ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

Virtual Machine Introspection: Security Architecture Overview

Swati Nirwal [1], Komal Pujari [2], Sakshi Rawat [3], Preeti Nagrath [4]

U.G. Student, Computer Science Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India[1]

U.G. Student, Computer Science Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India[2]

U.G. Student, Computer Science Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India[3]

Assistant Professor, Department of Computer Engineering, Bharati Vidyapeeth's College of Engineering, New Delhi, India[4]

ABSTRACT: The most serious issue in cloud computing is security which is a big hardship for the adoption of cloud. Some critical threats of cloud computing are multi-tenancy, loss of control, loss of data, outsider attacks, malicious insiders, availability, etc. Among many security issues in the cloud, virtual machine security is one of the very severe issues. Hence, monitoring of virtual machine (VM) is essential. Virtual Machine Introspection (VMI) depicts the mechanism of monitoring and analyzing the state of a virtual machine from hypervisor level. This paper focuses on the mechanism of monitoring virtual machines aimed at guaranteeing increased security to the cloud resources using security tools (VMI). It also includes a study of different architectures for providing the security and monitoring of virtual machines.

KEYWORDS: Virtualization, Security, Introspection, Intrusion Detection, Hypervisor

I. INTRODUCTION

Cloud Computing has become the most booming era of the IT technology. It is defined as a system, where the users or an enterprise share their data using virtualization technology. Cloud services provide elastic, on demand and instant services to the customers or users and charges customer usage as utility bill. Pay-as-you-Go, Elasticity, Scalability and Virtualization are considered some of the essential characteristics of Cloud Computing Model [1, 12]. With the aid of Cloud Computing come along challenges to this model. Security is the most challenging and serious concern in cloud which sometimes overrules its benefits. The issues with security can be grouped into sensitive data access, privacy, bug exploitation, recovery, accountability, malicious insiders, control of account, and multi tenancy issues. One of biggest challenges of security issues while designing of a cloud computing platform is that of virtual machine instance interconnectivity [11]. Because users who are having super-user access to their provisioned VMs may create a possibility where a VM can monitor another VM or access the elemental network interfaces, which is regarded as the break of isolation.

System virtual machine acts as a substitute for a real machine. VM's provide functionality needed to run the entire OS. Many operating systems and software can be installed on the virtual machine. A hypervisor uses native execution to share and manage hardware allowing for multiple environments which are isolated from one another yet exist on the same physical machine. Virtual machine attacks include VM-to-VM attacks, attacks on Hypervisors, Denial-Of-Service attacks, Isolation breakage, Remote management vulnerabilities etc. Thus the virtual machine monitors are used to inspect or monitor the virtual machines. VMI is one of the techniques used for monitoring the state of virtual machines in real time.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The contributions of this paper are as follows:

- It thoroughly inspects VMI techniques and frames their advantages and weaknesses.
- It summarizes various possible attacks and threats to VMI techniques.

The paper gives the overview of the topic in section II. Preliminaries and Related work are discussed in the section III. The proposed VMI is being explained along with enhanced-architecture and flowchart in the section III. The conclusion for the paper is given in the section IV.

II. RELATED WORK

Virtual Machine Introspection (VMI), which has its origin in cloud enabling technology virtualization, can effectively change security deployment in cloud environments. Virtual machine introspection is a way to monitor the virtual machine execution [10]. In [2], the authors proposed virtual machine introspection (VMI) to describe such virtualization assisted examination or scan and analysis. As no agents are needed to be installed in VMs, VMI is stealthier than traditional host security tools such as Firewall and Antivirus software. However, the precondition of VMI's functioning is the security of hypervisor, where VMI tools are deployed.

A. ADVANTAGES OF VMI

• A complete and untainted view of the system state.
• The ability to maneuver the VM state.
• A consistent view of the system state, since the VM may be paused.
• Complete isolation of the VMI structure from the guest or host operating system (OS).

