Secure Live VM Migration in Cloud Computing: A Survey

Suresh B.Rathod
Research Scholer
K.L.University, Green Fileds
Vaddeswaram, Vijayawada

V.Krishna Reddy, PhD
Professor
K.L.University, Green Fileds
Vaddeswaram, Vijayawada

ABSTRACT
Cloud computing (CC) refers to delivering applications, platform used to execute user application and Infrastructure to fulfill user hardware requirement as a service over internet. Virtual Machine (VM) is normally stored on Datacenters who consist of set of physical servers where VM is executing to fulfill service when gets accessed by end user. VM controlled by hypervisor also termed as VM Monitor (VMM). VMM manages VM execution, decides which VM to be selected for migration and how VM to be migrated. VM migration can be done by considering centralize VM migration or distributed approach. Once Migration decision done a caution need to be needed whether a VM to be transferred is free from attack, and the destination where VM is about to migrate is safe to execute on destination server. Considered a VM page is open to attack, it can be compromised by end world, also a destination server.

General Terms
Cloud security, VM migration.

Keywords
Keywords are your own designated keywords which can be used for easy location of the manuscript using any search engines.

VM, VMM, server, migration, CC.

1. INTRODUCTION
Cloud computing is gaining more popularity by providing services over internet, where user is going to be charged based on amount of bandwidth it consumes and time of accessing services. The services can be of software, a platform for application creation or execution, or an Infrastructure in the form of network, hardware etc. The CC has basic architectural structure is given in figure 1.

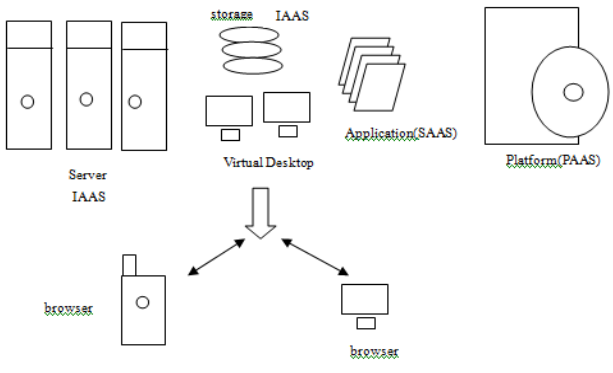

fig.1.cloud computing component

CC can be deployed by using either of following cloud types.

- Public cloud
- Private cloud
- Hybrid cloud
- Community cloud

Public cloud: - This is a cloud where all services from cloud service provider is being publicly available. Like amazon, google are some examples of this type of cloud.

Private cloud: - This is a cloud where services being available to within organization. Here no service being shared to public domain. Eucalyptus is one cloud platform where user can create its own private cloud.

Hybrid cloud: - This type of cloud where a private firm or organization can share its services to public cloud.

Community cloud:-It is multitenant environment where computing resources and services gets shared between set of organization in common goal. The goal can be improving performance of a particular service over a specific region or time. This paper gives different techniques available to a selecting VM for migration, threats associated in VM migration.

2. VIRTUALIZATION
Virtualization provides isolation of operating system from underlying hardware. Virtualization type includes network virtualization, Server Virtualization, Storage Virtualization and Operating System Virtualization.

Network Virtualization: In this type of virtualization a physical network would be virtualized such that user feel it has dedicated channel or link is assigned for him. The virtualization can be achieved by splitting total bandwidth into channel and allowing each user to have access over channel instead of whole bandwidth.

Operating System Virtualization: In this type of virtualization a operating system is virtualized such that multiple instance of operating system runs simultaneously on a physical server, and can get access to multiple instances for running applications. In this type of virtualization a user just types a command its service will be fulfilled by different instances of operating system running on same physical server.

Storage virtualization: In this case of virtualization a logical storage is created by hiding physical storage over network or local to the server. Storage involves set of data centers who store data physically over servers residing local to data centers or distributed over multiple servers in data centers. The virtual data storage is created by first collecting data from multiple data centers and collectively form a storage called virtual storage [17].

