Secure Virtualization for Cloud Environment Using Guest OS and VMM-based Technology

Mahda Noura¹, Sadra Mohammadalian², Leila Fathi³, Mahnoosh Torabi⁴

¹²³⁴Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor

E-mail: ¹m_noura67@yahoo.com, ²Sadra.m.alian@gmail.com, ³fathi_leila67@yahoo.com, ⁴mahnooshtorabi@yahoo.com

ABSTRACT

Cloud computing, the utility base computing, is going to become the mainstream of IT future. Governments and enterprises are realizing that by immigrating into the cloud they can significantly enhance their current infrastructure or application services with minimum cost and maximum elasticity. But securing cloud user digital assets and addressing privacy concerns of cloud customers has become serious challenge. Providing security in cloud always has to consider performance. Employing high secure methods with massive complexity will increase overall service cost, to address this problem in this paper a two-tier security architecture is proposed. This architecture use multiple work mode for security components in guest level to decrease security process over-head and a security supervisory in hypervisor layer to make sure avoiding from false security alarms.

Keywords: Component, Cloud, Security, Secure Sandbox, Cloud Security Architecture.

1 INTRODUCTION

Cloud computing is a new model for service based computing which aims to provide on-demand, low-cost, high-performance processing and storage and other computing resources. Cloud computing quick growth brought new generation of security threats and issues in addition to reformed classical security threats in cloud [1].

As a result of the growth of the technology, organizations have two different choices whether using existence technologies which are stable or new developing technologies. Virtualization is one of such developing technologist. Presently, in numerous organizations, virtualization has been converted to an approach of life. This technology has been employed to various parts of IT like: systems, networks, security and applications. Currently, the extensive evolution of this technology can be witnessed in cloud computing [2].

At the beginning virtualization was used for time sharing. Time sharing makes the computer programmers able to work on an enormous identical mainframe computer on their selected consoles in addition to eliminates waiting time. Due to portioning feature many of processes and applications were capable to execute at the same time. This improved the overall effectiveness of the computing environment and decreased the maintenance process [3, 6]. This general concept of enhancing resource utilization, and decreasing the maintenance was the main idea of the virtualization technology. Nowadays, this technology permits users and IT developers to have one physical host and execute several operating systems and discrepant applications on it.

Based on the present literatures, there are great discrepancies between virtualization meanings. Generally, it is believed that virtualization denotes to the computer components which deliver assumed functionality of real physical components in form of a managed abstract level.

In simple words virtualization is a technology which presents a layer of abstraction between
computer resources (underlying hardware and operating system). This layer of abstraction is well known as virtual machine monitor (VMM). VMM is a software abstraction which is located between the physical layer and the operating system that leads to running multiple virtual machines on each unit. Users observe each virtual machine (VM) as a single computer which is separated from the other one. All main privileges and controls over VMs are assigned to VMMS which has the ability to manage one or more VM and allocate adequate physical resources for each of them [2, 3, 5, 7].

In order to attain resource sharing Virtualization technology is able to run different operating systems independently on a single hardware [8]. The key intention of virtualization is to make the IT infrastructure simpler, and is able to simplify access to resources and resource administration. The resources are accessed to users via standard interfaces which are supported by the virtual resources. In the situation where there is variation on the underlying physical resources the client’s use is not influenced. Simultaneously, the general management of IT infrastructure can be made simpler because virtualization trims the coupling amongst the client and the resource, such that the client does not rely on a particular physical resource.

2 SECURITY ISSUES

However, when virtualization is employed to cloud computing it conveys different security risks and vulnerabilities which could be exploited by malicious users and cause main security events. In the following the most important risks of private cloud virtualization and their general solution are discussed [9].

2.1 Access Control Vulnerability

One of the most important security issues in the security field is access control in all network types. Access control means that different users have discrepant privileges to access the data and each user based on its rights has accessibility to part of the data. So, we need different security policies to protect data. The number of users is not effective in the protecting system. The standard for all data and applications in virtualization platform is the same, so the security policies which apply to accessing different data and applications are as well the same. As each user has its own privileges to access each part of the data and applications, the user can only have access to the portion of data that is permitted to his/her and the other part of data which the user does not have permission to access, is hidden from him/her. Thus, access control prevents the users to access sensitive data that the user does not have permission to access.

2.2 DOS attack Control Vulnerability

When the total number of clients and application services demands to grow intensely, the load capability balancing and migration approach should be employed to transfer to an alternative work area. Simultaneously, audit methods should be performed for clients who apply facilities, analyze every application in order to avoid a malicious client to apply a great deal of resources on the virtual platform. When disaster occurs, the virtual platform would go down and information loss would happen. It is necessary for the virtualization platform to recover quickly and continue to operate as ordinary mechanisms. Symantec’s which is a data protection recovery solution could be used for data security and disaster recovery [10].