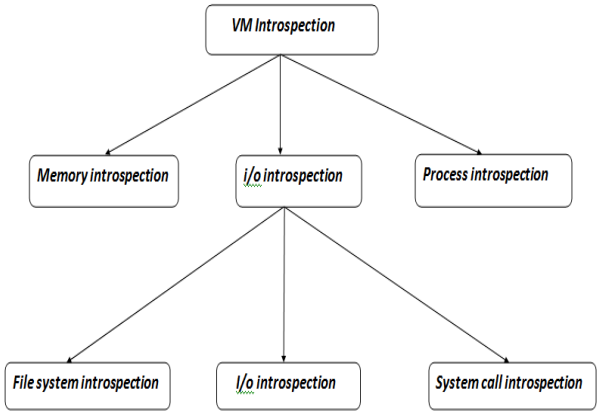

Fig. 1. Classification of VMI Techniques

B. CLASSIFICATION OF VMI

The events in a guest VM and a guest OS can be related and arranged to have introspection at various degrees [3]. Below is a brief overview:

1. Memory Introspection: Memory introspection is associated with live memory analysis. While the OS is active, the critical data structures are in the main memory. Different VMI techniques exists to access the main memory of a guest VM from a secure VM, which can be used for tasks such as intrusion detection or process analysis of the guest VM as depicted in Fig.1.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

2. System Events Introspection: I/O introspection deals with device drivers and other utility hardware communications.
(a) System Call introspection: System calls handles events such as context switching, memory access, page table access and interrupt handling. In virtualization technology enabled processors, the transition of a guest VM to the hypervisor and vice versa is managed by special system calls.
(b) Interrupt Requests Introspection: The VMI method is used to trace interrupt requests to detect process switching.
(c) I/O Device Driver Introspection: I/O device driver introspection deals with utility hardware communications.

3. Live Process Introspection: Process Introspection can be used debug any process during its execution cycle. It helps in the analysis of code and is useful for malware behavior analysis and debugging.

III. PRELIMINARY

Virtual Machine Introspection [4] can be conceptualized by the VMI architecture which is depicted in fig. 2. The VMI capably identifies the DOS attacks for the virtual machines based on predefined threshold access count values. The architecture consists of a Gateway Server and two cloud servers. The virtual applications runs in two cloud servers with separate VMI agent running in these two servers as depicted in Fig.3. The application is accessible to two different types of users which are admin and end users. The requests by users are received by the cloud servers via the gateway server. Various network activities are controlled by the network controller which consists of various VM profiles. Admin can login to monitor the status of the machines connected, state of servers and applications, and admin also has the right to change the password. Any application on the cloud server can be accessed by the end user using a common user interface. This architecture involves three modules which are VMI Agent, Attack Analyzer, and Network Controller.

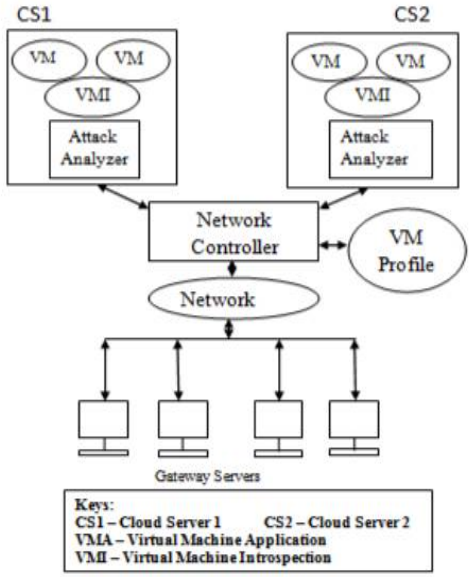

Fig. 2. Virtual Machine Introspection Architecture

The VMI agent monitors the connection activities in the network and alerts the attack analyzer about the threats for further detection. Each VMI agent running on two cloud servers is assigned a predefined threshold access value. When a cloud server receives request by an IP address, the agent obtains its details from the log file and increments its count. If that particular IP has accessed the applications more than the VMI agent's threshold access count value then it will

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

send an alert notification to the attack analyzer module. VMI agent and attack analyzer is further implemented to increase a level of security.

