Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

Secure Protected Live Migration for Energy Efficient Techniques

S. Vinay Deep
Department of CSE,
CMRIT Bangalore, Karnataka 560049, India

Harshitha Nagendra
Department of ISE,
CMRIT Bangalore, Karnataka 560049, India

Suraj J P Gowda
Department of CSE,
CMRIT Bangalore, Karnataka 560049, India

Rajashekar A
Department of CSE,
BTI Bangalore, Karnataka 560049, India

Dr. M Dhanalakshmi
Department of CSE,
East Point College of Engineering & Technology, Bangalore,
Karnataka 560049, India,

***Abstract* -In cloud data centre the VM scheduling technique is used to realize the energy efficient operation of servers and VM migration techniques provides multiple benefits such as resource distribution and energy aware consolidation. In VM migration while moving a task from one VM to another has various security threats. The security is more important during migration to protect the data from the hackers. In the proposed paper, illustrates the security features of energy efficient techniques when it performs live VM migration is the most vulnerable process in cloud for loss of data integrity, confidentiality, unauthorized access and authorization.**
In this paper we propose a secure energy aware provisioning for data centre resources on virtualized platforms. Energy efficient is achieved through VM scheduling, migration mechanism and ability to switch off resources of the physical machine that are not required by VM. Further we proposed solutions to security challenges occur during VM live migration. The implementation and verification of the proposed technique is evaluated using Cloudsim. The experimental results show that our approach reduces energy consumption in data centres.

Keywords: Virtual Machine (VM), Live Migration.

I.INTRODUCTION

Cloud computing is rapidly growing technology for large scale distributed and grid computing. The virtualization concepts used in cloud data centres are enabled to provide an on demand access to shared pool of configurable computing, as it improves the energy efficiency in data centre and ensures that resources are utilized efficiently. VM scheduling of resources is one of the major methods and concepts of consolidating multiple VMs (Virtual Machines) and migration policies are used to migrate the VMs from one server to another to reduce the energy consumption.

The VM migration moving the running virtual machines form source server to destination server. The live migration is performed using two methods namely pre copy and post copy algorithm. A pre copy algorithm the memory pages from source to destination virtual machines is copied on iteration, while copying if threshold is reached memory copying is stopped. The post copy techniques initiate the transfer of processor state and memory pages but fetched only on demand from source virtual machine. During VM migration has various security threats, thus we need to overcome threats from hackers.

Live migration of virtual machines has various security threats. The intruder can access and modify the content, it is known as Man-in Middle attack. Thus secure and endangered channel must be used to diminish snooping and tampering attempts on migrating data. The Denial-of Service attack reduces the performance of services by unauthorized user access. The internals attacks send the malicious code to target VMM and gaining control by manipulating data send to migrating VM. The Stack Overflow attack, the attackers to get control over execution code they exploit the integer signedness and attackers injecting unwanted traffic in the communication causes a buffer to overflow thereby memory is corrupted, next the Replay attack causes reordering issues, the attacker changes the order of memory pages buffered from source virtual machine to destination virtual machine and also the attacker instead of sending modified pages, resend the old copies of memory pages. In this proposed paper all the attacks and threats are reduced using security techniques in live migration.

This paper provides a secure way of minimizing energy consumption in data centres through minimizing no of physical machines using virtualized platforms. Energy efficiency is achieved through VM scheduling and live migration by providing security challenges during VM migration. The objective is power saving by reducing number of host used to run the VMs and Virtual machine

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

monitor (VMM) a security model is placed to ensure the VM security.

Scheduling of resources is one of the major methods to reduce the power consumption. The virtual machine scheduling among the servers and utilizing the resources efficiently results in minimizing the energy consumption.

The remainder of this paper is structured as follows. Section II we discuss Related Work. Section III is the Methodology. Section IV is Experimental Results. Section V paper is Conclusion.

II.RELATED WORK

Sukhpal Singh et al.[1] In their paper, authors emphasis on the development of energy based resource scheduling framework and present an algorithm that consider the energy between various data centre and Quality of Service. The performance of the proposed algorithm has been evaluated with the existing energy based scheduling algorithms.

