Volume 4, Issue 2, February 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Live-VM Migration Policies, Attacks & Security – A Survey

Shweta Rajput, Trupti manik
Computer Science and Technology
L.D College of Engineering
Ahmedabad, India

Abstract— Cloud Computing enables shared pool of IT resources as service. Cloud computing facilitate Virtualization through which it increase the provider 's density which turn into better server utilization, multi- tenancy and great profit margin. Virtualization provides an essential feature "Live-VM migration" which provides the capability to balance the load, system maintenance and fault tolerant, etc. There are many approaches for Live-VM migration like Pre-Copy, Improved Pre-Copy; which aimed to minimize the downtime and total migration time. When VM is migrated from one host to other host machine the data are susceptible to be attacked due to incongruous access channel, vulnerabilities in hypervisor and unsecured network routes. An attacker may gain privilege on migrated VM and divers it on untrusted host; it may overwhelm the legitimate destination host and may drip the information. To mitigate this situation VM access policies must define properly like who has right to migrate it, Strong encryption techniques or properly configured firewalls.

Keywords— Live migration, VM Migration, Security, cloud computing

I. INTRODUCTION

A. CLOUD COMPUTING

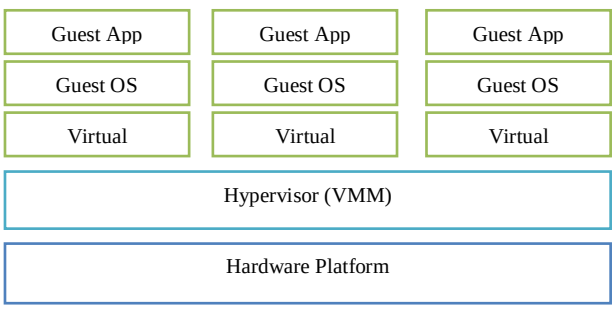
Cloud computing enables IT resources as a service, providers are developing a shared pool of configurable computing resources, which customers can dynamically provision and release on demands payable basis. Providers can reuse computing resources, and consumers reduce costs through on demand resource provisioning thus both provider and consumers get profited [1]. Cloud computing has three service models and four deployment models. A Service model includes Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a service (IaaS) [1]. Provider & consumer share the control of resources. According to the classical software stack notation In SaaS model service provider provides application as a service. Consumer is capable to use application running on a cloud Infrastructure via internet connection but could not access underlying software building block such as libraries, database, operating system drivers etc. SaaS provider has control at operating system level only. In PaaS model consumer can deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. Consumer has no accessibility to the operating system layer at provider side. Lastly in IaaS model provider enables the consumer to deploy and run arbitrary software, which can include operating systems and applications by provisioning processing, storage, networks, and other fundamental computing resources [13].

A deployment model includes private, public, hybrid and community cloud. A private cloud owns by an organizational for internal use only and exposed to its clients and employees. The public cloud is exposed publically. Hybrid cloud is mixture of private and public clod while the community cloud serves the consumer having shared concerns, such as mission objectives, security, privacy and compliance policy [13].

B. VIRTUALIZATION

Virtualization technologies provide isolation of operating systems from hardware. This separation enables hardware resource sharing. Virtualization can be achieved at different levels. The types of virtualizations are Server Virtualization, Network virtualization, Storage Virtualization and Operating system virtualization. System virtualization is when a single physical host runs a number of VMs on it. This VM has its own applications that run on its OS (guest OS). For the user, a VM behaves just like an independent physical machine.

