VM is then started at the destination and other memory pages are fetched (pulled) across the network from the source host on their first use. In the post-copy rule, the destination host handles the requests to VM services during the live migration process. The post-copy technique results ends up in downtime at the cost of increased total migration time.

C. Live Migration Process

Live Migration is a process where one Physical Machine transfers all service to a different Physical Machine or different VM of the same PM. It facilitates with a decrease in downtime, high availability, maintenance of VMs, workload balancing and you'll save power from performing VM migration.

Live migration of VM introduces serious security hazards in traditional data centres additionally as in the Cloud environment. The up to date analysis on live migration so far is performance bound and security problems haven't received a lot of attention. There are numerous security hazards in the live VM migration process gave by Xen, KVM and VMware hypervisors. For instance, in Xen an assailant can control with VMM or guest OS because of vulnerabilities in the migration module [3]. Similarly, VMware (VMotion) uncovers the private data of guest OS throughout the VM migration [3]. Without security features, the live migration process becomes a single point of failure for the Cloud environment. There's a critical need of research on security problems of the live migration process in Cloud

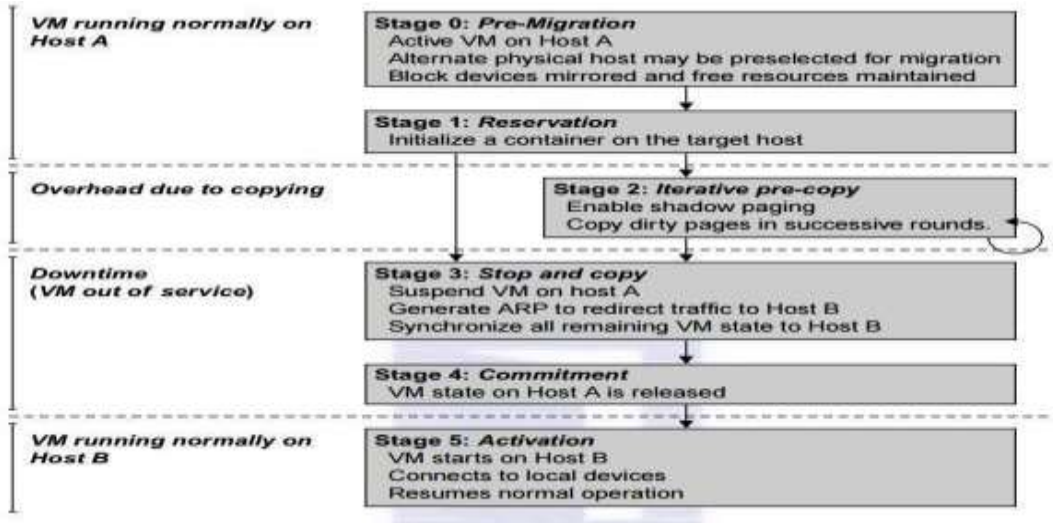

Fig. 1. Live Migration Process[11]

D. Identified threats and vulnerabilities in Live VM Migration

For the secure VM migration, much research has been accomplished with attention on offline migration. However live VM migration still must be actively investigated.

Live VM migration suffers from many vulnerabilities and threats which may be easily explored by the attackers. live migration attacks are often targeting one among these three different classes: (1) control plane (2) data plane and (3) migration module [11].

