International Journal of Research in Computer Science
eISSN 2249-8265 Volume 4 Issue 2 (2014) pp. 25-30
www.ijorcs.org, A Unit of White Globe Publications
doi: 10.7815/ijorcs.42.2014.082

USING VIRTUALIZATION TECHNIQUE TO INCREASE SECURITY AND REDUCE ENERGY CONSUMPTION IN CLOUD COMPUTING

Hamid Banirostam[1], Alireza Hedayati[2], Ahmad Khadem Zadeh[3]

[1]*Department of Computer Engineering, Science and Research Branch Guilan, Islamic Azad University, Rasht, IRAN*

Email: h.banirostam@yahoo.com

2Department of Computer Engineering, Islamic Azad University, Central Tehran Branch, Tehran, IRAN

Email: hedayati@iauctb.ac.ir

3Research Institute Information & Communication Technology, Tehran, IRAN

Email: zadeh@itrc.ac.ir

Abstract: *An approach has been presented in this paper in order to generate a secure environment on internet Based Virtual Computing platform and also to reduce energy consumption in green cloud computing. The proposed approach constantly checks the accuracy of stored data by means of a central control service inside the network environment and also checks system security through isolating single virtual machines using a common virtual environment. This approach has been simulated on two types of Virtual Machine Manager (VMM) Quick EMUlator (Qemu), HVM (Hardware Virtual Machine) Xen and outputs of the simulation in VMInsight show that when service is getting singly used, the overhead of its performance will be increased. As a secure system, the proposed approach is able to recognize malicious behaviors and assure service security by means of operational integrity measurement. Moreover, the rate of system efficiency has been evaluated according to the amount of energy consumption on five applications (Defragmentation, Compression, Linux Boot Decompression and Kernel Boot). Therefore, this has been resulted that to secure multi-tenant environment, managers and supervisors should independently install a security monitoring system for each Virtual Machines (VMs) which will come up to have the management heavy workload of. While the proposed approach, can respond to all VM's with just one virtual machine as a supervisor.*

Keywords: *Green Cloud Computing, Multi- tenancy, Virtualization, Data integrity.*

I. INTRODUCTION

Cloud computing can be considered as the result of natural development of virtualization technology so that physical resources can be used optimally by deployment cloud computing through virtualization and applications under network with the least energy and also by sharing resources within their environment. In recent years, great amount of using PCs has led us to face a significant energy loss because the lack of usage in the most hours of the day. Relying on virtualization, this possibility can be provided to set various services on a single physical machine which could result in optimizing energy and minimizing machines' idle time [1].

Through the abilities of rapid expansion and deploying common virtual resources, green cloud processing will have a great impact on energy reduction. One kind of developed cloud platforms is internet Based Virtual Computing (iVIC) [2] which enables users to generate a dynamic, ordered, and scalable environment of VMs which is allowed to have a rapid deployment of the operating system and software under network through browser based interface.

However it results in reduction of energy cost and saving energy, it would also face issues such as preventing malicious programs to enter VMs, the possibility of using security systems under network within virtual cloud environment, and applying comprehensive measurement system of the environment's current situation under critical circumstances and several kinds of control systems not to receipt unidentified individuals requests [3].

Continuing related work is studied in the second section. Third section includes presenting mechanism of the proposed approach and checks for data integrity and after that, the results of the surveys and simulations will be reviewed and ultimately conclusions will be displayed.

II. RELATED WORK

Virtual Machines (VM) have been generated in the midst of 1970s. VM is a logical process managed by control program simulating hardware. In fact, VMs are executing on a large computer in order to represent sharing resources and isolation. Some of VM systems such as VMware and Xen have been embedded in large companies [4]. VMM simultaneously acquires execution permission of a number of VMs and resources transparent distribution among them and isolation of VMs to prevent access to memory or disc space. Operating system executed inside a VM is traditionally considered as a guest operating system so that running programs on this system is mentioned as guest applications.

