Integrated Secure Architecture for Live Virtual Machine (VM) Migration in Cloud – A Survey

[1]Prashant Sahatiya, [2]Harshal Shah
[1]M.Tech Student, [2]Prof.
[1-2]Dept. of Computer Science Engineering
[1-2]Parul Institute of Engineering & Technology
Vadodara, India

Abstract— ***Abstract*** **- The core of Cloud computing includes virtualization of hardware resources such as storage, network and memory provided through virtual machines (VM). The live migration of these VMs is introduced to obtain multiple benefits which mainly include high availability, hardware maintenance, fault takeover and workload balancing. Besides various facilities of the VM migration, it is susceptible to severe security risks during migration process due to which the industry is hesitant to accept it. The research done so far is on the performance of migration process; whereas the security aspects in migration are not fully explored. We have carried out an extensive survey to investigate the vulnerabilities, threats and possible attacks on the live VM migration. Furthermore, we have identified security requirements for secure VM migration and presented a detailed analysis of existing solutions on the basis of these security requirements. Finally, limitations in the existing solutions are presented.**

Keywords— Virtualization, Live VM Migration, Cloud computing, Cloud security, Infrastructure as a Service (IaaS)

I. INTRODUCTION

Cloud computing is gaining attention in small and medium enterprises (SME's) because of lower infrastructural cost. It enables ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [1, 2]. Cloud computing provides services via Platform as a Service (PaaS), Software as a Service (SaaS) and Infrastructure as a Service (IaaS) delivery models. SaaS is a software distribution model in which applications reside on cloud service provider (CSP) and are available for its client via a web browser (e.g., Google docs). PaaS model refers to the delivery of operating systems and associated tools over the internet. A consumer deploys his application on the CSP without installing any platform or tool on their local machines. In IaaS delivery model, CSP outsource the processing, storage, network and all other computing resources in the form of VM's.

Cloud Computing is providing many benefits to SME's, however there are still many significant barriers in its adoption. The security of data and information in Cloud is the main concern of any organization. Cloud technology is combination of several other technologies such as Virtualization, Service Oriented Architecture (SOA) and web 2.0 [1]. Security limitations in these traditional technologies are also inherited in the overall security of Cloud along with their benefits. As Cloud infrastructure consists of large scale, distributed, heterogeneous and completely virtualized resources, therefore the traditional security mechanisms are not enough for this environment. In SaaS delivery model, the customer has very less control over the resources; therefore the CSP is responsible for managing the required security mechanism. In SaaS delivery model, the consumer has less control over the resources therefore the burden of security lies on CSP. Whereas the PaaS delivery model offers greater customer control as compare to SaaS, therefore both CSP and customer are responsible for resources security. IaaS offers greater customer control over security as compared to the PaaS or SaaS models. We need to understand the relationships and dependencies between these three Cloud delivery models. The PaaS and SaaS models are dependent on IaaS for their services, therefore any breach in IaaS model will also have an impact on the security of both PaaS and SaaS and vice versa. Virtualization is key technology in IaaS delivery model where CSP provides a pool of storage, network, and other computing resources in the form of VM. However, besides the various benefits of virtualization it has also introduced new opportunities for attackers [1, 2]. Therefore VM security becomes critical for overall security of IaaS model.

In IaaS model, CSP allocates resources to consumers using VM which is a core component of Cloud computing. Therefore, it is important to consider the security of VM in Cloud domain. Virtualization provides various benefits in Cloud but it also raises security risks that can affect the Cloud environment. The major virtualization specific vulnerabilities and threats that must be considered in Cloud include (i) VM poaching (ii) the VM jumping (iii) and unsecured live VM migration. In VM poaching attack, migration. In VM poaching attack, guest operating system (OS) takes up more CPU, memory or any other computing resources allocated to it against the other guest OS running in the same hypervisor. VM jumping attack, exploits the vulnerabilities of Hypervisors that allows malicious code to bypass VM protections and gain control to any other VM. Live VM migration tool used to transfer VM from one physical server to another with minimum downtime whereas offline or suspended VM migration increases the downtime. It provides work load balancing, hardware/system maintenance, high availability services, transparent mobility and consolidated management. The unsecured live VM migration potentially opens up the security risks and exposure for not only the migrated VM but also for the other guests OSes running on that Physical Server [3, 4, 5].