Ching-Chi et al.[2] In this paper one of the effective way to reduce power consumption is to consolidate the hosting workloads and shut down physical machines which become idle after consolidation and new algorithms Dynamic Round-Robin, is proposed for energy-aware virtual machine scheduling and compared with Greedy, Round Robin, Power save scheduling strategies.

Matthias Schmidt et al. [3] this paper, deal with the problem of distributing virtual machine images to a set of distributed compute nodes in a cross-cloud computing environment i.e., the connection of two or more Cloud computing sites. Virtualization offers both more flexibility and security through custom user images and user isolation.

Ahmed M Mahfouz et al. [4] in their paper proposed a technique to ensure the security in migration by reviewing the different stages involved in live migration and identifying the threats encountered in the process.

Anita H.M et al. [5] in their paper proposed XTS – AES algorithm in which equal size data units are encrypted to safely migrate one data centre to another data centre. It also avoids attackers from interpreting the data by ensuring security parameters such as confidentiality, access control and integrity.

Ke Yang et al. [6] proposed an optimized control strategy which combines multi-strategy mechanism with the prediction mechanism to reduce the number of the overloaded hosts, avoid instantaneous peak problem caused by the migration of virtual machines, solve the imbalance problem and the high-cost problem in tradition scheduling algorithm of migration.

Anit Khan et al. [7] discussed about Dynamic consolidation of Virtual Machines (VMs).They proposed a novel heuristic Dynamic VM Consolidation algorithm, RTDVMC, which minimizes the energy consumption of CDC through exploiting CSU provided information.

Subhra Priyadarshini et al. [8] in their paper discussed about the increasing energy consumption in the data center and came up with a proposal to route the load provided by the user to a suitable data center, so that the electricity cost will be minimized and utilization of renewable energy sources will be maximized.

M. R. Anala et al. [9] in their paper proposed an attack model and implemented a framework for secure live migration. It is an integrated solution which addresses network intrusion, access policy, and encryption and firewall protection.

S.Sengole Merlin et al. [10] in their paper proposed an automated intelligent system which detects the overload or under load condition to select a VM, then encryption is done with the help of security algorithm which renders integrity, confidentiality , mutual authentication and data security also the overall cost and time of the migration process is reduced significantly.

Kanwal Janjua et al. [11] in their paper have discussed six important security features and they were tested by the AVISPA tool.

Yuchen Wong et al. [12] in their paper proposed a familiarity model for load balancing and secure VM placement. Their best fit algorithm and load balancing algorithm make co residence difficult as well handle security issues**.**

Xin Wng et al. [13] in their paper proposed a co-resident threat defence mechanism which consists of co resident resistant Vm allocation (CRRVA), analytic hierarchy process based threat score mechanism (AHPTSM) and attach aware Vm allocation (AAVR). CRRVA is concerned with securely allocating Vm, AHPTSM calculates the threat score and AAVR migrates the high threat score VM with less migration cost.

Tayyaba Zeb et al. [14] in their paper proposed a security metric model to determine the attack resiliency measure, performance improvement factor and cost measure of VM migration.

In our proposed technique paper provides a secure way of minimizing energy consumption in data centres through minimizing no of physical machines using virtualized platforms and provides security challenges during VM migration. The objective is power saving by reducing number of host used to run the VMs and Virtual Machine Monitor (VMM) a security model is placed to ensure the VM security.

III.METHODOLOGY

The Virtual Machine Assignment algorithm considers host energy consumption and VM energy consumption classify the VMs based on the resource usage and schedule them, the resource utilization among the hosts in the cloud. In the energy efficient VM assignment algorithm resource utilization and energy consumption of hosts in cloud is determined, these values are stored into a table in ascending order. The m tasks arrive at the cloud

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

data centre, for each task a VM is created, the VM energy consumption is measured and these values are stored into a table in descending order to balance the resource utilization, the VMs resource utilization (CPU, memory) is measured and VMS are grouped into VM Memory type, VM CPU type. The VM memory type means more memory and minimum CPU is utilized (this task requires more memory and minimum CPU) and the resource utilized in VM CPU type is more CPU and minimum memory (the task requires more CPU and minimum memory for its execution). The classified VMs are scheduled for balancing the resource utilization across the computing nodes in cloud and while allocating VM on the host, it conforms that CPU, memory utilization does not exceed the maximum host CPU and memory threshold, Calculate the maximum power threshold of the host and find the total power threshold then allocates the VM on host which results into least increase in energy consumption, after the VMs allocation the energy consumption is reduced.