Server virtualization: In case of server virtualization a host machine provides an environment where a VM can be executed on physical host machine along with many guest VM with their own operating system. VM migration is easy as compared with process migration where in process migration a host system has to be in existence only a process need to be migrated towards remote location and has to get back in execution to physical source while using network for resolving system call or resources from remote location. VM migration involves VM itself to be migrated towards the destination host and get freed by originating host. Virtualization plays basic role in CC, where physical resources being offered to end user by creating its virtual image. The VM's are portable and can be easily transferred to many locations. The VM need to be executed on a layer called as hypervisor. The layer may be along with an operating system or can be run on hardware itself. The physical resource can be a storage, network, device an operating system. In modern Data centers for Cloud environment, virtualization has been considered the basic of resource management technology.

3. VIRTUAL MACHINE MANAGEMENT

VM can be managed by It is a piece of code that runs as computer software, firmware or hardware that creates and runs VM. A computer system that runs one or more VM termed as host machines. Each host termed as guest machine. The hypervisor presents a virtual operating platform to end user and manages the execution of guest machine. Multiple VM shares same underline hardware resources. The hypervisor can be classified as

Type-I (native hypervisor): This type of hypervisors runs directly on the host's hardware. It runs on top of the hardware and controls hardware and manages guest operating systems. Following example demonstrates the native hypervisor.

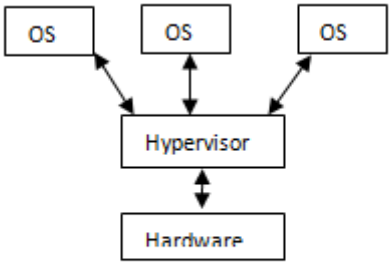

Fig.3 Type-I

Type-II (Host based): This type of hypervisor a runs within an operating system. It runs on top f operating system. It provides illusion of system by running on top of operating system as a component of an operating system. Following figure 2 illustrates mechanism of host based hypervisor.

4. VM MIGRATION

The VM migration works by selecting a specific VM from one physical server to other physical server. The migration is such that end user is unaware about a VM, its associated operating system, a network connection. When a VM migration is going on the end user is who is in connection with a VM does not change its location, neither has he changed its IP address. Whenever a VM migration process is going it deals steps as listed below.

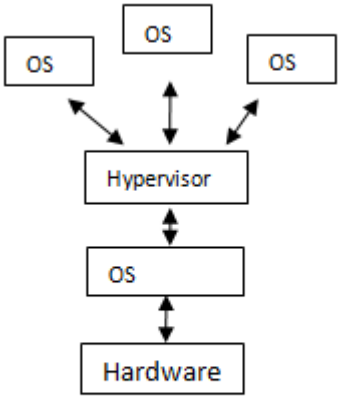

Fig 2 Type-II

- VM state:- preserver state of VM like CPU ,motherboard, network and storage
- External Connection:- preserver USB device attached and removable disks it has
- VM physical Memory: Associated physical memory

VM can be migrated by migrating a memory, a process and network associated to a VM. A disk can be directly copied from source machine to destination machine directly, but interfaces associated to a VM can't be migrated. The interface to memory is memory pages whereas for network an IP. VM should preserve its previous IP address. In a clustered environment a request to translated VM can be resolved by ARP protocol. ARP redirects a particular request on specified host where VM resides.

VM migration can be achieved by static VM migration or Dynamic VM migration to fulfill SLA agreement. In static VM migration, the required resources gets selected as per requirement in SLA, but in the case of dynamic VM provisioning, the resources being used for VM can be changed dynamically to handle unexpected workload change. In case of static VM migration allocated resources may not be fully utilized as some VM might not use allocated hardware resource that leads to wastage and those can't be taken away from the physical server as being mentioned in SLA. Dynamic VM migration works by assigning and taking resources done dynamically as change in load to a server.

Virtual Machine Migration Technique: Memory migration in CC done by following three phases

Push phase: in this certain pages of VM are pushed in network while VM still stays in running stage. To ensure consistency across the pages which are modified on host machine gets resent to the same destination.

Stop and copy phase: In this the execution of VM at source system is stopped; the pages of VM are transferred to the destination. The VM gets resumed at destination and starts providing services.

Pull phase: In this source system starts running on system; if it requires certain pages those can be faulted across the network.