Live migration of VM introduces severe security risks in traditional data centers as well as in Cloud environment. The contemporary research on live migration so far is performance oriented and security issues have not received much attention. There are several security risks in live VM migration process provided by Xen, KVM and VMware hypervisors. For instance, in Xen an attacker can gain control of VMM or guest OS due to vulnerabilities in migration module [3]. Similarly VMware (VMotion) exposes the sensitive information of guest OS during the VM migration [3]. Live VM migration without security features becomes single point of failure (SPF) for Cloud environment. There is an intensive need of research on security issues of live migration process in Cloud.

In this regard, we have carried out an extensive survey of live VM migration, identified the important vulnerabilities in migration module as well as in live VM migration process. Furthermore, discovered the various threats found in literature related to the VM migration in Cloud computing. We have also identified the security requirements for VM migration and analysis of existing solutions on the basis of these identified requirements. Furthermore, limitations of existing solutions and approaches are also explored. The rest of the paper is organized as follows: section II presents summary of the topics that are discussed in the VM migration literature. Section III presents the identified vulnerabilities and threats on live VM migration process. Section IV contains the analysis of existing solutions and limitations of VM Migration process and sections V concludes the paper along with future research directions.

II. LITERATURE SURVEY & WORK ANALYSIS

We have summarized the literature review in the Table I. We identified that most of the papers discussed the threats and vulnerabilities in live VM migration. As shown in the Table I, proposed solutions mostly target the offline VM migration and whereas live VM migration has not received much attention. Moreover security requirements for secure live VM migration process are also discussed. Furthermore, it is also discussed that insecure live VM migration raises security risk in IaaS model of Cloud Computing. Threats and vulnerabilities of migration process will also impact the security of IaaS model.

TABLE I SUMMARY OF LITERATURE ON VM MIGRATION

Topics/ References	1	3	6	7	9	10	11	12	13	14	15	16	17
Vulnerabilities	✓	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗
Threats / Attacks	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗	✓	✓	✓
Mechanism for Secure offline VM migration	✗	✗	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗
Mechanism for secure live VM migration	✗	✗	✗	✗	✗	✗	✓	✗	✓	✗	✗	✗	✓
IaaS security	✓	✗	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗
Security Requirements	✗	✓	✓	✓	✗	✓	✗	✗	✗	✗	✗	✗	✗

III. IDENTIFIED THREATS AND VULNERABILITIES IN LIVE VM MIGRATION

Jon et al [3] has empirically demonstrated that live VM migration process is prone to active and passive attacks. Attacks on live VM process are categorized into control plane, data plane and migration module classes.

A. Control Plane:

Hypervisor operations such as initiation and management of live VM migration must be authenticated and resistant against tampering. Furthermore, protection against spoofing and replays attack should be provided. A lack of security in the control plane may allow an attacker to exploit live migration operation in different ways:

1. Denial-of-Service (DoS) attack: Attacker will create many VM's on the host OS just to overload the host OS, which will not be able to accept any more migrated VM's.
2. Unnecessary migration of VM: Attacker will overload the host OS by unneeded VM's. This will force execution of the dynamic load balancing feature, which will ensure migration of some VMs to balance the load.
3. Incoming Migration Control: The attacker can initiate an unauthorized migration request, so VM can be migrated from secure source physical machine to a compromised attacker machine. This may result in attacker getting full control on the legitimate VM.
4. Outgoing Migration Control: The attacker can initiate the VM migration and can make the overuse of the cloud resources which can lead to failure of the VM.

5. Disrupt the regular operations of the VM: An attacker may migrate a VM from one host to another host without any goal except to interrupt the operations of the VM.
6. Attack on VMM and VM: Attacker will migrate a VM that has a malicious code to a host server that has the target VM. This code will exchange information with the VMM and the target VM through a covert-channel. This channel will compromise the confidentiality of the host server by leaking target VMs' information.
7. Advertising for false resource: Attacker advertises false resource availability for the target VM. For example, advertising that there is a large number of unused CPU cycles. This results in migration of the VM's to a compromised hypervisor migrating VM. The attacker gains information from the VM's migrating memory (e.g., passwords, keys, application data, capturing packets that are already authenticated, messages that have sensitive data will be overheard, etc.) [18].

B. Data Plane

Live VM Migration occurs in this plane, memory contents such as kernel states and application data transfer from one physical server to another. Attacker can use ARP spoofing or DNS poisoning techniques to launch man in the middle (MITM) attack on insecure communication channel. This introduces active and passive attacks during the migration process. Therefore secure and protected channel must be use to minimize snooping and tampering attempts on migration data. Hence, an attacker may place himself in the trans- mission channel to perform a man-in-the-middle attack using any of the techniques: Address

Resolution Protocol (ARP) spoofing, Domain Name System (DNS) poisoning, or route hijacking [18]. Man-in-the-middle attack can be one of the two types of attacks - passive and active:

1. Passive Attack: Attacker observes the transmission channel and other network streams used to get the information of migrating VM. The attacker gains information from the VM's migrating memory (e.g., passwords, keys, application data, capturing packets that are already authenticated, messages that have sensitive data will be overheard, etc.) [18].
2. Active attack: This attack is the most serious attack in which the attacker manipulates the memory contents (e.g., authentication service and pluggable authentication module in live migration) of migrating VM's [18].