A. VM Monitoring

VM monitoring can be classified into two groups. The first kind of VMM can be run directly on physical hardware and there is no operating system on that. Therefore, this VMM is completely responsible for scheduling and allocating system resources among VMs. ESX and Xen are both considered to be in this group. The second kind of VMM is to be run as an ordinary operating system which controls actual hardware resources and is usually a host operating system. Since host operating system has no knowledge of the second kind VMM, it behaves just as any other process within the system. GSX, VMware, UML, and FAU machine are some in the second group of VMMs [5]. Host operating system of this group is heavier than the first group's and it is also more prone for security vulnerabilities. Therefore, the first kind VMM is generally considered to be more secure than the second kind [6].

B. VM Based Service Architecture

While having different features, VM based security systems have common architecture. This has been demonstrated in Figure 1 that security systems can be noticed as a part of VM monitoring or getting embedded within an assigned VM. Some security systems also may run their components within the guest operating system. Although components are guests in the operating systems, they are often only responsible to generate security system requests within VMM or assigning a secure VM to implement the policy. Security policies are rarely implemented inside the guest operating system because of the risk of security systems there. Security in VM based services is based on this assumption that the Trusted Computing Base (TCB) is also secured. In the first kind, VM is to be the VM supervisor. Some of services in VM are assigned to the secure VM as a part of TCB [7].

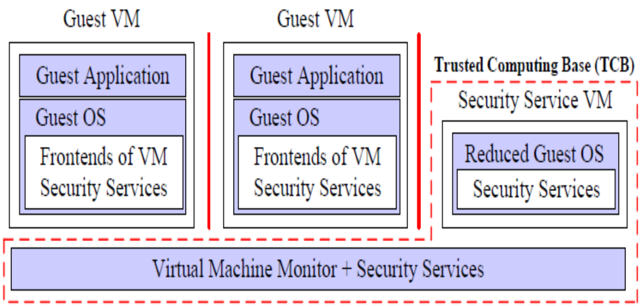

Figure 1. Architecture cloud-based security services

C. Security Services

Honeypot: This security service has been recently become a popular tool to recognize large scale attacks on internet. Generally Honeypots are categorized in two groups: low interaction and high interaction. However low interaction Honeypot accepts network messages but still they can give just a minimized answer and the behavior of a high interaction [8].

Security: Three phases of secure isolation, confident upload, and monitoring should be considered in secure application software running environment. In fact, the main motivation in secure isolation came up by the advent of IBM VM/370 and VMM technology. Through generating a number of VMs, VMM will cause monitoring on independent operating systems within the physical machines [8]. Yan Wen presented isolation model based on the hardware abstract layer called SVEE [9]. Flume system also was represented at the University of MIT in order to control information stream management and checking data integrity [9]. "Confident upload" as the second phase of security is in fact saving system integrity and accuracy against the intrusion of malicious applications which means assuring a software to be non- malicious while it is uploading [10]. Finally, the third phase is to be "Monitoring". Garfinkel has represented some solutions to control accuracy by presenting Honeypot system able to monitor VMM [10].

Data accuracy: there are different approaches in measuring data accuracy and different embedded software in process environment such as Prima, Tripwire, and IMA [11]. A secure system has to be generated through isolation mechanism in order to deploy applications and data in various presented services. Inside a physical network, common methods of isolation can perform filtering operation just like a firewall, so this can be mentioned as another challenge in virtual networks path [12]. One of the solutions for this challenge is Snort. Factually Snort is an Intrusion Prevention System (IPS) able to analyse real time traffic and sign in packs to the system on IP of networks. This ability can contain analysis protocol, searching for context (query), and adapting them to detect various threats such as buffer overflow, hidden port scan, CGI (Common Gateway Interface) attacks, SMB (Server Message Blocker) attacks, and fingerprinting operating system. But Snort mechanism also meets some limitations such as high start-up cost of the intrusion detection system, and confined capability to measure network traffic which ends up in some CPU cycles use [12].