Figure V-1 Server Virtualization



© 2014, IJARCSSE All Rights Reserved

Virtualization is the essential feature of cloud computing. The benefits of virtualization are well known, including multi-tenancy, better server utilization and data center consolidation. However, virtualization brings with it additional security concerns [3] which will be discussed in section**.**

C. HYPERVISOR

The most essential part of virtualization is the hypervisor or MMU is middleware between the virtualized guest operating system and the real hardware [10]. MMU has two types Type 1 hypervisors run directly on the system hardware and has self-contained operating platform that's why called bare metal hypervisor. Type 2 hypervisors run on a host operating system that delivers virtualization services, such as I/O device support and memory management. As Types1 hypervisor deals with hardware directly virtualization efficiency is higher make it more preferred approach than Type 2. Type1 hypervisors also provide higher performance efficiency, availability, and security than type 2 hypervisors. Type 2 hypervisors are used mainly on systems where support for a broad range of I/O devices is important and can be provided by the host operating system [11].

There are many hypervisor available like Xen, VMWare, KVM etc. Xen is type 1 while KVM is type 2 hypervisor.

D. VIRTUAL MACHINE

Virtual machine (VM) encapsulates an operating system and application in one unit. Server virtualization provide an ability to run entire VM including its own operating system i.e. guest operating system on another operating system i.e. host operating system.

VM can be migrated from one host to other host machine.VM migration is easier than the process migration as process migration suffers from *residual dependency* in which original host machine must remain present and network accessible in order to service certain calls or even memory accesses on behalf of migrated process while after successfully migrating VM the source machine is free [2]. VM migration would to consider three things one to minimize the downtime during which the execution of VM is suspended. Second minimize total migration time, time taken to transfer and activate the consistent copy of VM at destination. There are two kinds of migration cold VM migration and live VM migration.

- Cold Migration – In which VM stop current execution and migrate at destination side. There is no iterative phase in which modified page has to resend. Cold migration minimizes the total migration time but increases the downtime [16].
- Live Migration- In which the VM execution is not interrupted, first some of memory pages are copied to the destination after that VM halt and remaining pages are copied to destination and VM resume the execution at destination [14]. Live VM migration minimizes the downtime. The total migration time is higher compared to cold migration due to iteratively copy the dirty pages which are pre copy before migration [16].

There are many benefits of Live-VM migration includes easy maintenance, separation of concern between consumer and provider, fault tolerant and workload balancing etc. [2]. In this paper, the section II and section III, we discuss live VM migration policies and techniques. Section IV and Section V we layout the breaches in security mechanism and possible attacks due to these breaches respectively. In Section VI presents the security mechanism for migration and evaluation scheme is surveyed. Finally the conclusion and directions of future work are given in last section.

II. LIVE MIGRATION TECHNIQUES

As we previously discussed what is Live-VM migration and its benefits. In this section we go through the techniques which provide these benefits.

A. Energy Efficient Migration Techniques

Cloud computing gaining popularity makes higher no of data centre nodes which consume electricity by servers and their cooling systems [12]. The servers typically need up to 70% of their maximum power consumption even at their low utilization level [4]. Therefore there is a need for migration techniques that conserves the energy of servers by optimum the resource utilization [4] and put maximum number of server on sleep mode [12].

B. Load Balancing Migration Technique

This techniques distribute the load across the physical servers to improve the scalability of physical . The Load balancing aids in minimizing resource consumption, implementation of fail-over, enhancing scalability, avoiding bottlenecks and over-provisioning of resources etc [4].

C. Fault Tolerant Migration Techniques

Fault tolerance allows the virtual machines to continue its job if any part of system fails. VM migration from one host to another is based upon the prediction of the failure occurrences. This technique improves the availability of physical server and avoids performance degradation of applications [4].

© 2014, IJARCSSE All Rights Reserved

TABLE 1LIVE-VM MIGRATION TECHNIQUES & IT'S CATEGORIES

Technique	Categories
Energy Efficient Migration Techniques	1) Threshold based Approach 2) Managing Energy & server resources 3) Energy efficient Allocation 4) Energy efficient management of resources
Load Balancing Migration Techniques	1) Threshold based Approach 2) Resource usage 3) Network bandwidth usage 4) Variation of machine load

III. LIVE- VM MIGRATION STRATEGIES

To make Live-VM migration in clustered environment one should consider physical resources like memory, network and disk [2]. Live-VM migration includes memory migration and resource migration.