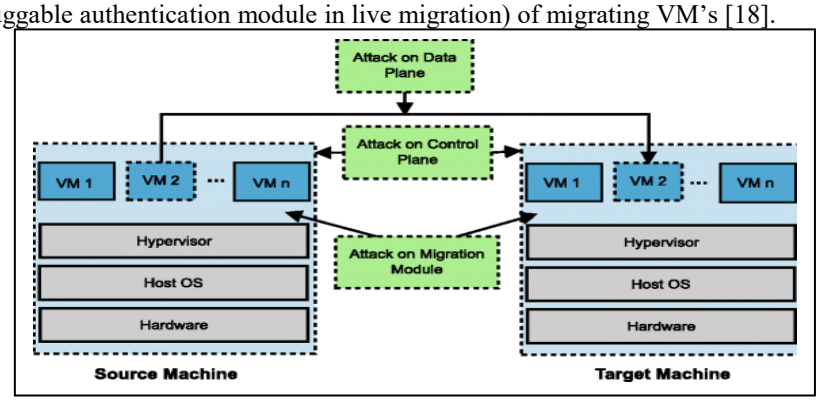

Figure 1Possible attacks during Live VM Migration [18]

C. Migration Module:

Migration module is a software component in the VMM that allows live migration of VM's. A guest OS can communicate with the host system and vice versa. Moreover, the host system has full control over all VM's running over its VMM. If the attacker is able to com- promise the VMM via its migration module, then the integrity of all guest VM's that are running above this VMM will be affected. Any VM in the future that will migrate to the affected VMM will also be compromised. VM with a low security level is exploited using the attack techniques in the migration module. When an attacker discovers a VM with a low security level during the migration process, they will attempt to compromise it and can do it easily. They can use it as a gate to compromise other VM's on the same host with higher levels of security [18]. Moreover, the attacker will be able to attack the VMM itself, after identifying a way to enter the system.

IV. ANALYSIS OF EXISTING SOLUTIONS AND APPROACHES

In this section we have identified and formulated essential security requirements that should be provided for secure live and offline VM migration in Cloud domain. Following is the description of each of these requirements. We have also performed extensive analysis of existing solutions with respect to these security requirements. Table II, is the result of our extensive analysis with respect to security aspects:

A. Security Requirement for VM Migration

We have identified the following security requirements for the live VM migration process. These requirements must be incorporated in secure live VM migration process [6, 7].

1. Integrity Verification of Platform
   The destination platform cryptographically identifies itself to source for trust establishment.
2. Authentication
   Attacker can launch MITM attack using technique such as route hijacking or ARP poisoning in the migration process. In order to avoid MITM attacks on live VM migration, source and destination platforms must mutually authenticate each other.
3. Authorization (Access control policies)
   Appropriate access control policies must be provided to secure the live VM migration process. An unauthorized user/role may launch VM initiate, migration operation. Unauthorized activities can be prevented using access control list (ACL's) in hypervisor.
4. Confidentiality and Integrity of VM during migration
   An encrypted channel must be established so that an attacker cannot get any information from VM contents and modification of contents can be properly detected. This will help to avoid active attacks such as memory manipulation on live migration and passive attacks such as leakage of sensitive information.
5. Replay Resistance
   Attacker can capture traffic and replay it latter to get authenticated in VM migration process. Therefore live VM migration process should be replay resistant. Nonce's can be used to prevent replay attack in migration.
6. Source Non-Repudiation
   Source host cannot deny from VM migration operation. This feature can be achieved by using Public key certificate

B. Existing VM Migration Solutions

In isolated migration network approach source and destination VM's grouped into Virtual LAN (VLAN). It isolates the migration traffic from other network traffic. Segregation of migration traffic will reduce the risk of exposure [6, 8].

Network Security Engine-Hypervisor (NSE-H) based approach is an extension to Hypervisor. It has firewall, IDS/IPS functionalities for protection against intrusions in virtual network. Its architecture consist of Virtual Machine Migration Agent (VMMA), Security Context Migration Agent (SCMA), Live Migration Coordinator (LMC) components [6].