D. Green Cloud Computing

Whereas, there has always been energy loss in idle systems, energy consumption has been constantly increasing in information centers. The amount of usage in idle servers is almost two times more than active ones. Considering this problem and also in order to optimization, David Meisner et al. has represented Powernap [13]. This solution provides optimizing energy through making active system migrate to idle system. Then in 2009, Francis and Richardson represented a model for virtualization by optimal use of energy [14]. IBM researchers also minimized task volume in servers based on a policy to turn on/off servers in particular conditions which eventually led in minimizing energy consumption. A solution will be proposed in this paper in order to optimizing energy of implementing green cloud computing also by virtualization.

III. THE PROPOSED APPROACH

Proposed approach of this paper has been implemented on iVIC platform. The main capability of this approach is VM resource management and providing operation security on this platform. It can make monitoring possible on running processes in order to ensure service security for operational accuracy measurement and preparing performance reports. This monitoring would become possible by VM Insight software which is a virtualization software based on the process of security monitoring system. At the beginning of execution in this approach, the systems approach to information provides a backup file of system's initiative situation. After that, all monitoring operations including comparison of system's initiative situation with its current situation will be performed dynamically.

Within this dynamic comparison, invalid changes which can lead to the lack of integrity will be identified. Then intrusion detection in network and also the network traffic will be dynamically checked by Snort. In the proposed approach, authentication and users' access method are recognized by a central supervising section which has control policies. Within the cloud multi-tenant shared environment, resource storages should be also considered because of using shared resource storages together with isolating users' access method with different goals. This is assumed in the proposed approach that VMs have been dynamically established inside the system and after verification, they would have access to the resources. Figure 2 illustrates the proposed model action and reaction against malicious intrusions.

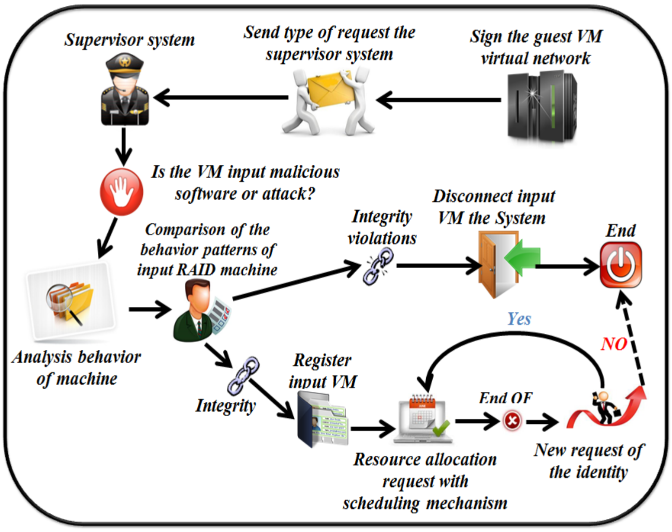

Figure 2. The Proposed model against malicious intrusion

First in the proposed approach, a VM with various goals enters virtual network and after that, it sends different requests including receiving virtual resources (hardware, software, storage, and etc.) to the system supervisor. At first system supervisor temporarily disconnects all entering VMs from the system to check up entering machine's behaviour. After that, it checks machine's characteristics to analyse its behaviour. This results in distinguishing malicious machine identification from non- malicious one. In order to recognize attacks or detect malicious software which might lead to accuracy violation of system integrity, a new pattern of machine behaviour will enter the system and will be compared to the patterns stored in the system database from before. In fact, malicious software has been already simulated on the noticed system and also intrusion results have been evaluated too. At last, if considering predefined patterns as attack and intrusion to the network, the behaviour has been recognized to be malicious, it will be disconnected from the system and also as an invalid identity, it will not get the permission of access to the resources. But if it is recognized as a valid identity then its characteristics will be registered within the comprehensive information database relevant to the virtual network system. This method will guarantee system security through avoiding invalid identity and on the other hand, since the operation of resource assignment would be available to a valid identity only by supervisor system confirming that, it will provide isolation operation inside shared environment of cloud resource storages.