Most of migration strategies use either of above phase or in combination of above phase. Author [2] has explained how VM can be migrated by using either of techniques like,

- **Pre-Copy:-**This is a combination of push phase and stop and copy phase where some of pages from VM gets transferred to the destination, VM still runs on source server, pages which are still on source system are termed as dirty pages which are transferred to destination as of jobs gets completed. VM execution halted at source and transferred to destination. Here stop and copy phase being used. In each round of pre-copying, the original host machine that holds VM, copies memory data of a VM that will be migrated, and sends the data to the receiving machine that is a system where new machine need to executed. In the mean time, the host that is a server where VM is currently running, records the changed bits of memory. These dirty bits are gets generated by the running applications in the VM. The dirty bit need to delivered to the destination system in next rounds. If the rate of dirty bit generation is lesser than total available dirty bits. The host system then suspends VM execution at host machine and copies all dirty bit at last round to destination host.

- **Post-Copy:**- In this VM's CPU state has already been transferred to the target and resumed. In this VM suspends its execution at source side. The migrating VM at source side copies minimal VM processor state to the target system resumes targeting node, and begins fetching memory pages from the source over the network.

5. APPROACHES FOR VM MIGRATION

5.1 Centralized VM migration

In this type of migration approach a centralized controller who controls VM selection, and distributing VM from heavy loaded server to low loaded server. Hear load means high cpu utilization or high power consumption. Initially when cloud is being configured VM can be distributed randomly to several physical servers. Clusters can be formed by grouping physical servers termed as region.VM gets transferred within server of same cluster or in between clusters. The clusters can be collocated on same data center or in between data centers. VM migration achieved by sending probe message from each physical server to a centralized controller physical server (CCS). Central controller receives messages at fix set of intervals, each message contain name of physical server, region where it belongs to and load information that it has. The CCS maintains a threshold value being used to take decision which VM need to selected for transmission and where it need to transmitted. The problem with this approach is that each server sends control message at fi set of interval only, what else if certain server gets full utilization and unable to provide service to executing can cross threshold value of CPU utilization and poser consumption.

5.1.1 Decentralized VM Migration

In this type of migration approach each physical server maintains a record for each server in active cloud running several VM. Decision for VM selection and migration for each server could be managed by controller residing along with VM In each physical servers. Each server broadcast messages to all participant physical servers at specific interval of time asynchronously. Each server updates information of each server who is participated in forming cloud to provide service to end user.

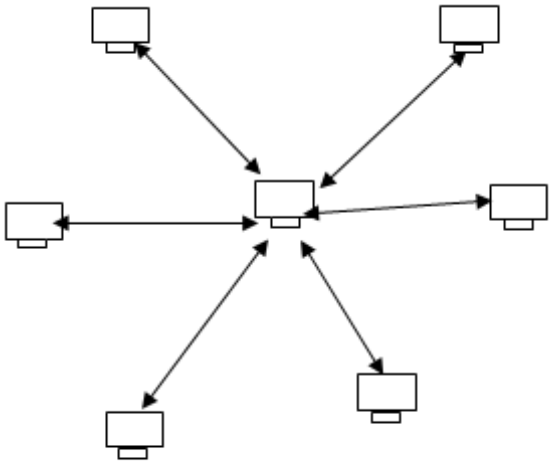

Fig.4 Centralized VM migration

The message contain information like cpu utilization, power consumption etc of each servers. Whenever a server is being full overloaded he starts VM migration process. Before migration decision taking place it first finds record of each server which server is under loaded or heavy loaded. The controller residing at server will selects low loaded server and start migrating VM to low loaded server, informing all participant server in migration process. Author [10] has given a approach for decentralized VM migration where each physical node maintain a table consisting of each servers utilization information Whenever a server is under heavy load it uses its table entry information to find out which server is under heavy load or under below average load. Following figure shows decentralized VM management.

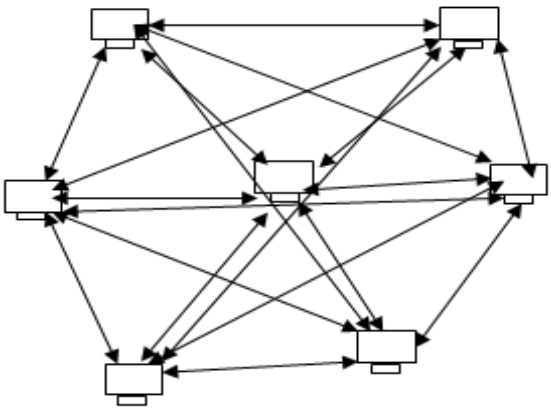

Fig.6 Decentralized VM Migration

6. SECURITY ISSUES IN LIVE VM MIGRATION

VM can have following issues that arise during VM migration.