A. Resource Migration

Memory can be easily transferred but what about the local resources that are associates to physical machine like disk and network. The challenge is what to do with network resource and local storage. To address network resources, the migrating OS i.e. OS of VM will take care of all it and includes the protocol states and IP addresses. Migrated host generate the ARP reply to advertise the new address in single switched LAN [2].

B. Migrating Memory

There are three phases for migrating memory. A migrating scheme generally uses two of them [2].

- Push phase: in this phase certain pages of source VM is pushed across the destination host while VM is running. The dirty pages are resend for consistency.
- Stop-and-copy phase: The source VM is halt, pages are copied across to the destination VM, and then the new VM is started.
- Pull phase: At the destination host the new VM starts its execution and, if it accesses a missing page that has not yet been copied, this page is faulted in across the network from the source VM.

The memory migration scheme uses one or two from the three phases. Pre-Migration and Improved Pre-Copy algorithm are described as follows.

C. Pre Copy Algorithm

First C. Clark provided the live migration policy using pre-copy approach. For consistent VM image transfer page level hardware protection is used and to control the impact of migration traffic on running service rate-adaptive algorithm is used.

The logical steps for Live-VM migrations using pre-copy algorithm are [2] as following and figure depict the flow of it.

Stage 0. Pre-Migration
Active source host and preselect a target for speed up the future migration.

Stage 1. Reservation
Initially get conformation of availability of required resources then initialize same size VM container on the destination. In case if required resources are not available, VM simply run on source machine.

Stage 2. Iterative Pre-Copy
In very first iteration all pages are copied to destination after that only those pages which get dirtied during first iteration are transferred.

Stage 3. Stop-and-Copy
VM is paused on destination and remaining pages are transferred. Consistent suspended copy is there at both source and destination side.

Stage 4. Commitment
Destination host inform the source of having consistent copy of VM, destination acknowledges this message as commitment of migration process and delete the VM image at source.

Stage 5. Activation
Destination VM is activated in this stage.

© 2014, IJARCSSE All Rights Reserved

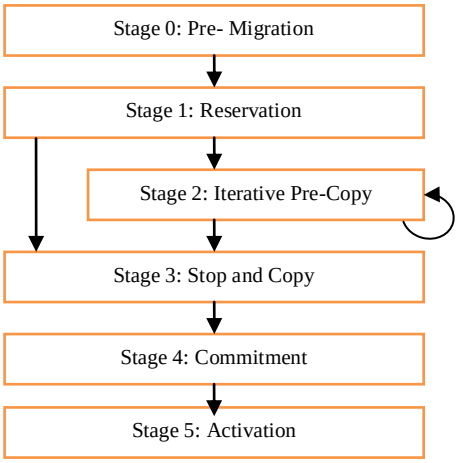


Figure V-2 Flow Chart of Pre-Copy Algorithm

D. Improved Pre Copy Algorithm

Improved Pre-Copy algorithm has same stages as pre-copy. The difference lies in iteration stage. Which Xen page will be migrated is decide by the page's used state which is divided into three categories are described as following [8]:

- TO_SEND**:** marked the pages which get dirty in the previous iteration process, i.e. the pages which need to be transmitted in this iteration.
- TO_SKIP: marked the pages which can be skipped in this iteration.
- TO_FIX**:** marked the pages which need to be transmitted in the last iteration.

The pages of TO_SEND bitmap which updated frequently are mapped to TO_SKIP bitmap and the pages which yet not mapped are stored in TO_FIX bitmap, are transmitted in the last round of the iteration process. A new bitmap TO_SEND_LAST is added records the frequently updated pages which need to be migrated last. The stages stop and copy and commitment contribute to the downtime of VM migration, while total migration time includes downtime and the duration of the stage iterative pre-copy. The improved pre-copy approach is mainly in iterative pre-copy, which first transfers all memory pages, then puts those frequently updated pages into the TO_SEND_LAST bitmap page, and sends those pages out in the last round. Analysis shows that it can complete the iteration process no more than 5 times.