2.3 Virtualization Platform Vulnerability

For a solution to this vulnerability a single administrator could be setup in each virtualization zone which may consist of two processes. The first process is a real time process executing in a safe zone tangled in virus and Trojan cleaning and repairing bugs. While, the second process which is located in an inaccessible region communicates with the outside world in order to update the virus library and gain information about the newest vulnerabilities and get those patches.

2.4 Vulnerability of Security Management inside Virtualization Platform

There are some security issues in designing virtual platforms. Sometimes despite the existence of security policies these types of problem can’t be solved. One solution to overcome this risk is to associate some new security mechanisms to virtualization platforms. All security mechanisms like firewall, intrusion detection, log checking, etc. are potentially useful to increase the security of virtual machines.

Due to providing the assurance that integrity and authentication of log file is supported, digital signature and digital watermarking mechanisms can be used beside the other security mechanisms. It is necessary for the virtual machine to use an embedded VMM. So, a security mechanism is required to monitor the invisible VM backboard flow for the equipment which is used to monitor the traditional network security.

Allocation of physical resources to each virtualized operating systems and applications
which run on top of it is one of the VMM duties. VMMs handle communications between physical resources and virtual OSs. [4, 11].

For controlling the physical resources, VMMs eliminate dependency between OS physical hardware resources. So, independent operating systems can run on the same platform concurrently.

Each VMM has three main attributes:

The first attribute is isolation. VMMs are responsible for controlling the allocation of the physical resources to each of VMs indeed. Due to isolation of each VM from the other ones, VMMs assign individual address spaces to each VM. In this way interactions and applications in a VM is hidden from the other one [11, 13].

The second VMM’s attribute is Inspection. VMMs have access to state of all host physical resources which contains: memory state, CPU and device state. Inspection makes each physical host protected from the other one when administrators save, copy, and move and instantiate environment [11, 13].

The third attribute of VMM is interposition. Administrative privileged instructions on hardware should be managed by VMMs. Virtual machines monitors interact directly with hardware which is on behalf of the guest OS to gain all guest OS’s traps and interrupts. All input/output requests from guest OSs are obtained by VMM [11, 13].

Clustering is another virtualization attribute. With clustering technology several different physical layers can host one or more virtual servers. Clustering has two main advantages.

The first one is to allow access to the data constantly. Clustering helps to have stable access to data, even when some parts of the system or networks breakdown. Another advantage of clustering is that it increases the load tolerance of the system even when a large number of users work with the system [3].

The security requirements of virtual machine monitoring systems are defined as [14]:

Effectiveness: The system must be capable of identifying most types of attacks and integrity harms.

Precision: The system must be capable (preferably) of avoiding false-positives, which is, incorrectly identifying malware attacks where official events are happening.

Transparency: The system must reduce visibility from VMs, which is, SP, SU, and possible invaders must not be capable of identifying the existence of the monitoring system.

Non-subvertability: The VMM system, cloud infrastructure and the sibling VMs have to be secure from attacks happening from a compromised client as well as, the monitoring system must not be feasible to inactivate or modify.

Deployability: The system must be capable of being implemented on all public and private clouds with the employment of the middleware and facilities in the general cloud model.

Accountability: The system must not have an interference with the cloud and its application activities; however information and snapshots should be gathered to impose accounting functionalities.

Consequently, virtualization makes high possibilities in the field of business. However, all virtualization technologies are combined to make a single architecture when the different security risks joined with it.

One of the most important concerns of virtualization is security. So, IT experts should identify the hint which joins to each of virtualization platforms. Thus, it is essential to set up some solutions for security challenges.

3 INTRUSION DETECTION SYSTEM

Monitoring malicious activities of a network and a system is one of the duties of IDS. IDS could be a hardware device or software. It can also monitor policy violations. At last, it makes reports based on monitoring information. Then it announces the reports to Management station or administration of system which can decide whether it is a correct or false alarm. If it is a correct alarm, it should take action on this intrusion [15, 17].

Host-based and Network-based are two different types of intrusion detection systems:

- Host-based intrusion detection systems (HIDS) involves an agent on a system/host that can analyze system calls, file-system modification and other host’s activities and current state to detect intrusion on the system[18, 19].

- Network intrusion detection system (NIDS) is another type of IDSs which can recognizes intrusion by monitoring multiple hosts that are connected to the network and also by network traffic examination. For examining traffic, first, it
should capture all traffic in the network and then it should analyze each packet’s content to delete malicious traffic [18].

Intrusion prevention system (IPS) is a system module in which intrusion detection can be performed at first and then it makes the way to stop potential intrusions which is detected [20].

