ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S9), 333–339, May 2015* DOI: 10.17485/ijst/2015/v8iS9/65589

Protection of Virtual Machines during Live Migration in Cloud Environment

R. Divyambika* and A. Umamakeswari

School of Computing, SASTRA University, Thanjavur - 613401, Tamil Nadu, India;
divyambika.it@gmail.com, aum@cse.sastra.edu

Abstract

Live migration of Virtual Machines (VM) is a fundamental highlight of "virtualization" that permits transition of a running VM from one physical server to the next without interrupting the VM. The main aim of this paper is to migrate the virtual machines in the cloud environment and thus avoid threats and vulnerabilities. In the previous technique, Protection Aegis for Live Migration (PALM) is used in which the virtual machines migrate in three different methods. They are Process Migration, Memory Migration and Resume/Suspend Migration. The main drawback of the existing technique is the performance degradation due to high downtime. But in the proposed technique, the migration of virtual machines is carried out by using XEN hypervisor which uses Regular and Live Migration techniques. In that XEN hypervisor, the Multi-Pass Algorithm is used to perform migration in an efficient way. When compared with other techniques, the XEN server has an advantage of lower total migration time for virtual machine migration. In earlier live migration, the current execution of running virtual machine is paused and then the VM is migrated to the destination server. After reaching the destination, the execution of virtual machine is resumed. So the migration time is very high. But in proposed method, the current execution of the virtual machine is not paused. The execution of the VM is not interrupted and also the migration time is very low. Also the downtime for migration is reduced by using XEN server. This improves the efficiency and performance by reducing the migration time and down time during live migration of virtual machines. This helps the business providers and industries to increase their productivity.

Keywords: Cloud Computing, Downtime Analysis, Elliptic Curve Cryptography (ECC) Security, Live Migration, Virtualization, XEN Hypervsior Protocol

1. Introduction

Earlier, while using cloud technologies users need to install software with an approved license. It has several limitations and the most predominant one is the time consuming nature while migrating between VMs. In a public cloud, cloud service providers allocate computational and storage resources to clients[1–3]. It is a major task for the cloud platform to maintain the security of data during its life cycle. The main objective is to ensure that one VM failure should not affect the running state of other VMs. Hence, performance enhancement is also one of the important goals in virtualization.

Virtualization gives different benefits in the Cloud; however, it additionally raises security hazards that can influence the Cloud environment. The real virtualization vulnerabilities and dangers that must be considered in the cloud are VM poaching, VM hops and unsecured live VM relocation. In VM poaching, the guest OS takes up more CPU memory. In VM bouncing4, the vulnerabilities of hypervisors prevent the VM from migrating to another server.

Live migration of Virtual Machines (VM) is a fundamental highlight of "virtualization" that permits transition of a running VM from one physical server to the next without interrupting the VM. This relocation ought to be

*Author for correspondence

apparent to the guest OS, servers running on the OS and remote clients of the virtual machine.

During live Migration, there are a few risks in terms of security[5] in a server. Attaining adaptability is troublesome and guaranteeing consistency of all VMs is a basic issue. The research is based on the approaches for live VM migration with vulnerabilities in the relocation process. Also the necessary security in VM relocation, threats and vulnerabilities are also discussed.

2. Related Works

Over the Internet, security cooperation among clients is a critical necessity in a cloud computing environment. The goal is to access the software through on-demand basis via internet without worrying about maintenance issues. To achieve this, a method called flexible, collaborative approach, named CyberLiveApp[6] has been proposed. This allows the user to share live virtual desktop application based on a cloud and virtualization infrastructure.

To support the VM desktop sharing among different clients, a secure access mechanism has been introduced to recognize their perspective benefits, in which window operation events are followed to process hidden areas of windows. An intermediary based window separating mechanism is likewise proposed to share desktops with diverse clients.

Server virtualization is a developing innovation that gives effective resource use and is inexpensive. It combines numerous physical servers into single physical server; thus the hardware resources, physical space, power utilization, cooling limit and man power are saved. This technology in virtualization supports "Green Technology"[7]. This also enhances the security, such as Access control policies, Digital signature, MAC or checksum, Encryption, IDS and Role Based access control[7].