Comparison of Pre-Copy algorithm with Improved Pre-Copy is depicted in tabular form as shown below.

Table 2 Comparison between Pre-Copy & Improved Pre-Copy Algorithm

Mechanism	No. Of Iteration	Downtime	Total Migration Time	Total Transferred Data
Pre-Copy	High	Low	High	Low
Improved Pre-Copy	Low	High	Low	High

IV. SECURITY ISSUES

There are three classes of threats to the migration process [5].

- Control Plane

If an attacker manipulate the control plane of a VMM, it is possible to influence live VM migrations and gaining control of a guest OS. That's why communication mechanisms employed by the VMM to initiate and manage live VM migrations must be authenticated and resistant to tampering. Also, the protocols used in the control plane must be protected against spoofing and replay attacks. A lack of proper access control may allow an attacker to arbitrarily initiate VM migrations.

- Data Plane

The data plane across which VM migrations occur must be secured and protected against snooping and tampering of guest OS state. Passive attacks against the data plane may result in leakage of sensitive information from the guest OS, while active attacks may result in a complete compromise of the guest OS.

- Migration Module

If the VMM component that implements migration functionality is vulnerable, an attacker may able to subvert the VMM and may gain complete control over both the VMM and any guest OSes; that why it must be robust against attacks. VMM must be updated with necessary patches.

© 2014, IJARCSSE All Rights Reserved

Xen's Vulnerability Map in tabular form is given below.

Table 3 Xen Vulnerability [7]

Trigger Source				Attack Vector	Attack Target		
NW	User	OS	Dom0		OS	Dom0	HV
	X		X	Virtual CPUs	X		X
	X			SMP	X		
	X	X	X	Soft MMU	X		X
	X	X		I&T.Mech			X
X	X	X		I/O and NW	X	X	
	X	X		Paravirt. I/O	X	X	
	X	X		VM Exits	X		X
		X		Hyper calls			X
	X	X		VM Management		X	X
X				Rem. Mgmt. SW			X
X		X		HV adds-ons		X	X

Each row illustrates a potential attack path; starting at some trigger source, exploiting a Xen Hypervisor functionality, to attack a set of targets. In each row, the trigger sources are less privileged software entities, while the attack targets are the more privileged software entities, thus enabling privilege escalation [7].

V. THREATS OR ATTACKS

Followings are the threats during Live-VM migration

A. Man-In-Middle Attack

An attacker tries to include some malicious information into on-going conversation between sender and receiver and to have knowledge of the important data transferred between them. In Cloud, an attacker is able to access the data communication among data centres [5] [15].

E. DOS

A denial of service attack involves saturating the target with bogus requests to prevent it from responding to legitimate requests in a timely manner [15]. Due to inappropriate outgoing migration channel is not properly configured than the similarly, by initiating outgoing migrations, an attacker may migrate a large number of guest VMs to a legitimate victim VMM, overloading it and causing disruptions [5]. The occurrence of a DoS attack increases bandwidth consumption besides causing congestion, making certain parts of the clouds inaccessible to the users [15].

F. VM Data Remanence

After successfully VM migration the image left behind known as data-remanence [15] on host must be deleted or encrypted to give assurance that legitimate user cloud not recovers the data [3].

G. VM Diversity

By initiating unauthorized incoming migrations, an attacker may cause guest VMs to be live migrated to the attacker's machine and gain full control over guest VMs [5] [14].

H. False Resource Advertising

In an environment where live migrations are initiated automatically to distribute load across a number of servers, an attacker may be able to falsely advertise available resources via the control plane. By pretending to have a large number of spare CPU cycles, the attacker may be able to influence the control plane to migrate a VM to a compromised VMM [5].

