Indonesian Journal of Electrical Engineering and Computer Science
Vol. 4, No. 3, December 2016, pp. 643 ~ 648
DOI: 10.11591/ijeecs.v4.i3.pp643-648

VMM based Secured Virtualization in Cloud-Computing

P. ILA Chandana Kumari[1], S. Swarajya Laxmi[2], B. Rekha[3], B. Pravallika[4], G. Chaitanya[5]
Syed Umar[6], Azeem Mohammed Abdu*[7]
[1,2,3,4,5,]Department of Computer Science Engineering, Institute of Aeronautical Engineering, Hyd
[6]Department of Computer Science Engineering, MLR Institute of Technology, Hyd
[7]Department of Electronics and Communications, KL University, Vaddeswaram
*Coresponding author, e-mail: mohammedazeem123@gmail.com

Abstract

Cloud computing, utility computing, the future will be the main IT field. The government and companies are realizing that foreigners can clearly increase the cloud with minimal costs and maximum flexibility in the plant or existing equipment. But the clouds to ensure user privacy and digital asset management challenge in cloud client. Protection must always contain a performance. The complex is a sure way to end the occupation of the problem; the study suggests two Ebionitism security architecture. The movement and different approaches to health and safety and the level of the best things for their security costs hyper-visor layer to a reduction in order to avoid false alarms.

Keywords*: cloud computing, virtualization, security.*

1. Introduction

Cloud computing is on-demand services as a result of the new models, low-cost, high-performance computing and storage resources. In extreme compute density for the next generation of threats and challenges to the development, as well as the classic security change threatens to Cloud Security [1]. Therefore, the development of the technology, organization, two different technologies in the forest or a new technology. Virtualization is one of the technologists. Now there are many organizations, virtualization and conversion. The technology works in many IT areas: systems, networks, security and applications. Now the development of this technology see in cloud computing.

Initially, virtualization using time division. Time-sharing computer programmers working on large mainframe console to download it to eliminate the wait. Because doses for different processes and applications simultaneously. Its environmental performance of the best overall settlement systems [3, 6]. The idea of service and reduce the maintenance of the basic concept of virtualization technology. Today, technology allows users and IT developers with some physical and multiple operating systems and inconsistent data. There is no contradiction between the book currently virtualization solutions. In general, we believe that virtualization of computer components for the performance of system components in the form of normal levels of available. In simple words, a virtualization technology that starts with a layer of abstraction computers (hardware and operating system). Abstraction layer called a virtual machine monitor (VMM). VMM is a layer of software abstraction between the physical and operating system to run multiple virtual machines on each unit. The value of work each virtual machine (VM) on the computer is different. VM VMM adjustment and control of one or more VMs and all physical distribution of their works [2, 3, 5, 7]. Being different from the local virtualization technology for their operating systems running on the same hardware [8]. The main intension virtualization and IT infrastructure, and can easily access the services and support. It was supported by the example of the job interview from a virtual office side. Questions about other unrelated changes to the user. At the same time, the IT infrastructure will be easier because trims pairing virtualization of people and goods, so people do not think.

Received September 27, 2016; Revised November 5, 2016; Accepted November 30, 2016

2. Security

But although some risks of job security and virtualization vulnerabilities can be exploited by the security services and content. Here are the main risk to the private cloud virtualization and discuss [9].

2.1. Vulnerability Access

One of the main security issues should be on the network and security areas. The access means to provide multiple users with different access rights to the data and all legal files. Therefore, it is important that a wide range of data security policies. Number of users of the system. The procedure for each platform and application virtualization of the data, and then the safety devices in order to obtain a series of data and applications, as well as the team. Because everyone has the right to access the data in the application, the user can send as part of the file to him/her, and other information the user access mentioned. As a result, no user control sensitive data and allows the user to use.

2.2 Check the Vulnerability to DoS Attacks

When you can use all the people and the equipment they need to grow strong, and can make the approach to immigration to switch to another workspace. At the same time, the search will be those in force, review each application to avoid damaging files on a virtual platform. When a disaster occurs, the virtual platform down, the loss of data occurs. It is important that the virtualization platform to quickly recover and continue working as usual. Symantec will use solutions for data protection for data security and disaster recovery [10].

2.3 Virtualization Platform

The solution is configured virtualization vulnerabilities, which may include various processes. The first method is devoid of real-time virus and Trojan wolves perform the care and treatment of the disease. When both are still inaccessible to communicate with the outside world, the virus changes the library and information on the latest vulnerabilities and patches to find the host hardware.