The framework includes defining role based access control policies to safeguard against illegal usage of migration privileges. The firewall is deployed to protect against malicious incoming and outgoing traffic. The reactive intrusion detection system is implemented using an open source intrusion detection system called Snort to protect the system against intrusions and network attacks. Finally, migration is done over a secure encrypted channel to preserve confidentiality of migrating data over the network.

A service called PEACE-VO[8] has been used in business process applications due to the increase in demand of resource sharing and collaboration. This approach is to build virtual organizations which bring a security risk to the participating domains. To find policy conflicts, Full Distribution algorithm has been developed. With this algorithm, sharing domains do not have to disclose their full local privacy policy. Two protocols were proposed for VO management and authorization. This can be successfully implemented in the CROWN[8] test bed. This method is efficient, but lacks security features.

3. Issues in Threats and Vulnerabilities

Initially the VM migration cannot encrypt the data to be transferred from one host to another. So, the intruder can easily access the content and modify it. This is called as man-in-the-middle attack which is shown in Figure 1. Thus an adversary eavesdrops the confidential data and replays them. Therefore, secure and endangered channel must be used to diminish snooping and tampering attempts on migrating data.

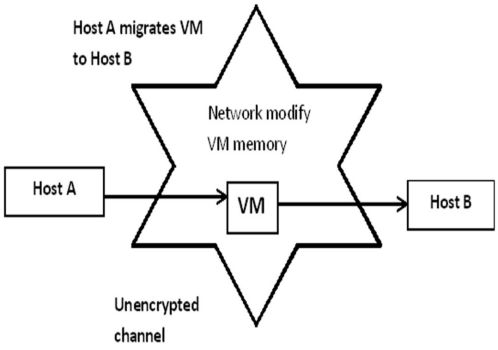

Figure 1. Man-in-the-middle attack.

Some of other attacks are Denial-of-Service (DoS) attack, which is to reduce the performance of services by unauthorized user access; internal attacks are those which send malicious code to target VMM to spoil them; guest VM attack deals with the crashing of VM and gaining control using rough code to send to migrating VM. Thus,

all the attacks and threats should be reduced with the help of some security methods during live migration.

4. System Architecture

4.1 Security in Live Migration

Protection Aegis for Live Migration (PALM) of VM is the security extension which leads to hypervisor-based process protection systems. In this system, the metadata should be marshaled without any threats. There are three different modules described in the VMM[9]. The Data Protector is the authority for encrypting and decrypting contents that resides in the protected processes inside the migrating VM. The Metadata Manager is responsible for arranging the metadata for transmitting and reconstructing them in the migration destination machine. The Security Guard safeguards the live migration system from several security susceptibilities. The approaches are classified into 3 different classes: 1. Process migration, 2. Memory migration and 3. Suspend/resume migration.

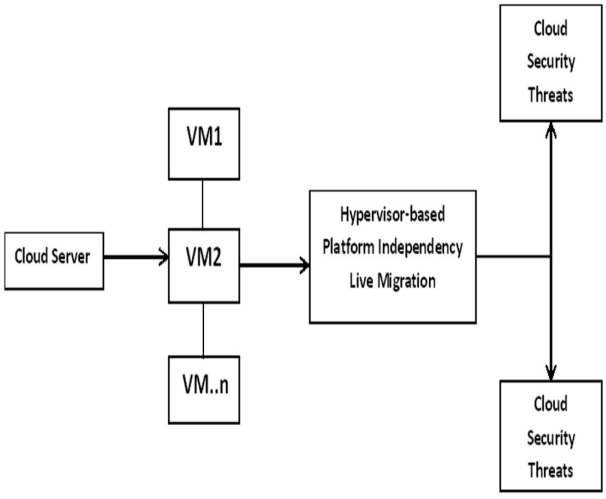

Figure 2. Hypervisor based process protection system architectural framework.