H. Information Leakage

Passive attacks against the data plane may result in leakage of sensitive information. By monitoring the migration transit path and associated network stream, an attacker can extract information from the memory of the migrating VM such as passwords, keys, application data, and other protected resources [17].

Table 4 Attacks & its Mitigation

Attack	Attack Vector	Countermeasure
Man-In-Middle	Unsecured Network route	Proper SSL Configuration or Strong Encryption Algorithm

© 2014, IJARCSSE All Rights Reserved

VM Diversity	Dom0 of Hypervisor	TCCP (Trusted Cloud Computing Platform)
False Resource Advertisement	Access Policy	Properly Configured Firewall Rules
Information Leakage	Unsecured transmission route	VLAN, Proper SSL Configuration or Strong Encryption Algorithm
DOS	Vulnerable Hypervisor, Access Policy	Intrusion Detection System (IDS), Properly defined access Policies rules
Data Remanence	Improper Storage Scheme	Strong Encryption Scheme, Zeroing/Reset or deletion of Left-Image

VI. SECURITY MECHENISM

A. *ROLE BASED LIVE MIGRATION*

The security framework in [6] is based on use of Intel vPro and TPM hardware and provide security solution for un-trusted/open platforms with reliability. The figure 2 below shows high level architecture of role based migration. It includes modules like *attestation service, seal storage, policy service, migration service* and *secured hypervisor.*

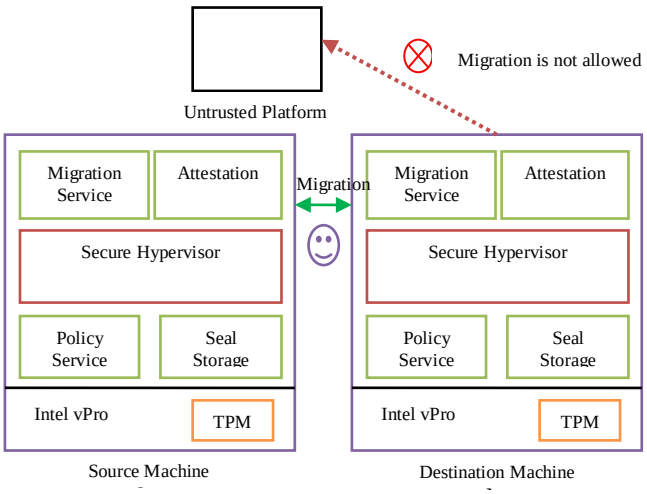


Figure V-1 High Level Architecture of Role Based Migration [6]

Attestation Service module gives confidence to a remote hypervisor by cryptographically identifies running hypervisor which establish trust. *Seal Storage* store private key and role-based policies. Using the private key of the tamper resistant TPM it encrypts the data that is responsible for attestation. A hash of the booted trusted OS is also included with the encrypted data such that the TPM only allows a trusted OS with the same hash to unseal it. *Policy Service* module parses and manages the role-based policies having decisions like who can migrate the VM, to which hosts VM can be migrated. *Migration Service* module is responsible to check whether the target remote machines meet the security requirement before migration if not it does the needful like software updating or patching. *Secure Hypervisor* This module protects the process of guest OS by Runtime Memory Measurement [13]

The steps involved for securing VM migration are first building trustworthy container for VM, second securing VM migrating and third securing hypervisor.