The most important aims of Intrusion Detection and prevention systems (IDPS) are: initially, detection of potential intrusions. Second, log of information about the intrusions. Third, finding a way to stop intrusions and finally it should announce to the security administrator about them.

3.1 IDS in Cloud Systems

Although IDS is one of the most effective security mechanism that is used in all classical commercial systems, but is not efficient and successful in cloud computing environments where the resources are mutually used between different clients according to requests and pay-per-use basis. Consequently, an efficient mechanism to deliver security must be included in the cloud environment in order to identify and avoid vulnerabilities which start from the cloud as well as the client who takes privilege of this technology from various locations [21].

There are three different models: anomaly, misuse and specification model [18, 22]. Anomaly model specify bad behaviors as “bad”. Misuse model checks states and actions against intrusion actions to see whether they match or not. Those states are defined as “bad” if they match. Moreover, states which violate the specification as bad are defined in the specification model. The models could be adaptive or static. In the adaptive model, neural networks are used in order to identify various types of intrusions. While, in the other model intrusion is determined [18].

4 PROPOSED MODEL

In order to fulfill cloud security monitoring requirements we proposed a solution that would focus on active monitoring while still provides a light weight passive monitoring. Our architecture adds some new components to the general cloud model (see figure 1) which will enable detection of any unauthorized system manipulation. In abstract, system provides data integrity by logging almost all the system modifications. To avoid extra over-head on VMM cloud default accounting functions will do the loggings.

![Fig. 1. Proposed model implemented on blue layers](image)

To reach a generalized solution, each VM contains an IDS unit which only works on data flows and if any anomaly is detected it will be reported in to the specific guest middleware and also firewall unit inside VMM. The VM which is suspected to intrusion will be blocked and all processes will get suspended. But, to provide transparency a sandbox will continue to respond illegal activity. Keeping a suspected process active will help to make sure avoiding false alarm and also to distinguish, attack type and selecting a prevention policy.

The sandbox has direct access to the protected memory space and processing power hardware layer. Through host-OS, this will gives sand-box ability to hide its process from attacker. The next module inside VMM is VM communicator. VM-communicator provides secure channel between VMs, also a firewall service which directly has access to access control list (ACL). Using ACL gives the provider the ability to act on VM to VM communication requests based on service level agreement. For SLA and ACL there are two separate databases located in VMM (see figure 2).
Another VMM duty in the system is to enhance cloud provider required functionalities to fulfill accountability. In addition to usage data gathered from guest OSs. These data are assumed as a reference of system behavior. To reach a higher level of security Process Registry is added to VMM, this module provides library in VMM. This library includes all legal process signatures. By using these signatures any anomaly in main system process can be detected very fast.

Sandbox-handler includes methods and system objects which are required creating an isolate area in processing and memory space (see figure 3).

4.1 Model details

Our model is dependent on selecting effective IDS method. IDS is not going to be discussed in the proposed solution, the model only specifies the location of IDS, since based on application and assumption various IDS might be used. Another assumption in designing this model is based on considering cloud default usage logging. Any anomaly in resource demand could be a potential attack.

It is necessary for the proposed solution to meet general computer security requirements such as confidentiality, integrity [18]. Encryption is one of the most elementary requirements to provide confidentiality and authentication. A problem exists in securing virtualization; a key sharing method or the compulsory use of unencrypted data transmission by the user is required. However, our model is introduced without any assumption on encryption.

In figure 2 the main system model consists of two components: Host level security analyzer (HLSA) module which monitors alarms from Guest Level Security Analyzer (GLSA) and also sandbox. The HLSA reports VMs status in three form, normal behavior, and aggressive behavior or attack objective. In addition to this HLSA signals firewall module inside inter-VM communicator to apply required actions.

The main role of the GLSA is gathering information about guest activities as well as supervisory control over guest machine. GLSA works in two mode silent and pursuit. Silent mode works until Virtual Machine Behavior Monitor (VM-BM) detects an anomaly in process resource usage or an unknown process starts to work (new process is a process which is not registered in process registry).

To monitor the behavior and workload of the VM-BM is attached to the GLSA (see figure 4). It constantly monitors system load and compares the results with cloud controller loges. Any anomaly within system will be reported to HLSA. At this point HLSA will decide whether it is a normal behavior or not. If it is normal a signal will be sent to cloud controller for resource allocation. Otherwise, the restriction process will be started.

5 CONCLUSION

In this paper, set of modules are proposed in order to add a distributed security machines in to the cloud which is useful for all service models, because it is deployed over virtualization and guest-OS. Resource consumption of security processes is controlled through multi-work model.