Figure 2 shows the Hypervisor based process Protection System architecture which protects the metadata using cryptography technique and Hashing Algorithm. The secured Hypervisor based process Protection protocol is to identify the various attacks and perform a platform independent migration.

4.2 Process Migration

Process migration is the process of migrating a virtual machine from source host to destination without any threats[8]. These requirements must be incorporated in secure live VM migration process.

4.2.1 Integrity

Before the migration starts, the source must be integrated with the destination and verified whether it is correct target or not. The destination platform cryptographically exhibits its identity to source for trust establishment.

4.2.2 Authentication

An attacker can launch Man-In-The-Middle (MITM) attack using route hijacking or ARP poisoning techniques in the migration process. In order to avoid MITM attacks during live VM migration, source and destination platforms must perform mutual authentication.

4.2.3 Authorization (Access Control Policies)

Appropriate access control policies must be provided to protect the live VM migration process. An unauthorized user/role may launch VM and initiate migration operation. Unauthorized activities can be prevented using access control lists (ACL's) in the hypervisor.

4.2.4 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.

4.2.5 Replay Resistance

An attacker can capture traffic and replay it later 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.

4.2.6 Source Non-Repudiation

Source host cannot deny the VM migration operation. This feature can be achieved by using public key certificates.

4.3 Memory Migration

Some of the extensions are added to the live migration to increase the confidentiality inside the migrating VM. Confidentiality protection involves encryption. Memory migration is carried out in two phases: Pre-copy, Stop-and-copy.

4.3.1 Pre-Copy

In the pre-copy phase, the memory pages are mapped by the Migration Manager (MM) and the entire memory of the migrating VM is sent. It maps a set of pages in its memory space, sends the pages, unmaps the batch and maps the next batch until all pages are sent. As the migrating VM is still processed in this phase, some of the pages sent earlier are dirtied again. The VMM tracks the dirtied pages and reports to the MM and resets the VMM tracking records and starts a new round to send these dirtied pages. The fault is handled by the Data Protector in the VMM. The Data Protector encrypts the content of the protected page.

4.3.2 Stop-and-Copy

When the pre-copy threshold is reached, the MM suspends the VM and transmits the remaining states. Two steps are added after the MM sending the remaining dirtied pages. It invokes a newly added hyper call to retrieve protection metadata and transmits them. The hash values collected with the keys should be encrypted again using the session key before passing them to the MM.

4.4 Resume/Suspend Migration

After accepting all the memory pages, the VM picture resumes on the target machine. As the reassembling methodology is under the control of the MM, it may swap the substance of two secured pages of an ensured procedure. This is conceivable as VM image is not hashed as a whole.

5. Analysis of Existing Solutions

The peculiarity of reusing domain policy can help virtual machine association to focus on the existing solutions. The limitations of a distributed policy[8] are the occurrence of conflicts during the execution of security checking, as well as possible threat and single point of failure problem.

In CyberLiveApp[6], a multi-user accessing mechanism and controlling viewable desktop areas are provided at the application window granularity. This can also enable/disable input devices such as the mouse and keyboard. The main disadvantage is the occurrence of network traffic overhead during desktop sharing between different VM. If VM increases, the system process slows down and gets hanged.

In isolated migration network approach, source and destination VMs are grouped in Virtual LAN (VLAN)[5]. It isolates the migration traffic from other network traffic. Segregation of migration traffic will reduce the risk of exposure.

6. Implementation

Advancing business needs around cloud applications and cell phones and the need to reduce expenses require completely new considerations for access control. To overcome the existing limitations, Elliptic Curve Cryptography (ECC) and also XEN hypervisor technique with the iterative Multipass algorithm have been used. XEN hypervisor is used to migrate the VM in different physical servers. This method is easier for clients to achieve better availability and less migration time. Hence the possible threats and attacks are also reduced by ECC. Good performance, better migration time, confidentiality and integrity will be achieved on virtual machines during live migration by applying these techniques.