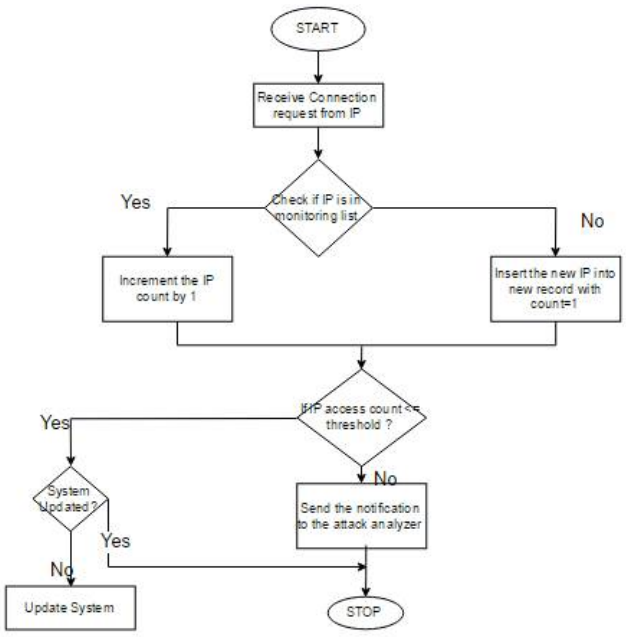

Fig. 3. VMI Agent

There are three dominant challenges that can be identified in the development of VMI-based applications, i.e., interpreting the state information, identifying relevant state information, and classification of states [2]. They have reasoned and approached the theoretical limitations of a VMI-based IDS, considering it from an intrusion detection prospect.

The way of inspecting a virtual machine from the outside with the objective of analyzing the software running inside it is virtual machine introspection (VMI). In [5], Garfinkel and Rosenblum present the vast potential that VMI has for intrusion detection, as well as other fields within IT security. For building intrusion detection systems, they presented a new architecture that provides good visibility of the monitored host, while still providing strong isolation for the IDS, hence providing significant resistance to both evasion and attack.

A design focused on encrypting the VMI, named CryptVMI [7], was proposed which could keep the virtual instance's confidentiality from the admin of the cloud and the user gets the full status of their VM instances. The design has two components - *Query Handler* and *Introspection Application.* The user's queries are verified and encrypted by the handler and further sent to the introspection application which decrypts the command and transfers back the decrypted result to the client.

VMI can also be offered as a cloud service where users can request introspection for their virtual machines [8]. This gives the customers certain privileges such as monitoring of their own virtual machines without security compromises. Hence the cloud VMI has a capability to form cloud-centric applications based on VMI that can execute VMI functions from a centralized perspective on distributed virtual machines.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

The paper titled "Leveraging VMI for Hot-Hardening of Arbitrary Cloud-User Applications [9]" proposed a security agent named Security Monkey with back-end network architecture which aims to significantly improve security settings of cloud users. This architecture employs VMI techniques to access current configuration settings and locate, read and write potential settings of running applications.

IV. PROPOSED WORK

This model classifies a VMI system into its basic components and their interactions, thus reflecting important design decisions.
The VMI architecture which is depicted in Figure.2.comprises of three modules such as VMI Agent, Attack Analyzer, and Network Controller which effectively detects the attacks for the virtual machines based on predefined threshold access count values.

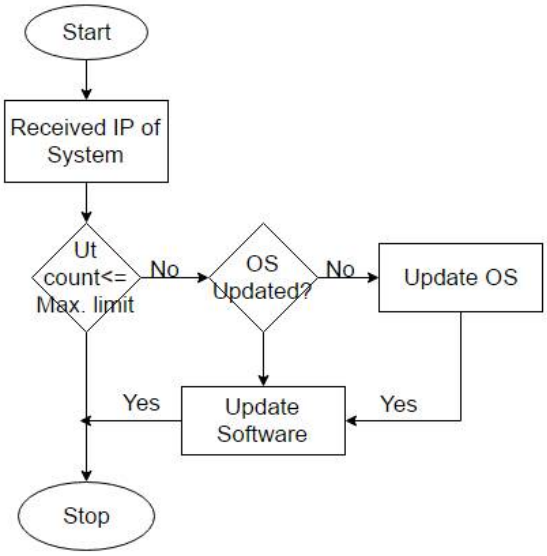

Fig. 4. Update Checker

The proposed model architecture introduces an additional layer of security known as Update Checker [6] which is proposed to check the virtual machines for the necessity of updates. The main concept of the Update Checker is forming a central database which will contain all the information such as list of installed packages, the exact version of the installed package and list of repositories that are used for each VM. This model gives a combined approach that checks for software updates, OS Updates and scans virtual machines for known security vulnerabilities as shown in Fig.4.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