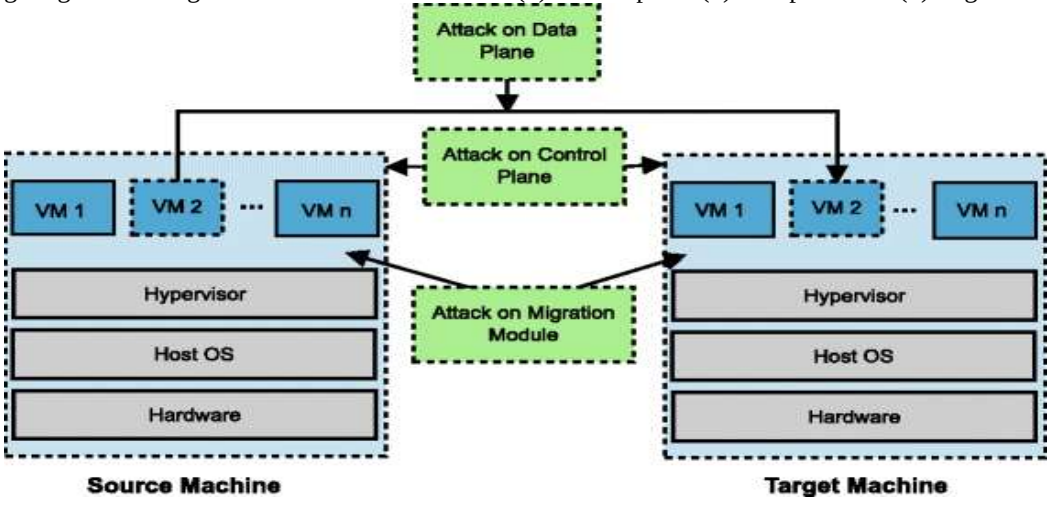

Fig. 2. Possible attacks during the time of migration[10].

1) Control Plane

Hypervisor operations like initiation and management of live VM migration must be authenticated and resistant against tampering. meanwhile, protection against spoofing and replays attacks should be provided [10].

2) (ii) Data Plane

Live VM Migration occurs during this plane, memory contents like kernel states and application data transfer from one physical server to a different [10].

3) (iii) Migration Module

VM Migration functionality of VMM is implemented by the software component which is understood as the migration module. Back doors in migration module attacker to compromise the Hypervisor and any guest OSes as well

E. DOS & DDOS Attacks during the time of migration

Computer network uses TCP Protocol for data transfer or Packets are sent by TCP Protocol. The attacker can attack by sending one or more packet to the network this may cause target server and network resources to get overloaded this is called DDOS attack. It's difficult to get attack packets from diverse traffic [14]

1) Volume-based attacks

This type sends a greater number of requests or data to the network devices to be Overloaded, by that network's bandwidth goes broad. Hence new requests are cannot be catered by the server. The resultant network cannot work.

2) Protocol-based attacks

Traffic flooding attacks are popular attacks. the attackers send a large number of apparently authentic UDP packets, TCP/IP, ICMP packets in network host. Resultant traffic increases in the network [14].

3) Application-based attacks

This type of attack conducts Application based attack whereby attack is performed on a webserver. This causes down all web services hosted on a web server such as websites. A normal attack on webservice can degrade the performance.

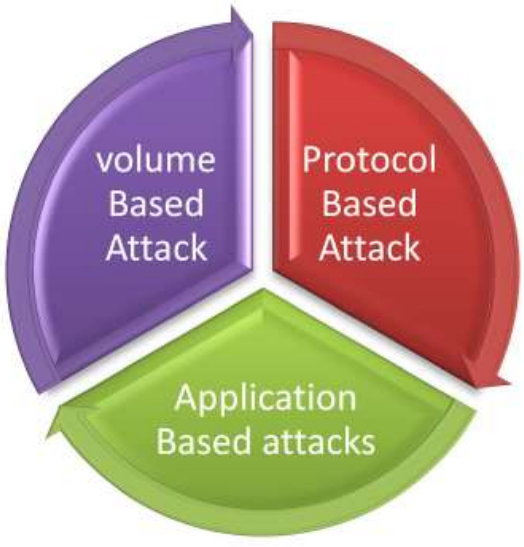

Fig. 3. Attack Methods on VMs [14].

When we are talking about security, we must go through attacks also so we have focused on DDOS Attacks.

There are many kinds of DDOS attacks such as UDP flood, ICMP flood, SYNCHRO flood, Ping of Death, Slowloris, HTTP flood attacks.

1) UDP Flood Attack:

It does a session with less connection. It is trying to reach any one of the ports in target pc with one or a lot of varied UDP packets. This service is not using the session so it will have to check the packet is reached at the destination or not.

2) ICMP Flood Attacks:

We do ping requests to check whether the host is reachable or not. Attackers send a large number of packets while not awaiting replies. This consumes a lot of bandwidth and causes ICMP flood attacks [14].

