A Secure live Migration of Virtual Machine using Pretty Good Privacy Minimum Migration in Cloud Environment

Prof. Anurag Shrivastava[1], Prof. Jyoti Sondhi[2], Prabhat Pandey[3]

[1]*Associate Professor*, [2]*Assistant Professor*, [3]*PG Scholar*

Department of CSE, NRIIRT, Bhopal – 462022, India

Abstract- Security features accomplished data security into a Virtual machine represents a threat to the safeguarding of sensitive information and the gathering of intelligence. In this thesis work, I investigate how the encryption technique can be used for sensitive information to provide security in virtual machine during migration within a same datacenter. In this method, I tried to configuring the datacenter, host and virtual machine and then in the next stage tried to allocate each virtual machine to each host. And then we start our simulation process. After that the client/customer sends its request known as cloudlet to their respective VM. The VM process the customer's request, when the utilization of host it overloaded then the VM is migrated from one host to another host. The selection of VM is based on the policy called minimum migration time (MMT) and the allocation of VM is based on the policy called Local Regression Robust (LRR). Before starting the process of migration VM get encrypted by using the PGP (Pretty Good Privacy) technique which includes DES and RSA and then it is migrated from one host to another host within the same datacenter. After the whole simulation we calculate the average time of migration and SLA violation. We implement and study the performance of our algorithms on a cloud computing simulation toolkit known as CloudSim using Random workload data. Simulation results introduce that our proposed techniques provide security in default VM located inside a host designed in CloudSim.

Keywords: Cloud computing, VM placement, Encryption, PGP technique.

I. INTRODUCTION

Live migration is an essential feature of virtualization defined as a process of dynamically transferring running VMs from one physical server to another physical server with negligible or zero downtime and without interrupting services running in VM [4].It is a powerful tool for system administrator and it is required in many cases like online system maintenance, fault tolerance, workload balancing, testing and consolidation of VMs etc. For instance, due to resource conflict the VMs running on the same physical machine may fail to serve continuously so to avoid this failover of the VMs, it is become necessary to live migrate of one or more VM running on one physical server to another physical server to achieve continued and uninterrupted service.

The main advantage of this technique is that multiple VMs can run on top of a single hypervisor, which can make resource utilization much more efficient. our particular interest are on those VMs with high availability requirements, such as the ones deployed by cloud providers, given that they generate the need to minimize the downtime associated with routine operations [2].

Most of the previous work has focused on the implementation of live migration with minute or no consideration towards its security. Unfortunately several vulnerabilities are revealed in the implementation of live migration in Xen, VMware and etc. The major one is the migration protocol that does not encrypt migration data. All migrating data i.e. kernel memory, application state, sensitive data such as passwords and keys etc are transmitted as a clear text. Thus there is a no chance for confidentiality and secrecy of transmitted data.

II. SYSTEM ARCHITECTURE

To evaluate various policies for resource provisioning, load balancing, workload modeling and performance modeling, we needed repeated testing under varying system and user configuration. It is always very difficult to perform these testing in real practice and therefore there is a need of simulation. Simulation is an act of imitating behavior of some process by means of something suitably analogous. Here we have used Cloudsim simulation toolkit [5] for simulating cloud environment.

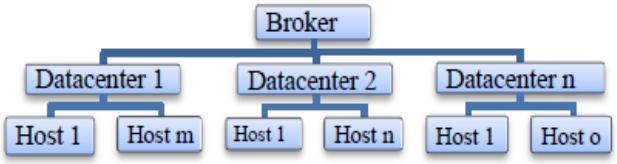

Fig 2.1 Three Level System Architecture

In this work, our system has comprises of number of distributed serving nodes and users that can change their geographic location with time i.e. experiment will be performed on heterogeneous system. To perform working in hierarchical manner, we had chosen three level architecture as shown in figure 1. The first level is the Broker level, whenever a request arrives broker performs the task of datacenter selection on the basis of some parameter like least latency from user or minimum load on

datacenter. Next level is the datacenter level to decide which host will handle the request. Last one is host level where virtual machines are created and Actual processing is done by virtual machine.

III. RELATED WORK

Wei Wang, Xiaoxin Wn, et al. Presented a novel technique to provide a security for the live migration. The technique which they have proposed is called role based live migration. This states that A VM will be either migrated into a host, or migrated out from the host [6].

Ben Lin, Kai Miao, et al. Proposed the overall secure framework which uses a secured hypervisor design that provides the protection on key applications in a Guest VM by utilizing hardware techniques to provide trust services to the software programs. [6]

OS.Sebastian Biedermann et. al. developed a "live migration defence framework" (LMDF). With this framework user can enforce specific security policies targeting unintended but avoidable live migrations [6].