6.1 Elliptic Curve Cryptography

ECC is the advanced method in public key cryptography. It provides a considerably more secure foundation than earliest public key cryptography systems like RSA. One of the primary advantages in examination of non-ECC cryptography is the same level of security[7–9] which is provided by the keys of smaller size.

Benefits of ECC technique:

- Smaller keys, cipher text and signatures.
- Very fast key generation.
- Fast signatures.
- Moderately fast encryption and decryption.

6.2 XEN Hypervisor

Migration of virtual machines is the ability to save the running state of the VM. This is the basic requirement for all VM migrations[13,14]. So the XEN hypervisor mainly

saves all of this content to a disk and then reboots the virtual machine on a different host server. To achieve this, there are two different methods. One is Save and Restore Migration[15]; another one is Regular and Live Migration. In this paper, the Regular and Live Migration are proposed by using Multipass algorithm.

6.2.1 Regular and Live Migration

Using this method, a copy of VM image and configuration files is needed on each server or a shared storage system can be used to store all VM files. But it is very dangerous to keep multiple copies of virtual machines which leads to corruption.

The steps to followed are:

1. The execution process of virtual machine is paused by XEN host.
2. From the source host, the memory and process information for VM is migrated to the destination server.
3. At the destination host, the execution of a VM is resumed.

Using XEN hypervisor, the amount of time it takes for migration is reduced during the process. But the downtime has not been reduced considerably and thus, client's requirements are not satisfied. To achieve this, an iterative Multipass algorithm is used.

6.2.2 Multipass Algorithm

begin

Initially check whether it has enough resources to run VM from the source server
Initialize the virtual machine memory
end the VM memory to the destination server
WHILE the initial copy of memory is finished
Memory has been changed and sent to the destination server
ENDWHILE
IF the number of changing pages are low
The final state of the VM is transferred to destination host
ELSE
Repeat until all the pages are changed to lower
ENDIF
Transfer the control of VM to new host server.

end

7. Results

The proposed work has been implemented using SQL server and Visual studio 2012 and XEN hypervisor center. XEN server[16] is connected to center to migrate the virtual machine between different servers. Better performance and less migration time can be achieved during VM migration. The client gets registered in XEN server and requests the VM for processing information. But the files in the VM are already migrated by migrator in XEN, so the XEN server automatically redirects the files to new host server to access the VM. Figure 3 shows the migration process from source server to the destination server. When the migrate application file option is selected, a migration that takes place which is shown in the progress bar. After completing process the migration time is displayed in the textbox.

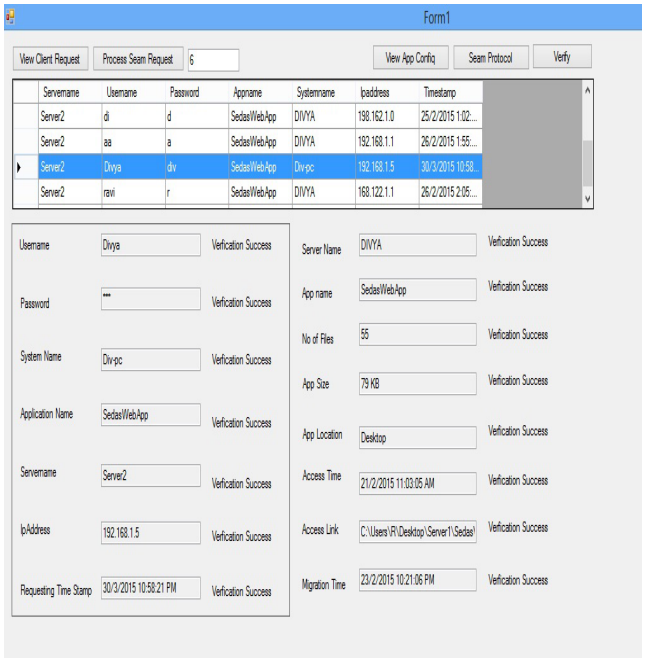

Figure 3. Migration process from source server to destination server.