- *The Proposed Approach Algorithm*

Since each various physical machine independently manages several VMs, security of the environment in accessing shared resources is the most important priority in the storage of multi-tenant resource environment. Proposed method securely manages access to VMs shared resources through verifying user identity and determining control policies.

- *12 steps of the Proposed Algorithm*

1. VM (guest VM) entrance to the system which is shared resources storage.
2. Sending request to system supervisor.
3. Start-up the operation of new VM identification through comparing with the behaviours of software already stored as malicious behaviour in system bank.
4. Checking whether or not a new identity has been recognized to be valid. If yes then go to line 5, unless go to line 12.
5. Verifying new VM identity.
6. Determining control policies to limit the access to common resource pool such as VM likely to Full, Write, Read and Access.
7. Granting a certificate or VM authentication.
8. Allocating a physical machine to VM in order to receive and run requested resources and also to have remote access to resources.
9. Running scheduling mechanisms to allocate resources and eliminate allocated resources available to VM.
10. Releasing the resource after the task is finished.
11. If user requests for a new resource, go to line 8, unless go to the next line.
12. End.

Behaviour patterns of recognized malicious identities are stored in a file. Now, to achieve such patterns in this paper, simulation has been performed on two kinds of VM: Qemu and HVM Xen. Through this simulation, some samples of malicious software have been directly run within VM insight environment and then results have been applied on the proposed approach to detect and discover its behaviours. Results of this software are demonstrated in Table 1.

Table 1. Behavior tracing and detection model

Trust	*Route*	*Bytes Recei_ved*	*Bytes Sent*	*CPU Stat_us*	*Server or applica_tion*	*No parent recess*	*No parent process*
Yes	*/user/sbin/acpid*	*3*	*14343*	*0%*	*acpid*	*1592*	*1593*
Yes	*/user/sbin/Apache*	*0*	*0*	*0%*	*Apach_e*	*1631*	*1632*
Yes	*bin/login*	*177*	*18083*	*0%*	*Login*	*1683*	*1752*
No	*/user/bin/ ls*	*0*	*0*	*0%*	*Is*	*1752*	*2845*

According to Table 1, the proposed approach can discover malicious software which cause violation of system integrity through comparing network's sent or received number of bytes.

Five established applications including Compression, Defragmentation, Linux Boot, Decompression and Kernel Boot in the environment have been used to achieve evaluation results in order to evaluate the amount of energy consumption in VM insight hardware in Qemu and HVM Xen. Qemu evaluation results are shown in Figure 3 and VMInsight evaluation results together with HVM Xen have been presented in Figure 4 by using the proposed approach.

Considering the comparison between Figures 3 and 4, it can be perceived that when a service is being used separately, the overhead of its performance grows about 12%. So this can be concluded that the proposed approach can be considered as a secure system able to detect threatening behaviour too. After that, the results of Figure 5 shows the amount of system efficiency regarding to the amount of energy consumption by simulating five applications of Defragmentation, Compression, Linux Boot, Decompression and Kernel Boot..