A. Management Services

Migration controller used is based on the server is overloaded, it determines a workload on the server that should be migrated and as a second step it searches for a new server which is least loaded that has sufficient resources to host the workload. In an under loaded situation, the controller chooses the least loaded server and tries to shut it down. The Migration controller is a feedback control loop. Whenever the resource utilisation is low or high, a trigger is set off by the advisor module which is sent to the migration controller which then takes necessary actions. This implementation follows two rules as follows

Server whose cpu and memory consumption exceeds the maximum threshold is considered to be overloaded. The migration controller identifies a workload to migrate and an appropriate target is chosen depending on which is least loaded. In the absence of such a servers new server is set up to which the workload is migrated.
Server whose cpu and memory consumption doesn't meet the minimum threshold is considered to be under loaded. This minimum threshold is calculated from the average utilization of the overall system. This is helpful in preventing thrashing. Migration controller chooses a least loaded server and tries to determine a target server before shutting it down. If a target server remains unidentified, the shutdown process is stopped. Additional servers are not set up.

B. Preserving Security in live migration

In the security VM live migration preserves the privacy and integrity of protected data, eliminates the security vulnerabilities improved by the live migration and solves the namespace conflict, packing the maintenance metadata in the hypervisor and reestablishing the protection base on the target platform.

C. Security Live Migration

The attack model of live migration process discusses how the migration process can be attacked by the intruders.
The attack model of live migration of VM includes follows attack point is:

Attack on management input/output
Denial-of-service attack: Attackers can attack more virtual machine towards itself by false resource advertisement.
Attackers can migrate a more virtual machine stealing the bandwidth blocking genuine migrations. This cause serious issue in an environment where migrations are initiated automatically.

Replay attack: Attackers can resend the old copies of memory pages to destination where the modified pages are needed. This occurs due to frequent dirtying of pages. Attackers can change the order of memory pages transferred from source virtual machine to destination virtual machine. This causes reordering issues in the destination virtual machine.

VM inter communication attack
Overflow attack: Attackers can cause a buffer overflow by injecting unwanted traffic in the communication channel, thereby the memory of the running process is corrupted
Attackers can exploit the integer signedness so that it gets the control over execution of code in privileged mode.

Replay Attack : The migration manager provide the encrypted image of the protected page and send it over network if the page is dirtied in previous round. If a protected page is dirtied multiple times, it is possible for a replay attack that a malicious migration manager sends the old content instead of the new version. To prevent this attack, we hash the content of each protected page in the stop-and-copy phase.

Guest VM and host OS communication attack : VM communicate with host system and host with VM. The host OS has complete control over all the guest VMs running over it. Similarly a malicious guest VM can compromise the host OS.

Attack on transmission network channel : The migration data appears as clear text over the network. Thus the transmission channel is susceptible to man-in-middle attack. The attack can be passive attack or active attack. The passive attacks include eavesdropping of messages for sensitive data, passwords and keys, capturing authenticated packets and replying them. The active attack includes manipulating authentication services like login, Pam, manipulating kernel memory etc.

Protected Security Modules:
The Figure 1 Protected security live migration has these security modules are applicable to the host VM. This

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

module ensures that the migrating source or destination is trusted.

a) MAC/Digital Signature: This module uses MAC or digital signature to ensure that migration data is not modified during transmission over the insecure network and protects integrity of migration data. b. Intrusion Detection System: An IDS detects and reports malicious intrusion attempts. They display in the form of alerts like log message, an email to system administrator, and pop up console message etc. c. The control policies define the user can create a VM, who can migrate a VM and can delete a VM. d. Encryption/Decryption: This module is responsible for encrypting the migration data and metadata at the source and decrypting the same at the destination. e. Firewall: It allows the administrator to define firewall rules that controls the open ports for communication, the protocols for communication, and the list of allowed and rejected hosts/VMs.