Figure 4 shows the process of the Migrator in XEN server. When the client chooses the source server to access the VM, the Migrator redirects to the destination server after verifying the request. Finally, it displays the message "verification success" to the client and gives permission to access the files.

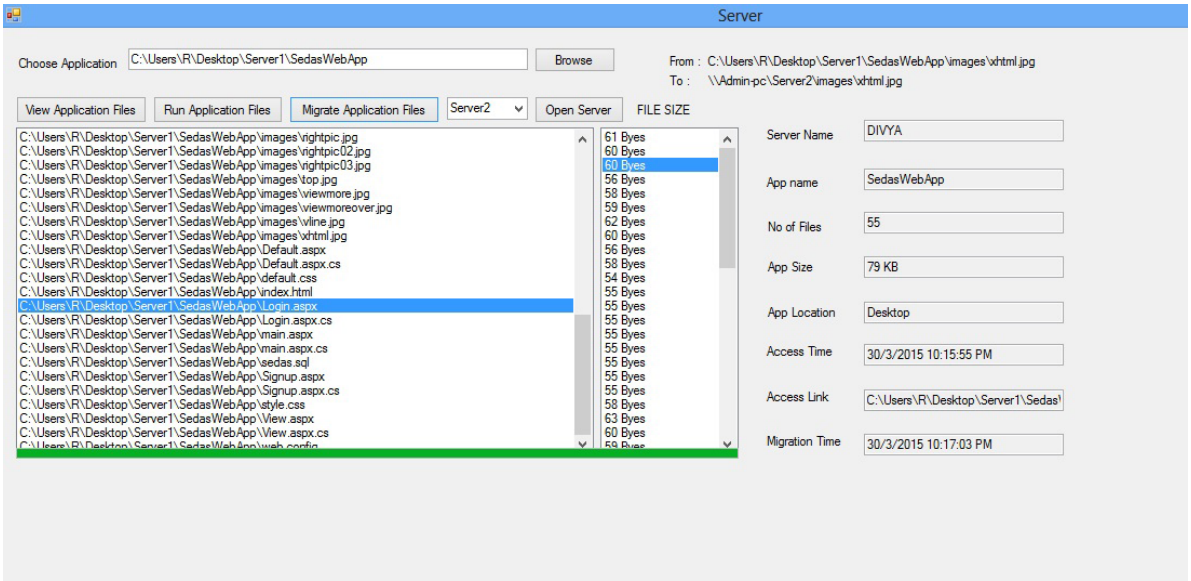

Figure 4. Process of migrator in XEN server.

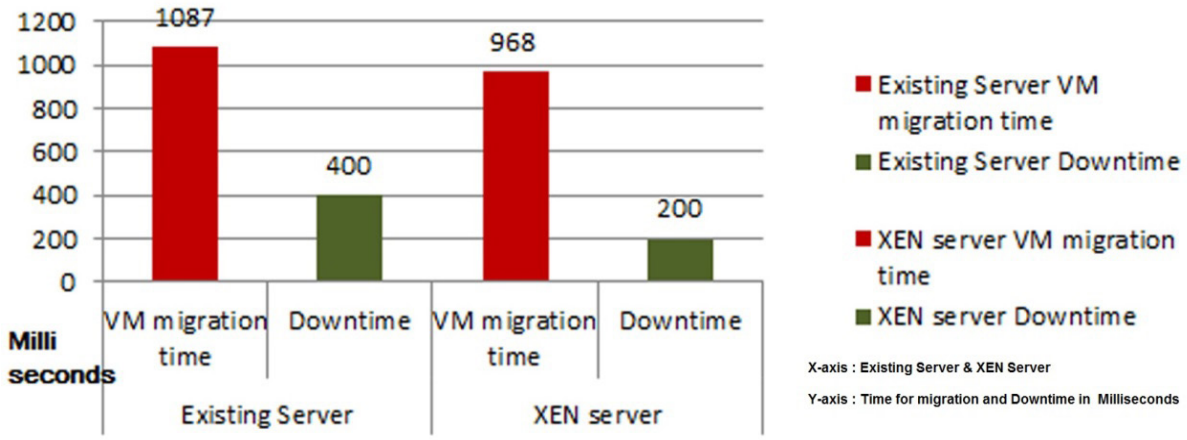

Figure 5. Comparison of existing server and XEN server.