Policy/Role based migration approach uses Intel vPro technology for protection of migration process. It consists of Attestation Service, Seal Storage, Policy Service, Migration Service and Secure Hypervisor components [6,9].

Secure VM-vTPM migration protocol consist of authentication, attestation and data transfer stages. In the first stage, both parties mutually authenticate each other and establish secure session for subsequent communication. After authentication and secure channel establishment, remote attestation performed by source to check/verify the system integrity. In the last step, VM and vTPM transfer occurs. Source host first suspends the VM along vTPM, encrypt them and then transfer to destination machine. Furthermore, source host also deletes VM along its vTPM [6, 10].

The improved vTPM migration protocol consist of establishment of trusted channel and secure data transfer phases. In establishment of trusted channel phase, first both parties mutually authenticate each other and then property based remote attestation is done by source host to check/verify the integrity. Both parties negotiate cryptographic mechanism, hash schemes and key exchanges using DH key agreement protocol. After establishment of authenticated and secure session, VM and vTPM transfer mechanism is initiated. Source host suspends the VM and its associated vTPM and takes hash of vTPM components. Encryption on VM and vTPM package is performed and then transferred to destination host [7].

Kenneth et al [11] proposed design consist of inter cloud proxies, secure channel between proxies, migration with non-shared storage and virtual network migration components. Inter cloud proxies used to restrict access to those hosts which are used in inter cloud VM mobility. The proxy server at the source and destination clouds communicates with each other and hides the details of source and destination Cloud hosts. SSH tunnel is established between proxies for secure VM migration and VM states and memory is transferred during the migration process.

Trusted Cloud Security Level (TCSL) proposed new architecture for cloud platform with set of policies to customize zones. TCSL is the logical unions of VM's and isolates trusted zones based on security requirements of VM's in cloud. Every trusted zone in trusted cloud has a security level. VM migration in trusted cloud is managed by Reliable Migration Module (RMM). It consist of Central Security Management, Cloud Security Management, Security Attributes and Waiting Queue for Migration layers [12].

RSA with SSL based Secure VM migration process is consists of three steps. First, load calculation on physical host then RSA with SSL protocol is used for authentication and encryption mechanism as well as for protection and privacy of memory contents.

Finally, Pre-copy or Post-copy migration techniques used for live migration between source and destination [13].

Trusted Token (TT) based migration approach consists of set policy, implement migration policy and audit migration components. User's policy contains the acceptable Trust Assurance Level (TAL) value of the target cloud platform for VM migration.TT is a trust credential which contains TAL value issued by Platform Trust Assurance Authority (PTTA) based on hardware and software components of platform. VM migration occurs if TAL value in TT of destination platform is acceptable against the TAL value of user migration policy. TPM-based bind key pair is used for encryption of VM [14].

Fengzhe et al [17] proposed secure VM migration in customized VMM called VMM enforced protection system which provides security to processes in Virtual Machine. Protected memory pages are also stored in VMM. CHAOS is used to maintain encryption keys for application in VM and Overshadow maintains keys for protected pages. It consist of three main modules: 1) migration data protection module, which is used to encrypt ,decrypt and intercept protected processes or pages during migration operation 2) meta data management module, used to manage (migration and reconstruction) metadata (encryption keys, process identities etc) at receiver end after migration process 3) security guard provide security during live migration operation[17].

C. LIMITATIONS OF EXISTING SOLUTIONS

Isolated Migration Network: It only segregates the migration traffic from network traffic. It gets more complex and administrative cost increased with population of VM's [6, 8].

Network Security Engine-Hypervisor (NSE-H): NSE-H based approach does not support any of the security requirements for VM migrations depicted in Table II [6].

Role based secure migration: It cannot be integrated with current deployed infrastructure because changes are required at software and hardware levels. Live migration is not supported in this approach [6, 9].

Secure VM-vTPM: Live migration is not supported in vTPM based migration protocol. Keys of vTPM are also stored outside the TPM, therefore prone to leakage and unauthorized modification. The vTPM state is also migrated, so it is an overhead and it increases the migration time [6, 10].

Improved vTPM migration Protocol: Live migration is not supported in vTPM based migration tools. The vTPM state is also migrated along with VM. It is an overhead and it increases the migration time as well [7].

VM mobility using SSH tunnel: Authorization is not supported in this solution. Furthermore it requires port forwarding on firewalls [11].

Trusted Cloud Security Level (TCSL): This approach does not provide any of the identified security requirements for VM migration. TCSL, isolates the VM's based on their security level in trusted zone of Cloud. TCSL based solutions cannot integrate with existing Cloud Infrastructures. It requires changes in cloud platform for reliable and security features [12].