Jamkhedkar P., Szefer J. et al. presented a Framework named security in demand is an infrastructure as a service for clouds. It maps various hardware and software security architecture's properties to cloud which is expected by customers. SLAs and new combinations of security features are designed on the new security architectures [7].

Norshazrul Azman , Hideo Masuda et al. Were performing a live migration under an IPsec implemented transmission channel is indeed secure because the confidentiality and integrity of the migration data remains intact but as penalty, a great amount of CPU overhead is produced due to encryption and packets processing and an increased migration time which decreases the migration performance[8].

Hsu et al, describes the important issue of energy conservation for data centers. We consider the problem of provisioning physical servers to a sequence of jobs, and reducing the total energy consumption. [10]

IV. PROPOSED METHODOLOGY

The main security risk in live migration is the migration protocol that does not encrypt migration data. So to overcome this drawback here we come out with the solution to provide a better security for the live migration of virtual machines. We have implemented our work on CloudSim simulator. To provide a security here we have used the RSA & DES encryption technique.

The basic algorithm of proposed work is as follows:

Step 1: Configure the Datacenter, Host and Virtual Machines.

Step 1: Allocate the host on the Datacenter.

Step 2: Now allocate each virtual machine to each Host.

Step 3: Once it has been decided that a host is overloaded then select particular VMs to migrate from this host. For this purpose, we use Minimum Migration Time policy for virtual machine selection.

Step 4: After a selection of a VM to migrate, the host is checked again for being overloaded. If it is still considered as being overloaded, the VM selection policy is applied again to select another VM to migrate from the host. This is following steps repeated until the host is considered as being not overloaded.

(4.1) The Minimum Migration Time (MMT) policy migrates a VM v that requires the minimum time to complete a migration relatively to the other VMs allocated to the host.

(4.2) The Migration time is estimated as the amount of RAM utilized by the VM divided by the spare network bandwidth available for the host j. Let V_j be a set of VMs currently allocated to the host j.

(4.3) MMT policy finds amount of RAM utilized by VM as per availability of network bandwidth.

Step 5: The VMs selected for migration are allocated to the destination hosts. Before performing the following steps:

1. while(true)

{

Execute the data center

if there is migration due to some issue then,

{

Encrypt the Virtual machine applying DES and RSA and Migrate from previous host to new host

}

else

continue the execution.

}//End While

Step 6: The system finds the host with the minimum utilization compared to the other hosts, and tries to place the VMs from this host on other hosts keeping them not overloaded.

Step 7: If this can be accomplished, the VMs are set for migration to the determined target hosts, and the source host is switched to the sleep mode once all the migrations have been completed.

Step 8: If all the VMs from the source host cannot be placed on other hosts, the host is kept active.

Step 9: This process is iteratively repeated for all hosts that have not been considered as being overloaded.

Step 10: Finally, Obtain hosts and virtual machine map.

V. SIMULATION CONFIGURATION

We have used Cloudsim simulation toolkit for testing our proposed algorithm. A hypothetical configuration has been generated on the basis of results of reference taken for this work.

In this work we have used heterogeneous environment, thus to simulate the process on CloudSim we use the following configuration:

Datacenter: 01

Virtual machine: 50

Host: 50

. Table 5.1 shows datacenter configuration that we have used for our experiments. In this work we have simulated 1 datacenters with variable number of hosts (ranges from 1 to 50) and processing elements (varies from 24 to 27). Table 5.2 gives configuration of host in a datacenter. Each host differs from other on the basis of two parameters namely (i) RAM capacity and (ii) number of processing elements. These parameters have direct impact on number of requests that a host can fulfill successfully. Table 5.3 gives configuration of virtual machine. Response time of any request depends mainly on VM's MIPS i.e. how many instructions a VM can process per second. Response time will be less for VM with large MIPS. In this work we have taken MIPS value from 2000 to 5000.

Object Name	Number of replicas	Number of host in each datacenter	Total PE in each datacenter	System architecture
Datacenter	1	50	24-28	x86

Table 5.1: Configuration of Datacenters

Object name	RAM capacity	Number of processing elements
Host	2000-5000	5-7

Table 5.2: Configuration of Hosts in each datacenter

Object name	Total number used in simulation	Required Processing element	Million instructions per second
Virtual Machine	50	1	2000-5000

Table 5.3: Configuration of Virtual machines

VI. RESULT ANALYSIS

The simulation is initialized by the Main class which creates instances of the scheduler, the job and machine loader, the failure loader and other entities as required by the standard CloudSim 3.0.2.