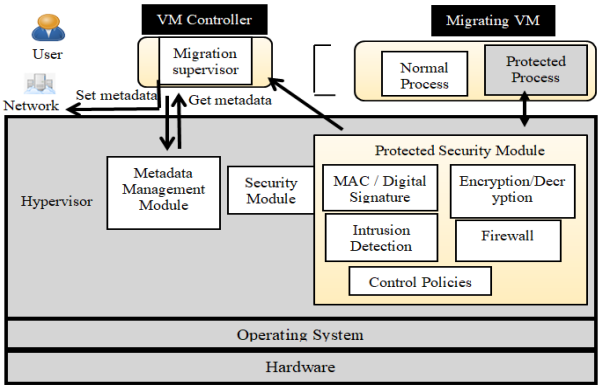

Figure 1: Protected Secure Live Migration

IV.EXPERIMENTAL RESULTS

We have evaluated the proposed algorithms through simulations using the CloudSim toolkit [17, 18] with an extension enabling secure power-aware simulations. We have chosen CloudSim toolkit as a simulation framework, as it is built for simulation of Cloud computing environments. We have extended the framework in order to enable our proposed energy aware algorithm simulations as the core framework does not provide this capability. In addition, we have incorporated a security module to ensure VM security during migration.

Table 1: Clouds Simulation Setup

No of Data Centres	1
No of Cloudlets	500 Number with size of cloudlet is 50000 MI
No of Hosts in Data Centre	100
Resource Configuration of each host	Host have one CPU core with 1000 to 6000 MIPs, 8GB RAM, 1 TB disk
Resource Configuration of each VM	25 VM with 500 to 4000 MIPs, 512MB RAM, 1 GB disk
Bandwidth availability	2000 Mbps to 6000 Mbps

The simulated data center consists of 100 heterogeneous physical nodes. Each node is modeled to have one CPU core with performance equivalent to 1000, 2000 or 3000 MIPS, 8 GB of RAM and 1 TB of storage. Users submit requests for provisioning of 290 heterogeneous VMs that fill the full capacity of the data center. We simulated a Non Power Aware policy (NPA) and Dynamic Voltage Frequency Scaling (DVFS) that adjusts the voltage and frequency of CPU according to current utilization. We simulated a Single Threshold policy (ST) and two-threshold policy aimed at Minimization of Migrations (MM). Besides that, the policies have been evaluated with different values of the thresholds.

Table 1 Simulation Result

Policy	Energy	SLA	Migrations	AVG SLA
NPA	8.9KWh			
DVFS	3.99KWh			
ST	2.00KWh	4.99%	34,225	80%
MM	1.56KWh	8.05%	33,230	84%
DRR	1.40KWh	8.03%	34,115	85%

The simulation results are presented in Table 1. Our results show that dynamic reallocation of VMs using VM Scheduling algorithm saves more energy compared to static allocation policies. DRR policy allows achieving the best energy savings with less energy consumption relatively to NPA, DVFS, MM and ST policies respectively. MM policy leads to more than 10 times fewer VM migrations than ST. The results show the flexibility of the algorithm, as the thresholds can be adjusted according to SLA requirements.

V.CONCLUSION

In this paper, we have proposed a secure energy-aware provisioning of cloud computing resources in virtualized platforms. Our simulation results convinced us that VMs migration using scheduling techniques for server consolidation is an extremely feasible solution to reduce energy consumption in a data center without compromising on security. We are convinced that proposed security migration strategies during migration guards against Overflow attack and Replay Attacks. Future work includes other security threats facing VM migration shall be investigated. Further focus on analysis and measuring of VM migration cost in a cluster.

VI.REFERENCES

[1] Sukhpal Singh and Inderveer Chana, Energy based Efficient Resource Scheduling: A Step Towards Green Computing, in International Journal of Energy, Information and Communications ,Vol.5, Issue 2 2014, pp.35-52.

[2] Ching-Chi, Pangffeng, Jan-jan Wu, "Energy-Aware Virtual machine Dynamic provision and scheduling for cloud computing." In Proc. of the 2011 IEEE 4th International Conference on cloud computing.