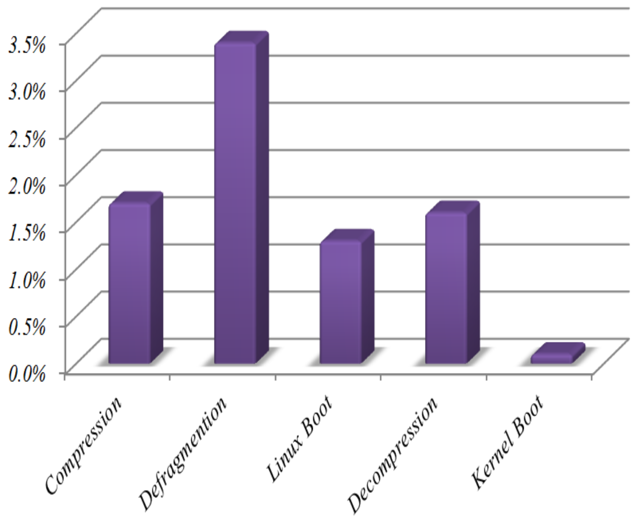

Figure 3. Runtime Overhead of VM insight on Qemu

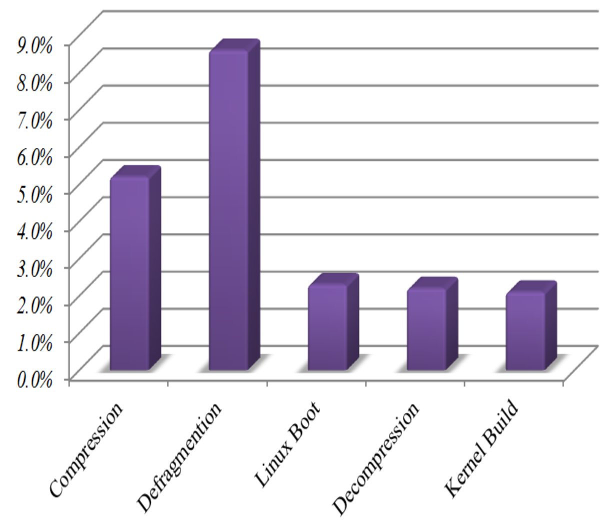

Figure 4. Runtime Overhead of VM insight on HVMXEN

Figure 5, in fact, is an energy comparison between Qume VM physical machine and the proposed approach. Considering this figure, it can be observed that if each of three mentioned infrastructures is applied singly and separately to run the applications, the amount of e-consumption will be high because using the proposed approach to secure the environment and Qume will be followed by a significant amount of overhead in energy and cost. Factually to secure a multi-tenant environment, managers and supervisors should install a supervision security system independently for every VM which leads to a heavy management workload. Furthermore, because of extra energy consumption for each VM monitoring system, the cost of energy consumption and energy loss will be increased. Besides, installing virtual secure monitoring on independent operating systems of every physical machine will also increase energy consumption significantly because each physical machine is allowed to run 20 VM in average while the proposed approach can response all VMs only by one supervisor VM.

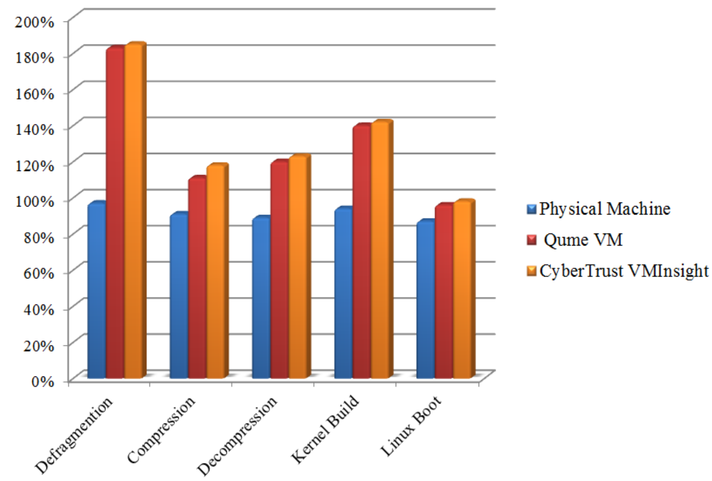

Figure 5. Energy consumed by different applications in different machines

IV. CONCLUSIONS

In this paper, an approach was proposed on iVIC platform. Performance of the proposed approach in management of VM resources facilitates security of performed operations on the platform. This approach also examines noticed machine behavior and distinguishes between identities of malicious and non- malicious machines. This paper showed simulations of two kinds of VMMs (Qume, and HVM Xen) and according to the comparison between these simulations, this was resulted that when a service is singly used, its performance overhead grows about 12%. So this can be concluded that the proposed approach can be considered as a secure system which is also able to detect threatening behaviors. Moreover, the rate of system efficiency was evaluated according to the amount of energy consumption on five applications including Compression, Defragmentation, Linux Boot, Decompression and Kernel Boot. Results of this paper showed that if each of three mentioned infrastructures were applying separately, the amount of energy consumption will be high because using the proposed approach to secure the environment and Qume will be followed by energy and cost overhead. In fact, to secure a multi-tenant environment, managers and supervisors should independently install a security monitoring system for every VM which leads to have a heavy management workload. Also because of extra energy consumption for each VM monitoring system, the cost of both energy consumption and energy loss are to be increased while the proposed approach is able to respond all VMs by having only one VM supervisor.