- Building trustworthy container for virtual machine
  Remote attestation first checks the equality of destination VM container's security requirements. If the requirement doesn't meet the back-end cloud will guide to build a trust worthy container with the help of hardware support. After the installation of trusted container, its integrity is checked.
- Securing VM Migration
  The figure shows the detailed steps for role based migration. There are two kinds of migration migrate-out and Migrate-in. In Migrate-out, the owner of VM make request for going outside to migration service module. The request verification done based on pre deployed policy means where it is allowed to migrate or not while in Migrating-In the VM owner initiate incoming request to migrating service module and VM policies are loaded

© 2014, IJARCSSE All Rights Reserved

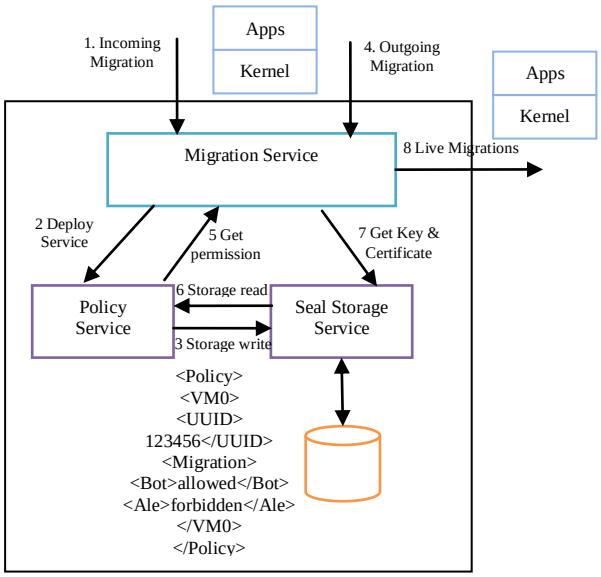


Figure V-2 Role Based Migration [6]

- Securing Hypervisor
  The overall framework uses a secured hypervisor design which uses Intel vPro technology and can hide program's memory from other high privilege system software in a single commodity OS.

B. NETWORK SECURITY SENDBOX

The security framework is based on state full firewall technology and provides both guarantee of distinct security level requirement and full-lifecycle protection for VM [9]. It includes the following agents.

- Security Policies Create Agent (SPCA) – Specifies the security policies of VM when it created.
- Virtual Machine Create Agent (VMCA) – Responsible for VM creation
- Virtual Machine Migration Agent (VMMA) – Responsible to transfer VM instance from one host to another.
- Security Context Migration Agent (SCMA) – Synchronize of Security context of VM with target. VMMA is the responsibility of SCMA agent.
- Security Policies Migration Agent (SPMA) - SPMA relocates the SPs which belong to the virtual machine from the source to the target.
- Security Sandbox Controller (SSC) – Schedules all these five agents.

The three phases of security framework are:

- VM creation phase – The VMCA creates VM instance, and SPCA parses the security needs of the VM and generates the related SPs for the VM so as to customize the security level for the VM as needed. The SSC manages the VMCA and SPCA working in parallel way to ensure that the VM related SPs becomes effective before the virtual network interface card of virtual machine is enabled.
- VM migration phase – SSC triggers the VMMA to migrate virtual machine instance, the SCMA to synchronize the related security context of the virtual machine, and as well the SPMA to resume the SPs on the destination.
- VM destruction phase – SSC destroys the virtual machine instance and removes the related security polices from security engines.

SPCA configures the firewall for hypervisor whether to accept or discard the packet. When the SCMA is disabled, the downloading will be stopped after migration, otherwise the downloading will be continued after a short downtime.

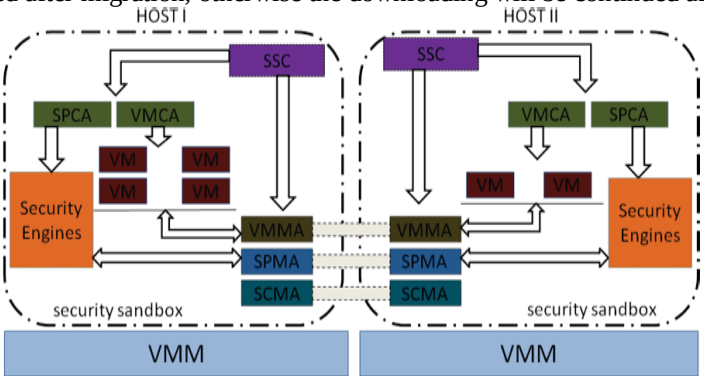


Figure V-3 Architecture of Network Security SendBox

© 2014, IJARCSSE All Rights Reserved

VII. CRITICAL ANALYSIS

Mechanism	Authenticity	Confidentiality	Integrity
Role Based Migration	√	√	√
Network Security Send Box		√	