The well divided and dispatched security workload will keep communication between guests–OS security module on a minimum level. It is very important since cloud controller functions naturally have overload on the VMs. Transparency is provided by employing protected sandbox which provides an environment to follow risks or attack
behavior. This will equip the system with the ability to kill illegal process and continue legitimated activities.

6 FUTURE WORK

In order to evaluate our model in future works, the proposed solution will be implemented in to the Eucalyptus [23]. Default Eucalyptus configuration will be compared with proposed architecture in term of performance and security. In order to security evaluation a set of attacks will be selected which is harmonized with Eucalyptus known vulnerabilities such as signature wrapping attacks, Cross Site Scripting attacks and specifically script injection attacks. The goal is experiment a realistic distributed attack to reach this Open Computing Language (OpenCL) is going to be attack development platform.

7 REFERENCES

[1] L. McLaughlin. (2008, Cloud Computing Survey: IT Leaders See Big Promise, Have Big Security Questions. Available: http://www.cio.com
[2] F. A. Bazargan, Y. Chan Yeob, and J. Zemerly, "Understanding the security challenges of virtualized environments," in Internet Technology and Secured Transactions (ICITST), 2011 International Conference for, 2011, pp. 67-72.
[3] Blate, Alex, and Kevin Jeffay. "Gini in a Bottle: A Case Study of Pareto's Principle in the Wild" International Journal of Computer Networks and Communications Security 1.1 (2013).
[4] J. Hoopes, Virtualization for security: including sandboxing, disaster recovery, high availability, forensic analysis, and honeypotting: Syngress, 2008.
[5] J. Sahoo, S. Mohapatra, and R. Lath, "Virtualization: A survey on concepts, taxonomy and associated security issues," Bangkok, 2010, pp. 222-226.
[6] S. J. Vaughan-Nichols, "Virtualization sparks security concerns," Computer, vol. 41, pp. 13-15, 2008.
[7] E. Ray and E. Schultz, "Virtualization security," presented at the Proceedings of the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies, Oak Ridge, Tennessee, 2009.
[8] J. W. Rittinghouse and J. F. Ransome, Cloud computing: implementation, management, and security: CRC, 2009.
[9] K. Ren, C. Wang, and Q. Wang, "Security challenges for the public cloud," IEEE Internet Computing, vol. 16, pp. 69-73, 2012.
[10]L. Xiangyang, Y. Lin, M. Linru, C. Shammaing, and D. Hao, "Virtualization Security Risks and Solutions of Cloud Computing via Divide-Conquer Strategy," in Multimedia Information Networking and Security (MINES), 2011 Third International Conference on, 2011, pp. 637-641.
[11]P. A. Karger and D. R. Safford, "I/O for virtual machine monitors: Security and performance issues," Security & Privacy, IEEE, vol. 6, pp. 16-23, 2008.
[12]L. M. Kaufman, "Can a Trusted Environment Provide Security" Security & Privacy, IEEE, vol. 8, pp. 50-52, 2010.
[13]K. Nance, M. Bishop, and B. Hay, "Virtual Machine Introspection: Observation or Interference" Security & Privacy, IEEE, vol. 6, pp. 32-37, 2008.
[14]F. Lombardi and R. Di Pietro, "Secure virtualization for cloud computing," Journal of Network and Computer Applications, vol. 34, pp. 1113-1122, 2011.
[15]C. P. Pfleeger and S. L. Pfleeger, Security in computing: Prentice hall, 2003.
[16]T. F. Lunt, "A survey of intrusion detection techniques," Computers and Security, vol. 12, pp. 405-418, 1993.
[17]B. Mukherjee, L. T. Heberlein, and K. N. Levitt, "Network intrusion detection," IEEE Network, vol. 8, pp. 26-41, 1994.
[18]S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, and A. Misra, "Intrusion detection system in cloud computing environment," presented at the Proceedings of the International Conference #38; Workshop on Emerging Trends in Technology, Mumbai, Maharashtra, India, 2011.
[19]F. A. Bin Hamid Ali and Y. Y. Len, "Development of host based intrusion detection system for log files," 2011, pp. 281-285.
[20] S. Anand and V. Ramachandran, "A generic model for an application based intrusion prevention detection system," Computer Systems Science and Engineering, vol. 19, pp. 233-240, 2004.

[21] K. Vieira, A. Schulter, C. Westphall, and C. M. Westphall, "Intrusion detection for grid and cloud computing," IT Professional, vol. 12, pp. 38-43, 2010.

[22] M. Bishop, "Computer Security: Art and Science. 2003," ed: Addison-Wesley.

[23] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-Source Cloud-Computing System," in Cluster Computing and the Grid, 2009. CCGRID '09. 9th IEEE/ACM International Symposium on, 2009, pp. 124-131.