V. REFERENCES

[1] Celesti Francesco, A., Villari, M.T and Puliafito, A., "Improving Virtual Machine Migration in Federated Cloud Environments", Second International Conference on Evolving Internet, 20-25 September 2010., pp. 61-67. doi: 10.1109/INTERNET.2010.20

[2] Chen, Y., Wo, T. and Li, J., "An efficient resource management system for on-line virtual cluster provision", IEEE ICC, 2009 , pp.72–79. doi: 10.1109/CLOUD.2009.64

[3] Shwetha,B. and Balagoni,Y., "Secure Data Storage In Cloud Computing", International Journal of Research in Computer Science, vol.1, 2011, pp.63-73. doi: 10.7815/ijorcs.11.2011.006

[4] Mateescu, G., Gentzsch , W.and J. Ribbens, C., "Hybrid computingwhere HPC meets grid and cloud computing", ELSEVIER FGCS, 2011, pp. 440–453. doi: 10.1016/j.future.2010.11.003

[5] Zissis, D.and Lekkas,D., "Addressing cloud computing security issues", ELSEVIER FGCS, 2011, pp. 583-592. doi: 10.1016/j.future.2010.12.006

[6] Li, J., Huai, J., Hu, C. and Zhu, Y., "A Secure Collaboration Service for Dynamic Virtual Organizations", IS Elsevier, vol. 180, issue 17, 2010, pp. 3086–3107. doi: 10.1016/j.ins.2010.05.014

[7] Ray, S. and De Sarkar, A., "Execution Analysis of Load Balancing Algorithms in Cloud Computing Environment", IJCCSA, Vol.2, No.5, 2012, pp. 1-13.

[8] Suakanto, S., H.Supangkat, S. and Saragih, R, "Performance Measurment of Cloud Computing Services", IJCCSA, Vol.2, No.2, 2012, pp. 9-20.

[9] M. Azab, A., Ning, P., C. Sezer, E. and Zhang, X, "HIMA: a hypervisor based integrity measurement agent", IEEE Computer Society , 2009,pp. 461-470. doi: 10.1109/ACSAC.2009.50

[10] Zhao, X., Borders, K. and Prakash, A., "Virtual machine security system", ACSE, 2009, pp. 339-365.

[11] Lombardi, F. and Di Pierto, R., (2009), "KvmSec: a security extension for Linux kernel virtual machines", ACM SAC, March 8-12, pp. 2029-2034. doi: 10.1145/1529282.1529733

[12] Beloglazov, A. and Buyya, R., "Energy Efficient Allocation of Virtual Machines in Cloud Data Centers", IEEE/ACM ISCluster, 2009, pp. 557-578. doi: 10.1109/CCGRID.2010.45

[13] Meisner, D., T. Gold, B. and F. Wenisch, T., "PowerNap: eliminating server idle power", ASPLOS 2009,7-11 March, pp. 205–216.

[14] Alam, M., "Cloud Algebra for Handling Unstructured Data in Cloud Database Managements System", IJCCSA, Vol.2, 2012, pp. 35-42. doi: 10.1145/2393216.2393221

How to cite

Hamid Banirostam, Alireza Hedayati, Ahmad Khadem Zadeh, "*Using Virtualization Technique to Increase Security and Reduce Energy Consumption in Cloud Computing*". *International Journal of Research in Computer Science*, 4 (2): pp. 25-30, March 2014. doi: 10.7815/ijorcs.42.2014.082