Access Control: An incomplete and inappropriate access policy over VM can lead to unauthorized user to initiated live VM migration, abort migration. An unauthorized user might insert a malicious code in VM and can use same for getting access over other VM; also can use same VM to launch attack and compromise destination host where it is about to migrated and getting executed.

Authentication: Cloud service provider provides service using VM. Initially VM gets distributed to multiple servers by cloud service provider to provide services to different regions. There are multiple cloud service providers where cloud user subscribes services from multiple service providers. User signs SLA for each type of service. As cloud service provider uses to replicate data over multiple servers, user needs to get access for each server using login credentials given by service provider. When user tries to get access he needs to provide login credential over servers and have to authenticate from each servers for each service. These redundant actions may exploit user credentials over internet..

Data Confidentiality: VM migration involves control messages need to be exchanged in between hypervisors executing on host and destination; these messages are normally in text format. As there is network involve in communication between hypervisor an intruder can easily get access over control messages and can initiate or stop VM migration. VM consist of data, when VM migration initiated the data along with VM state need to preserved, but the pages never encrypted or decrypted The data which involves in migration appears clear text data over internet. So data gets visible to attacker where he can misuse or change content of data also can retransmit modified state data to the destination host.

Accountability: CC needs a mechanism where user and VM should be monitored frequently, because in case of down time or in case where VM gets malfunctioning, user might lost its content and can blame over service provider regarding data loss or data theft. A monitoring mechanism should be inculpated over CC where whenever VM migration process done using auto or manually; log of each action from user and VM should be maintained.

Data Integrity: Data integrity is one of the major issues in VM migration. Transmitting data over network involves intruders who can directly access data over network. The data over network goes in the form of text, which can be easily captured over network and content of such might altered by the intruder. A packet in network gets captured by user and can generate a false request over network to initiate VM transmission and can halt execution of VM.

Availability: Once attacker gains access over physical host by finding vulnerabilities, it might initiates large number of VM migration to intended host where attacker has interest. Doing this causes destination host to be over loaded. Overloading a host lead to downgrading performance of host and generates large amount of traffic over network causing server down and ultimately not allowing legit imitate user to gain access over service.

Privacy: one of the features of CC is that it maintains transparency to VM migration. The VM gets migrated without user understanding users who stores data or access data from VM. The VM migration might involves passing nation boundaries; each nation has their own laws that lead to open access to user data.

7. SECURE VM MIGRATION

Security is one of major issue in cloud computing.CC provides service over internet; it might be possible that on using a type of CC user can lose its sensitive data in internet or towards cloud service provider. Through virtualization the resources can be easily consolidated, partitioned, and isolated [11].

Virtualization has following characteristics.

- Partitioning
- Isolation
- encapsulation

Partitioning: Many application and operating system can run on same physical system without interrupting to other application execution or operating systems services.

Isolation: Each machine in cloud is isolated such that if one of machine is infected with virus or gets crashed, whole system never gets infected.

Encapsulation: Encapsulation protects each application such that no application can interfere in other application execution..

VM execution gets managed by hypervisor which runs on top of hardware or along with operating system. VM is transferred to the destination as of pre copy or post copy approach. When a VM is being transferred towards destination it goes through internet which is full of viruses and filled with lot of intruders. An attacker can monitor the traffic and launch a man in middle attack, also the VM to be migrated at remote location might not be secure, so the migrated VM might be prone to various attacks or it may malfunction. To overcome that Author [2] has discussed various types of solution that can be applied to secure the VM migration towards end system .Author [12] has discussed an approach where hash code is being added to each VM that can be used to authorize VM towards destination host. Unlike any software hypervisors are robust and secure, they might have vulnerabilities which can be easily exploited by attacker. Guest OS executes on top of hypervisor, as the hypervisor has its own policy called as isolation where each machine execution is isolated from other guest OS. Hypervisor has its own level of security parameters where it can judge executing guest OS based on set of policies defined as cloud vendor. If it finds any guest OS doing malfunctioning, a guest OS execution can be stopped by hypervisor. But the problems arise if hypervisor itself gets compromised. If hypervisor gets crashed all system will be crashed. Author [13] has discussed an approach to provide security to hypervisor and VM where he discussed how HREM and HSEM component being utilized to do monitoring and reliability checking. Where HSEM is host based security model who just monitor each VM behavior and HSREM responsible to checking reliability, each VM residing on each hypervisor. Author [14] has discussed hypervisor based security where he explored secure booting process can provide security to hypervisor also he has explored ways to provide security to I/O call between hypervisor and guest OS. The authors in [15] have discussed the CoM framework for a secure VM migration. Author [15] has discussed framework