[3] Matthias Schmidt, Niels Fallenbeck, Matthew Smith, Bernd Freisleben,"Efficient Distribution of Virtual Machines for Cloud Computing" 18th Euromicro Conference on Parallel, Distributed and Network-based processing, 2010

[4] Ahmed M Mahfouz, Md Lutfar Rahman and Sajjan G Shiva, "Secure live virtual machine migration through runtime

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 09, September-2020

monitors," 2017 Tenth International Conference on Contemporary Computing (IC3), Noida, 10-12 Aug 2017, pp. 1-5.

[5] Anitha H. M and P. Jayarekha, "Secure virtual machine migration in virtualized environment," 2018 2nd International Conference on Inventive Systems and Control (ICISC), Coimbatore, 19-20 Jan 2018, pp. 938-943.

[6] Ke Yang, JianhuaGu, TianhaiZhao, Guofie Sun, "An optimisedControl Strategy for Load Balancing based on LiveMigration of Virtual Machine", at the Sixth Annual China grid Conference,Liaoning,China,22-23 August 2011, pp. 141-146.

[7] MdAnit Khan, Andrew P Paplinski, Abdul Malik Khan, ManzurMurshed,RajkumarBuyya, "Exploiting user provide information in dynamic consolidation of virtual machines to minimize energy consumption of cloud data centers", Third International Conference on Fog and Mobile Edge Computing (FMEC), Barcelona, Spain, 23-26 April 2018, pp. 105-114.

[8] Subhra Priyadarshini Biswal, Satya Prakash Sahoo, "Fuzzy Logic Based Cost and Energy Efficient Load Balancing Cloud Computing Environment", at Second InternationalConference on Intelligent Computing and Control Systems (ICICCS),Madurai,India,14-15 June 2018, PP.158-163.

[9] M. R. Anala, Jyoti Shetty and G. Shobha, "A framework for secure live migration of virtual machines," 2013 International Conference on Advances in Computing, Communications and Informatics (ICACCI), Mysore, 22-25 Aug 2013, pp. 243-248.

[10] S. Sengole Merlin, Nisha Maria Arunkumar and Miriam A. Angela, "Automated Intelligent Systems for Secure Live Migration," 2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT), Coimbatore, 20-21 April 2018, pp. 1360-1371.

[11] Kanwal Janjua and Waris Ali, "Enhanced Secure Mechanism for Virtual Machine Migration in Clouds," 2018 International Conference on Frontiers of Information Technology (FIT), Islamabad, Pakistan, 17-19 Dec 2018, pp. 135-140.

[12] Yuchen Wong and Qingni Shen, "Secure Virtual Machine Placement and Load Balancing Algorithms with High Efficiency," 2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications (ISPA/IUCC/BDCloud/SocialCom/SustainCom), Melbourne, Australia, 2018, pp. 613-620.

[13] Xin Wang, Liming Wang, Fabiao Miao and Jin Yang, "SVMDF: A Secure Virtual Machine Deployment Framework to Mitigate Co-Resident Threat in Cloud," 2019 IEEE Symposium on Computers and Communications (ISCC), Barcelona, Spain, 29 June-3rd July 2019, pp. 1-7.

[14] Tayyaba Zeb, Muhammad Yousaf, Humaira Afzal and Muhammad Rafiq Mufti, "A quantitative security metric model for security controls: Secure virtual machine migration protocol as target of assessment," in China Communications, vol. 15, no. 8, pp. 126-140, Aug. 2018.

[15] Korir Sammy,Ren Shengbing,Cheruiyot Wilson,"Energy Efficient Security Preserving VM Live Migration In Data Centres for Cloud Computing",in International Journal of Computer Science Issues,Vol. 9,Issue 2,No 3, March 2012

[16] Gokul Geetha Narayanan,RA.K Saravanaguru,"Securing VM migration through IPSec tunnelling and onion routing algorithm",at 2nd Int. Conf. Intelligent Computing and Control Systems,Madurai,India,14-15 June 2018

[17] R.Buyya. Cloud Simulator cloudsim version 2.1, GRIDS Lab, http://code.google.com/p/cloudsim, July 27, 2010.

[18] Open Cloud Manifesto. [Online]. Available: http://www.opencloudmanifesto.org/.