3) SYN Flood Attacks:

In general TCP follows three-way handshaking. The destination sends a synchronization request to the destination host server. The servers respond to the destination clients by sending synchronization acknowledgments. Then the client will launch the Synchronization Acknowledgement. The host server system that continuously was awaiting a reply [14].

4) Ping of Death Attacks:

The attacker will throw malware attacking ping request packets to one or more computers. There is a limit for packet length. This will cause the buffer over within the host. This will result in DDoS attacks.

5) Slowloris Attacks:

This attack creates a continuous connection to the host server. Half of the requests will be sent to the target server. The target host server is open for the ever-wrong connection. It invariably a lot of a number of HTTP request however never complete the request [14].

6) HTTP flood Attacks:

The attacker carried out these attacks by GET and POST methods. It tries to accomplish a resource request with a large number of resources. These will fallout in HTTP Flood DDoS attacks.

In this paper-author have included palm (protection aegis for live migration) method. They have implemented a module for privacy and integrity of sensitive data but due to an increase in scalability systems performance gets down. [16] In another paper they have used TAL (trusted assurance level) where trust token which is used as a trusted credential. in the previous method there was PTAA (platform trust assurance authority) used as a proxy server for authentication of server.in this method PTAA removed thereby scalability and performance issue is solved [17]. ARM (Attack resiliency matrices) is very useful where we have to find the most secure node in the cloud system. ARM is the ratio of block attack and total no of attempted attacks. you can find PIF (Performance Improvement Factor) where the ratio of ARM (new)-ARM (old) and ARM (old). Lastly CBM, you can find cost-benefit matrices [18].

Technique	Advantages	Disadvantages
isolated migration network [4]	- In this approach source and destination VM's grouped into Virtual LAN (VLAN). It isolates the migration of traffic from other network traffic. Segregation of migration traffic will reduce the danger of exposure	-It only segregates the migration traffic from network traffic. It gets more complex and administrative cost increased with a population of VM's
Network Security Engine-Hypervisor (NSE-H) [4]	This approach is an extension to Hypervisor. It has a firewall, IDS/IPS functionalities for protection against intrusions in a virtual network.	-NSE-H based approach does not support any of the security requirements for VM migrations depicted in Table.
Improved vTPM migration protocol [5]	It consists of the establishment of a trusted channel and secures data transfer phases. In the establishment of a trusted channel phase, first both parties mutually authenticate each other and then property based remote attestation is done by a source host to check/verify the integrity.	Live migration is not supported in vTPM based migration tools. The vTPM state is additionally migrated along-side VM.
Secure VM-vTPM migration protocol [8]	It consists of authentication, attestation and data transfer stages.	Live migration is not supported in a vTPM based migration protocol. Keys of vTPM are also stored outside the TPM
Inter-cloud VM mobility [9]	the design consists of inter-cloud proxies, secure channels between proxies, migration with non-shared storage and virtual network migration components.	Authorization is not supported in this solution. Furthermore, it requires port forwarding on firewalls.
Trusted Cloud Security Level (TCSL) [10]	the logical union of VM's and isolates trusted zones based on security requirements of VM's in the cloud.	This approach does not provide any of the identified security requirements for VM migration.
DOS Attacks [14]	This paper shows how attacks are performed which are the type of attack and hoe to prevent them.	Cannot work on server-side attack prevention.
Counter And Time-stamp [15]	They have discussed policy about migration such as confidentiality and integrity maintain by having counter and times-stamp.	
PALM Method (Protection Aegis of Live Migration in VMs) [16]	Privacy and integrity are maintained.	Performance degradation of live migration.

Trusted Token and TAL (Trusted Assurance Level) Method [17]	Scalability and performance improved.	Degrades security level.
ARM, PIF, CBM Metrics [18]	By this method, we can check and we can know which node is most secure.	The performance issue is there.

Fig. 4. Survey Table of Different Methods

III. CONCLUSION

To Conclude, we get to know which are the problem constrain. We have surveyed so many techniques of migration and security given by them. Two things we need to cater first is migration and second is security. We have studied attack methods on VMs by we say that systems have some kind of vulnerability. We have to stop those doors for attackers.