The energy consumption, VM migration, execution time and Hosts Shutdown can be evaluated through without security and with security is as follows:

Parameters	Without Security	With Security
SLA	0.030%	0.033%
SLA perf degradation	0.21%	0.20%
SLA time per active host	16.60%	15.81%
Overall SLA violation	4.74%	4.61%
Average SLA violation	15.65%	14.09%
Execution time - VM selection mean	0.00161 sec	0.00149 sec
Execution time - host selection mean	0.00557sec	0.00549sec
Execution time - VM reallocation mean	0.01835 sec	0.01715 sec
Execution time - total mean	0.05116 sec	0.04997 sec

Table 1: Comparison of Performance Degradation due to Migration, Execution Time and SLA Violation among Without Security and With Security.

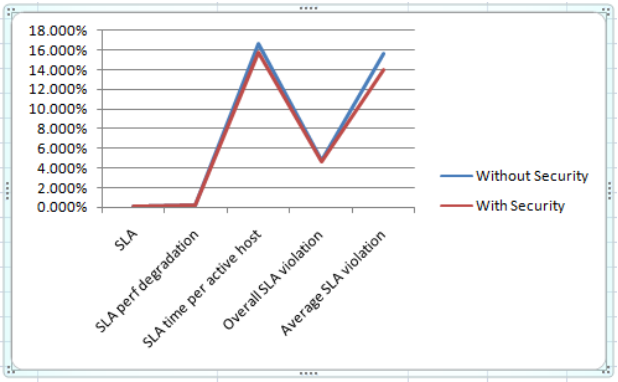

Fig 1: Comparison of Performance Degradation due to Migration, Execution Time and SLA Violation among Without Security and With Security.

Parameters	Without Security	With Security
Energy consumption (Kwh)	47.59	38.38
Number of VM migrations	4201	4199
Number of host shutdowns	1192	1189

Table 2: Comparison of Energy Consumption, Number of Host Shutdowns and Number of VM Migration among Without Security and With Security.

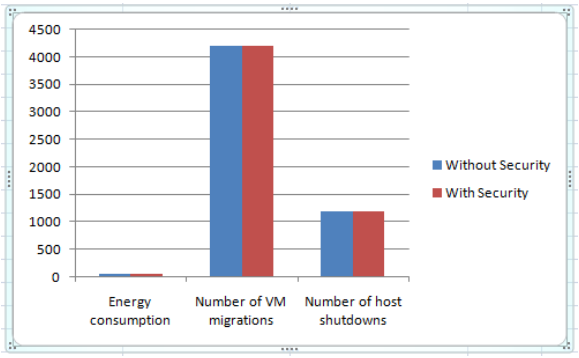

Fig 2: Comparison of Energy Consumption, Number of Host Shutdowns and Number of VM Migration among Without Security and With Security.

VII. CONCLUSION AND FUTURE WORK

In this work, we proposed an optimized method to secure live migration of virtual machine. Using this method we can assure to user or organization who wanted to use the

services of cloud computing to process their data, to store their data, will be in safe hand. Results shows that the live migration of virtual machines is in secure environment and our proposed techniques managed to get lower power consumption, less amount of SLA violation and less amount of performance degradation and fewer amounts of migration time as compare than without secure VM. This method provides a facility to the user that if migration will happened due to some reason like the over utilization of host where the virtual machine is actually running which we consider on our experimental results, then that migration will be secured with the help of encrypting the virtual machine.

REFERENCES

[1] Jie Tao, Holger Marten, David Kramer and Wolfgang Karl, "An Intuitive Framework for Accessing Computing Clouds", ELSEVIER International Conference on Computational Science (ICCS), pp. 2049–2057, April 2011.

[2] Tarun Goyal, Ajit Singh and Aakansha Agrawal, "Cloudsim: simulator for cloud computing infrastructure and modeling", ELSEVIER International Conference on modeling, optimization and computing (ICMOC), vol. 38, pp. 3566-3572, 2012.

[3] Grobauer, B.; Walloschek, T.; Stocker,E.;(2011), "Understanding Cloud Computing Vulnerabilities",5487489 searchabstrSecurity & Privacy, IEEE, Vol 9, pp 50

[4] Gansen Z; Chunming R; Jin L; Feng Z; Yong T; (2010),,"Trusted Data Sharing over Untrusted Cloud Storage Providers",2010 IEEE Second International Conference on Cloud Computing Technology and Science (CloudCom), pp 97, Nov. 30 2010-Dec. 3 2010.

[5] Kresimir P; Zeljko H; (2010), "Cloud computing security issues and challenges", MIPRO 2010, May 24-28, 2010, Opatija, Croatia.

[6] Minqi Z; Rong Z; Wei X; Weining Q; Aoying Z; (2010),"Security and Privacy in Cloud Computing: A Survey", Sixth international conference on Semantics Knowledge and Grid (SKG), pp 105, 1-3 Nov. 2010.