using the concept of hypervisors where he termed as Network Security Engines hypervisor (NSE-H). He has discussed NSE as IDS with firewall to remove intrusion which occurred in virtual environment. The CoM framework uses IDS in order to work in context of live migration.

8. CONCLUSION

Live VM migration can be done by either central or decentralize mechanism, where security is more critical issue. Security to VM should be done in order to provide secure live migration. This paper discusses various issues associated with Live VM migration and associated solutions.

9. ACKNOWLEDGMENTS

We would like thank the department of Computer Science and Engineering, K.L. University for undertaking this research. The help and assistance provided by them is quite inspirational.

10. REFERENCES

[1] Chunxiao Li, Anand Raghunathan, Niraj K. Jha "Secure Virtual Machine Execution under an Untrusted Management OS" 2010 IEEE 3rd International Conference on Cloud Computing.

[2] Diego Perez-Botero "A Brief Tutorial on Live Virtual Machine Migration From a Security Perspective" International Journal of Computer Applications International Journal of Computer Applications.

[3] K.Mukherjee "A secure Cloud 2010," International Conference on Recent Trends in Information, Telecommunication and Computing.

[4] Wei Wang, Xiaoxin Wu, Ben Lin, Kai Miao, Xiaoyan Dang "Secured VM Live Migration in Personal Cloud," IEEE, 2010.

[5] Flavio Lombardi a, RobertoDiPietro b,c, "Secure virtualization for cloud computing"

[6] Mahdi Aiash, Glenford Mapp, Orhan Gemikonakli "Secure Live Virtual Machines Migration: Issues and Solutions".

[7] Tom Liston, Senior Security Consultant – Intelguardians Handler – SANS Internet Storm Center "On the Cutting Edge: Thwarting Virtual Machine Detection".

[8] Jie Zheng, T. S. Eugene Ng, Kunwadee Sripanidkulchai, Zhaolei Liu "Pacer: A Progress Management System for Live Virtual Machine Migration in Cloud Computing," IEEE transactions on network and service management.

[9] NIST "Guildeline on security and proivacy in public cloud computing," December 2011.

[10] Xiaoying Wang, Xiaojing Liu, Lihua Fan, and Xuhan Jia "Research Article:A Decentralized Virtual Machine Migration Approach ofData Centers for Cloud Computing," Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 878542.

[11] Hai Jinn, WeiGao , SongWu, XuanhuaShi , XiaoxinWu,FanZhou "Optimizing the live migration of virtual machine by CPU scheduling,**"** Journal of Network and Computer Applications 34(2011)1088–1096.

[12] Chunxiao Li, Anand Raghunathan, Niraj K. Jha **"**Secure Virtual Machine Execution under an Untrusted Management OS**"** 2010 IEEE 3rd International Conference on Cloud Computing.

[13] Farzad Sabahi "Secure Virtualization for Cloud Environment Using Hypervisor-based Technology" International Journal of Machine Learning and Computing, Vol. 2, No. 1, February 2012.

[14] Yueqi ang Cheng Guardian: Hypervisor as Security Foothold for Personal Computers M. Huth et al. (Eds.): TRUST 2013, LNCS 7904, pp. 19–36, 2013.c©Springer-Verlag Berlin Heidelberg 2013.

[15] C. Xianqin, G. Xiaopeng, W. Han, W. Sumei, L. Xiang. Application- Transparent Live Migration for virtual machine on network security enhanced hypervisor. Research paper. China Communications. Page 32 42, 2011.Jenni Susan Reuben "A Survey on Virtual Machine Security," TKK T-110.5290 Seminar on Network Security 2007-10-11/12.

[16] RaviTeja Kanakala, V.Krishna Reddy, K.Thirupathi Rao "Analysis on Virtualization Technologies in Cloud," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) , Volume 3 Issue 7, pp 2567-2574, July 2014.