REFERENCES

[1] P. Mell, T. Grance, "The NIST Definition of Cloud Computing," NIST Spe. Pub. 800-145.

[2] C. Clark, K. Fraser, S. Hand, J.Hansen, E.Jul, C. Limpach, I. Pratt, A. Warfield " Live Migration of Virtual Machins", 2005.

[3] D. Asprey, R. Zhao, K.Balraj, A.Chaudhri, M. Rodriguez, " Security Guidance for Critical Areas of Focus in Cloud Computing", V3.0, Domain 13 Page 157-161, 2009.

[4] P. Leelipushpam, Dr. J.Sharmila, "Live-VM Migration Techniques In Cloud Environment – A Survey", In Proc. IEEE Conference on Information and Communication Technologies,2013.

[5] J. Oberheide, E. Cooke, F.Jahanian, "Empirical Exploitation of Live Virtual Machine Migration", In: Proce. of Black Hat Security Conference,Washington, DC. 2008 http://www.eecs.umich.edu/fjgroup/pubs/blackhat08-migration.pdf .

[6] W. Wang, Y. Zhang, B. Lin, X. Wu, K. Miao, "Secured and Reliable VM Migration in Personal Cloud", In Proceedings of 16th ACM Conference on Computer and Communications Security, CCS, 2009. ICCET, China.

[7] D. Botero, J. Szefer, R. Lee," Characterizing Hypervisor Vulnerabilities in Cloud Computing Servers ",in Proceedings of the Workshop on Security in Cloud Computing (SCC), Hangzhou - China 2013.

[8] Fei Ma, Feng Liu, Zhen Liu, "Live Virtual Machine Migration based on Improved Pre-copy Approach", Beijing – China,2010

[9] G. Xiaopeng, W. Sumei,C.Xianqin, "VNSS: A Network Security Sandbox For Virtual Computing Environment" ,

[10] S. Biedermann, M. Zittel, S.Katzenbeisser, "Improving Security of Virtual Machines during Live Migrations", In Proce Eleventh Annual Conference on Privacy, Security and Trust (PST), 2013.

[11] YamunaDevi. L, Aruna. P, Sudha Devi. D, Priya. N, "Security in Virtual Machine Live Migration for KVM", 2011.

[12] C. Ghribi, M. Hadji,D. Zeghlache, "Energy Efficient VM Scheduling for Cloud Data Centers: Exact allocation and migration algorithms", In Proc. 13th IEEE/ACM International Symposium on Cluster, Cloud, and Grid Computing, 2013.

[13] F. Liu, J. Tong, J.Mao, R.Bohn, J. Messina, L.Badger, D. Leaf, " NIST Cloud Computing Reference Architecture Recommendations", NIST Spe. Pub. 500-292.

[14] H. Tsai, M.Siebenhaar, A. Miede, Yu-Lun Huang, R.Steinmetz, "Threat as a Service? Virtualization's Impact on Cloud Security", Pub. The IEEE computer Society, Page 32-37, January/February 2012.

[15] R. Bhadauria, S.Sanyal, "Survey on Security Issues in Cloud Computing and Associated Mitigation Techniques", September 2011.

[16] Cold Migration and Live Migration , https://wiki.umiacs.umd.edu/VirtualMeshTest/index.php/Cold_Migration_and_Live_Migration

© 2014, IJARCSSE All Rights Reserved