[7] Popovic K; Hocenski Z; (2010), "Cloud computing security issues and challenge", 5533317searchabstractMIPRO, 2010 Proceedings of the 33rd International Convention , pp 344,24-28 May 2010.

[8] Jensen, M.; Schwenk, J.; Gruschka, N.; Iacono, L.L.; (2010), "On Technical Security Issues in Cloud Computing", IEEE International Conference on Cloud Computing, 2009. CLOUD '09, pp 109, 21-25 Sept. 2009. 5708519.

[9] Jianfeng Y; Zhibin C; (2010), "Cloud Computing Research and Security Issues", IEEE 2010 International Conference on Computational Intelligence and Software Engineering (CiSE), pp1, 10-12 Dec 2010.

[10] Yung-Ching Hsu,Pangfeng Liu and Jan-Jan Wu, "Job Sequence Scheduling for Cloud Computing ," International Conference on Cloud and Service Computing, 2011.

[11] Jansen, W.A.; (2010), " Cloud Hooks: Security and Privacy Issues in Cloud Computing5719001 IEEE 2011 44th Hawaii International Conference on System Sciences (HICSS), pp1, 4-7 Jan. 2011.

[12] M. Miller, "Cloud Computing- Web based applications that change the way you work and collaborate online", First edition, Pearson Education India, Aug., 2008.

[13] B. Sosinsky, "Cloud Computing Bible", First Edition, John Wiley & Sons, Jan. 2011.

[14] Rodrigo N. Calheiros, Rajiv Ranjan, César A. F. De Rose, and Rajkumar Buyya, "CloudSim: a toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms", ACM journal of Software-Practice & Experience, vol.41 issue 1, pp. 23-50, Jan. 2011.

[15] Cloud Security Alliance "Top Threats to Cloud Computing" Version 1.0 (2010).

[16] Guidelines on Security and Privacy in Public Cloud Computing, SSpecial Publication 800-144 Wayne Jansen, Timothy Grance, Computer Security Division, Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, MD 20899-8930

[17] Shuai Z; Shufen Z; Xuebin C; Xiuzhen H; (2010), "Cloud Computing Research and Development Trend", 2nd International conference on Future Networks, 2010. ICFN ' 10. pp 23, 22-24 Jan 2010.

[18] Chang, L, Ti ; Chin L; Chang, A.Y.; Chun J, C;(2010), " Information security issue of enterprises adopting the application of cloud computing", IEEE 2010 Sixth International Conference on Networked Computing and Advanced Information Management (NCM),pp 645, 16-18 Aug. 2010.

[19] R. Maggiani; (2009), "Cloud computing is changing how we communicate," 2009 IEEE International Professional Communication Conference, IPCC 2009,Waikiki, HI, United states ,pp 1, 19-22 July.

[20] Geng L; David F; Jinzy Z; Glenn D; (2009), "Cloud computing: IT as Service, "IEEE computer society IT Professional", Vol. 11, pp.10-13, March-April 2009.

[21] Isaac Agudo 1, David Nuñez , Gabriele Giammatteo , Panagiotis Rizomiliotis , Costas Lambrinoudakis, "Cryptography goes to the Cloud".

[22] Grobauer, B.; Walloschek, T.; Stocker,E.;(2011), "Understanding Cloud Computing Vulnerabilities",5487489 Search Labs Security & Privacy, IEEE, Vol 9, pp 50

[23] Yaohui Hu, Sanket P., Tianlin Li, Emine Kaynar, "Performance Analysis of Encryption in securing the Live Migration of Virtual machines", "National Science Foundation".

[24] Sebastian Biedermann, Martin Zittel and Stefan Katzenbeisser, "Improving Security of Virtual Machines during Live Migrations", "IEEE 11th annual conference on Privacy, Security and Trust(PST)", 2013

[25] Pramod Jamkhedkar, Jakub Szefer, Diego Perez-Botero, Tianwei Zhang, Gina Triolo and Ruby B. Lee, "A Framework for Realizing Security on Demand in Cloud Computing", "IEEE International conference on Cloud Computing Technology and Science", 2013.

[26] Anala M R, Jyoti S. Shobha G, "A Framework for Secure Live Migration of Virtual Machines", IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013.

[27] G. Booch, "Object-Oriented Analysis and Design with Applications", 2nd Edition, Benjamin/Cummings Publishing Company, Redwood City, California, 1994.

[28] D. Chappell, "Introducing the Azure services platform", Microsoft corporation, White Paper, Oct. 2008.

[29] R. Buyya, R Ranjan and R.N. Calheiros, "Modeling and Simulation of Scalable Cloud Computing Environments and the CloudSim Toolkit: Challenges and Opportunities", IEEE 7th High Performance Computing and Simulation Conference, vol. 21, pp. 1-11, June 2009.