IV. ACKNOWLEDGMENT

First of all. Thank you for giving me hope and Accomplish paper, I would like to acknowledge the support that I had got from Dr. Harshal Shah and Dr. Kaushal Shah professors at the CSE Department in Parul Institute of Technology. I have a great thankful to Professor Dr. Kirit Modi, HOD of CSE. I want to express warm gratitude to all staff members of the Parul University Computer Science and Engineering Department.

REFERENCES

[1] "Cloud Computing" https://www.webopedia.com/TERM/C/cloud_computing.html

[2] "What is Live VM Migration" https://searchservervirtualization.techtarget.com/definition/live-migration

[3] "Live VM Migration and Performance Effects" http://www.brainkart.com/article/Live-VM-Migration-Steps-and-Performance-Effects_11345/

[4] J. Shetty, Anala M. R, Shobha G, "A survey on techniques of secure live migration of virtual machine", International Journal of Computer Applications (0975 – 8887), vol. 39, no.12, February 2012.

[5] X. Wan, X. Zhang, L. Chen and J. Zhu, "An improved vTPM migration protocol based trusted channel", International Conference on Systems and Informatics, 2012, pp. 871-875.

[6] OpenStack Security Guide, 2013. http://docs.openstack.org/security-guide/security-guide.pdf.

[7] W. Wang, Y. Zhang, B. Lin, X. Wu and K. Miao, "Secured and reliable VM migration in personal cloud", 2nd International Conference on Computer Engineering and Technology, 2010.

[8] B. Danev, R. J. Masti, G. O. Karame and S. Capkun,"Enabling secure VM-vTPM migration in private clouds", Proceedings of the 27th Annual Computer Security Applications Conference, December 05- 09, 2010, Orlando, Florida.

[9] K. Nagin, D. Hadas, Z. Dubitzky, A. Glikson, I. Loy, B. Rochwerger and L. Schour, "Inter-cloud mobility of virtual machines", International Conference on Systems and Storage, May 30-June 01, 2010, Haifa, Israel.

[10] Prashant Sahatiya, Harshal Shah, "SECURE LIVE VIRTUAL MACHINE MIGRATION IN CLOUD COMPUTING ", IJRAR - International Journal of Research and Analytical Reviews (IJRAR), E-ISSN 2348-1269, P- ISSN 2349-5138, Volume.6, Issue 1, Page No pp.176-182, March 2019

[11] Anita Choudhary, Mahesh Chandra Govil, Girdhari Singh, Lalit K. Awasthi, Emmanuel S. Pilli, Divya Kapil, "A critical survey of live virtual machine migration techniques", Journal of Cloud Computing, Springer, November 2017.

[12] Gurpreet Singh, Supriya, "A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security", International Journal of Computer Applications, April-2013.

[13] Subramaniam.T.K1*, Deepa "PREVENTING DISTRIBUTED DENIAL OF SERVICE ATTACKS IN CLOUD ENVIRONMENTS". International Journal of Information Technology, Control and Automation (IJITCA) Vol. 6, No.2, April 2016.

[14] Yasmin R., Memarian M.R., Hosseinzadeh S., Conti M., Leppänen V. (2018) Investigating the Possibility of Data Leakage in Time of Live VM Migration. In: Dehghantanha A., Conti M., Dargahi T. (eds) Cyber Threat Intelligence. Advances in Information Security, vol 70. Springer, Cham

[15] F. Zhang, Y. Huang, H. Wang, H. Chen and B. Zang, "PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection," 2008 Third Asia-Pacific Trusted Infrastructure Technologies Conference, Hubei, 2008, pp. 9-18.

[16] M. Aslam, C. Gehrmann and M. Björkman, "Security and Trust Preserving VM Migrations in Public Clouds," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, 2012, pp. 869-876.

[17] T. Zeb, M. Yousaf, H. Afzal and M. R. Mufti, "A quantitative security metric model for security controls: Secure virtual machine migration protocol as target of assessment," in China Communications, vol. 15, no. 8, pp. 126-140, Aug. 2018.