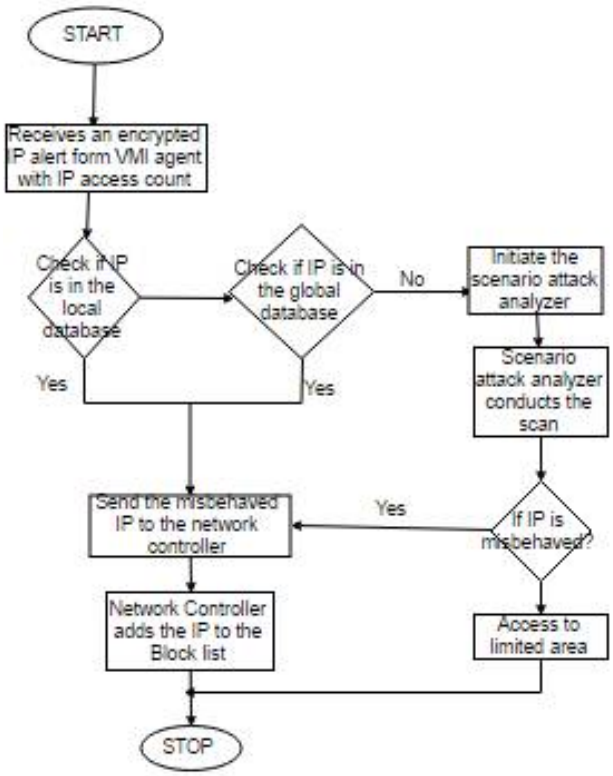

Fig. 5. Attack Analyzer

When cloud server receives a request by an IP address the agent will obtain its details from the log file and increment its count. If that particular IP has a count less than the VMI agent's threshold value, it will check whether the system is updated or not. Checking of update will be done to know which software is actually outdated or affected by some remote security vulnerabilities. If that IP has accessed the applications more than VMI agent's threshold access count value then, an alert notification will be sent to the attack analyzer module as depicted in Figure.5.

V. CONCLUSION

In this paper, we reviewed the existing VMI architectures and proposed an enhanced VMI architecture to detect the attacks and increase cloud security. The misbehaved users should be successfully blocked at the gateway level using VMI agent and attacker analyzer. The VM will be checked for updates for security vulnerabilities using Update Checker. In such cases, the user would not be given permission to access the hidden files of the admin.

REFERENCES

[1] AlJahdali, Hussain, et al. "Multi-tenancy in cloud computing." Service Oriented System Engineering (SOSE), 2014 IEEE 8th International Symposium on. IEEE, 2014.
[2] Pfoh, Jonas, Christian Schneider, and Claudia Eckert. "A formal model for virtual machine introspection." *Proceedings of the 1st ACM workshop on Virtual machine security*. ACM, 2009.
[3] More, Asit, and Shashikala Tapaswi. "Virtual machine introspection: towards bridging the semantic gap." *Journal of Cloud Computing* 3.1 (2014): 1.
[4] Rachana, S. C., and H. S. Guruprasad. "Virtual Machine Introspection." *Compusoft* 3.6 (2014): 860.
[5] Garfinkel, Tal, and Mendel Rosenblum. "A Virtual Machine Introspection Based Architecture for Intrusion Detection." *NDSS*. Vol. 3. 2003.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 2, February 2017

[6] Schwarzkopf, Roland, et al. "Increasing virtual machine security in cloud environments." *Journal of Cloud Computing: Advances, Systems and Applications* 1.1 (2012): 1

[7] Yao, Fangzhou, and Roy H. Campbell. "CryptVMI: Encrypted Virtual Machine Introspection in the Cloud." *2014 IEEE 7th International Conference on Cloud Computing*. IEEE, 2014.

[8] wook Baek, Hyun, Abhinav Srivastava, and Jacobus Van der Merwe. "Cloudvmi: Virtual machine introspection as a cloud service." *Cloud Engineering (IC2E), 2014 IEEE International Conference on*. IEEE, 2014.

[9] Biedermann, Sebastian, Stefan Katzenbeisser, and Jakub Szefer. "Leveraging virtual machine introspection for hot-hardening of arbitrary cloud-user applications." *6th USENIX Workshop on Hot Topics in Cloud Computing (HotCloud 14)*. 2014.

[10] Nance, Kara, Matt Bishop, and Brian Hay. "Virtual machine introspection: Observation or interference?." *IEEE Security & Privacy* 6.5 (2008).

[11] Wu, Hanqian, et al. "Network security for virtual machine in cloud computing." *Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference on*. IEEE, 2010.

[12] Aljahdali, Hussain, Paul Townend, and Jie Xu. "Enhancing multi-tenancy security in the cloud IaaS model over public deployment." *Service Oriented System Engineering (SOSE), 2013 IEEE 7th International Symposium on*. IEEE, 2013.