TABLE II ANALYSIS OF EXISTING SOLUTIONS AND APPROACHES

Security Requirements	Paper reference Number									
	[6]	[6]	[9]	[10]	[7]	[11]	[12]	[13]	[14]	[17]
Integrity verification of platform	×	×	✓	✓	✓	×	×	×	✓	×
Authenticati on of platform	×	×	×	✓	✓	✓	×	✓	×	×
Authorization	×	×	✓	×	×	×	×	×	×	×
Confidential ity and Integrity	×	×	✓	✓	✓	✓	×	✓	✓	✓
Replay Resistance	×	×	×	✓	✓	✓	×	✓	✓	✓
Source Non-Repudiation	×	×	×	✓	✓	✓	×	✓	✓	×

Secure Migration using RSA with SSL Protocol: RSA based authentication required public keys of all hypervisors for authentication in migration process. It makes management of Public keys difficult. This approach does not comply with security requirements as shown in Table II [13].

Trust Token based migration: It gets complex as a number of user simultaneously perform VM migration in Cloud. TAL value is dependent upon on hardware and software components of platform so a little change in platform requires new TAL value signed by PTTA. It will also degrade performance because TPM is main bottleneck in this solution. Furthermore, it does not support the live VM migration process [14].

Protection Aegis for Live Migration of VM's (PALM): It increases the downtime by migrating metadata along VM. Furthermore it does not provide authentication/authorization security features [17].

V. CONCLUSION AND FUTURE WORK

Live VM migration is useful feature but it introduces security risks in traditional data centers as well as in Cloud environment. In this paper, we have investigated the vulnerabilities and threats on the live VM migration. Furthermore, we have defined security requirements for the detailed analysis of existing solutions and explored their limitations. There is no complete solution for live VM migration which fulfills the aforementioned security requirements. Furthermore, live migration is not supported in vTPM based solutions. In Our future work we will propose a solution for live migration that fulfills the security requirements as well as easily integrated with existing Cloud infrastructures.

REFERENCES

1. K. Hashizume, D. G. Rosado, E. Fernández-Medina, and E. B. Fernandez, “An analysis of security issues for cloud computing,” Journal of Internet Services and Applications 2013.
2. P. Mell, T. Grance, 'The NIST definition of cloud computing". NIST,Special Publication 800–145, Gaithersburg, MD.
3. J. Oberheide, E. Cooke and F. Jahanian, “Empirical exploitation of live Virtual Machine migration”, Proc. of BlackHat DC convention 2008.
4. V. Vaidya, "Virtualization vulnerabilities and threats: a solution white paper", RedCannon Security Inc, 2009. http://www.redcannon.com/vDefense/VM_security_wp.pdf.
5. Steve Orrin, Virtualization Security: Challenges and Solutions, 2010. http://365.rsaconference.com/servlet/JiveServlet/previewBody/255 5- 102-2-3214/STAR-303.pdf.
6. 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.
7. 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.
8. OpenStack Security Guide, 2013. http://docs.openstack.org/security- guide/security-guide.pdf.
9. 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.
10. B. Danev, R. J. Masti, G. O. Karame and S. Capkun,“Enabling secure VM-vTPM migration in private clouds”, Proceedings of the 18th Annual Computer Security Applications Conference, December 05- 09, 2011, Orlando, Florida.
11. 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, 2011, Haifa, Israel.
12. Y. Chen, Q. Shen, P. Sun, Y. Li, Z. Chen and S. Qing, “Reliable migration module in trusted cloud based on security level – design and

implementation", International Parallel and Distributed Processing Symposium Workshops & PhD Forum 2012.
13. V. P. Patil and G.A. Patil, "Migrating process and virtual machine in the cloud: load balancing and security perspectives," International Journal of Advanced Computer Science and Information Technology 2012, vol. 1, pp. 11-19.
14. M. Aslam, C. Gehrmann, M. Bjorkman "Security and trust preserving VM migrations in public clouds", International Conference on Trust, Security and Privacy in Computing and Communications 2012.
15. P. Botero, Diego "A brief tutorial on live virtual machine migration from a security perspective", University of Princeton, USA.
16. A. Rehman, S. Alqahtani, A. Altameem and T. Saba, "Virtual machine security challenges: case studies", International Journal of Machine Learning and Cybernetics: 1-14, April 2013.
17. F. Zhang, Y. Huang, H. Wang, H. Chen, B. Zang, "PALM: security preserving VM live migration for systems with VMM- enforced protection", Third Asia-Pacific Trusted Infrastructure Technologies Conference, 2008.
18. 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.