Figure 5 shows the comparison of existing server and XEN server with respect to migration time and down-time in milliseconds. XEN server shows good result when compared to existing and also reduces the threats and vulnerabilities.

8. Conclusion

Live migration facilitates proactive maintenance and optimizes the utilization of available CPU resources. The extension of hypervisor-based process protection system is XEN hypervisor, which migrates the virtual machine with less migration time and protects privacy contents using encryption and hashing. When the Migrator disputes a call to guide a group of memory pages of the relocating VM, at that point the VMM scrambles the secured pages. This will help to reduce the vulnerabilities and threats. Experimental analysis of the techniques indicates the reduction of performance degradation and improvement of the efficiency. In future, the encryption and hashing techniques can be extended with Security Enhanced Application Migration protocol (SEAM) which

provides more security and also increase the performance as well as reduce downtime.

9. References

1 Pal AS, Pattnaik BPK. Classification of virtualization environment for cloud computing. Indian Journal of Science and Technology. 2013; 6(1):3965–71.

2 Neela TJ, Saravanan N. Privacy preserving approaches in cloud: a survey. Indian Journal of Science and Technology. 2013; 6(5):4531–5.

3 Paul PK. Cloud computing based green information infrastructure: the future of eco friendly information science practice. PIJR. 2013; 2(11):122–4.

4 Voorsluys W, Broberg J, Venugopal S, Buyya R. Cost of virtual machine live migration in clouds: A performance evaluation. Cloud Computing; Springer; 2009. p. 254–65.

5 Medina V, García JM. A survey of migration mechanisms of virtual machines. ACM Computing Surveys (CSUR). 2014; 46(3):30.

6 Li J, Jia Y, Liu L, Wo T. CyberLiveApp: A secure sharing and migration approach for live virtual desktop applications in a cloud environment. Future Generat Comput Syst. 2013; 29(1):330–40.

7 Anala M, Shetty J, Shobha G. A framework for secure live migration of virtual machines. IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI); 2013.

8 Li J, Huai J, Hu C, Zhu Y. A secure collaboration service for dynamic virtual organizations. Inform Sci. 2010; 180(17):3086–107.

9 Zhang F, Chen H. Security-preserving live migration of virtual machines in the cloud. J Netw Syst Manag. 2013; 21(4):562–87.

10 Zissis D, Lekkas D. Addressing cloud computing security issues. Future Generat Comput Syst. 2012; 28(3):583–92.

11 Loganayagi B, Sujatha S. Enhanced cloud security by combining virtualization and policy monitoring techniques. Procedia Engineering. 2012; 30:654–61.

12 Fernandes DA, Soares LF, Gomes JV, Freire MM, Inacio PR. Security issues in cloud environments: A survey. Int J Inform Secur. 2014; 13(2):113–70.

13 Clark C, Fraser K, Hand S, Hansen JG, Jul E, Limpach C, et al. Live migration of virtual machines. Proceedings of the 2nd conference on Symposium on Networked Systems Design and Implementation-Volume 2; 2005: USENIX Association.

14 Wood T, Shenoy PJ, Venkataramani A, Yousif MS. Black-box and Gray-box Strategies for Virtual Machine Migration. NSDI; 2007.

15 Dewan P, Durham D, Khosravi H, Long M, Nagabhushan G. A hypervisor-based system for protecting software runtime memory and persistent storage. Proceedings of the 2008 Spring Simulation Multiconference; 2008: Society for Computer Simulation International.

16 Barham P, Dragovic B, Fraser K, Hand S, Harris T, Ho A, et al. Xen and the art of virtualization. ACM SIGOPS Operating Systems Review. 2003; 37(5):164–77.