2.4. Virtualization Security Management Platform Vulnerabilities

Some security develops a virtual platform. Perhaps for the security policies, such problems can not be solved. This is a way for the various safety systems and the new virtualization platform to overcome. All safety systems and firewalls, intrusion detection, access control, security and other services connected to the virtual machine. It supports the log file is backed up and can be used to create a water system and other security systems. It important to look around and try to VMM virtual machine. Therefore, for system monitoring control of invisible security fence VM product which is used in the conventional network security. physical resources each virtual operating systems and applications to run on one of the VMM. VMM cultural communication between the physical and virtual operating systems. [4, 11]. Manage shared resources, remove plaque OS VMMS physical hardware resources. Therefore, the independent operating systems running on the same platform. VMM has three main tasks:

1) The first is the quality of insulation. VMM attribution of responsibility for the management of common resources to each VM. Since each VM isolation from other VMM came into position on each VM. Consequently, the interaction with the World and others [11, 13] in position.
2) Program the second evaluation VMM. Have access to all the resources VMM: vehicle condition CPU status and unity. Researchers against each other, or other guidelines, copy, move, and create an instance for the environment [11, 13].
3) The third aspect is administered VMM. Administrative information VMM able to control the hardware. Virtual machines can communicate with the hardware that represents the guest operating system to access the guest operating system and level. All visitor applications input / output VMM OSS [11, 13].

Virtualization source instructor. The cluster technology, the most common layer includes one or more virtual servers. Two main advantages group, the first is that the access to the data will be preserved. Clustering helps physical access to the data, although some parts of the body or tissue damage. The second is to improve education and tolerance, even if a large number of users working on [3] system. The security needs of the virtual machine monitoring system [14]:

1) Efficiency: The system should be able to most of the fighting and the truth hurts.

2) Accuracy: The system will be able to avoid (if possible) false positives do not know a heart attack when the policeman.
3) Elegance: The system lowers VM visibility, SP, on, and the occupants, knowing that a monitoring system.
4) Sub-vertability: VMM systems, infrastructure, cloud and VM will be safe from damage caused by the attack, the system can be turned off or control to overcome.
5) Setup: The system will be able to use all forms of public and private cloud services and the general characteristics and middle-ware.
6) Dynamic Response: It can control at the time of the attack system to strengthen, and if it comes to the necessary protective measures, it is recommended that it is important for conservation efforts and waste of customers and / or security middle-ware components remotely.
7) Applications: The system does not affect the use of the cloud and activities; However, the images are stitched by the providers to adapt.

So, in business opportunities virtualization. But virtualization, and consolidate the various risks to important security issues of the it.One virtualization security technology. Therefore, experts have reported that the board contact the virtualize- platform. Therefore, it is important to say that some of the security issues.

3. Sensor System

Network monitoring and one of the tasks of the IDS system. IDS can be hardware or software. We love the damage. Finally, the foundation is information about the track. So tell the police management and administrative systems to determine whether the alarm is true or false. If this is a warning, you need to take action during the invasion [15, 17]. Detection systems, host-based or network-based intrusion in two ways: host host-based intrusion detection (HIDS) System Agent / when the system needs to identify, exchange and other user activity and the current status of the installation in [18, 19] system. A Network Intrusion Detection System (NIDS) in any other form of IDS detects intrusions by monitoring multiple hosts connected to the network testing and network traffic. The study of the road, which was to establish the first all traffic on the network and you need to check the contents of each packet of traffic [18].

It is to Intrusion Prevent System (IPS) is a modular system that can make possible in a bag, and then make your way to the intrusion detection to stop [20]. The main purpose of intrusion detection and prevention (IDP) in an open system. Second, enter your system information. Third, find a way to decline and eventually given to stop security officials.

3.1. Cloud IDS

When IDS is one of the immune system is effective for all traditional business processes, but the area is not cloud computing efficient and successful use of its resources as opposed to every need of the customer and a pay per use. Therefore, an effective system in question to achieve a secure cloud environment, and start watching with cloud and client to use the privileges of the different technological areas [21].

Four forms of the Council: In view of the need to accommodate safety of cloud solutions better, while providing a simple family supervision. The movement is equipped with the latest in the public cloud model (see Figure 1), which detection unauthorized processing system. Detected physical integrity, the change virtually all systems. In order to prevent the increase of standard will give access to the VMM head in the clouds.

Access to full resolution to each device IDS VM, work on the road, or if you notice anything unusual in the firewall, where guests VMM middleware and devices registered trademarks. A VM should be closed and not closed single system. But understand sandbox to respond to illegal activities. Helps keep active needs to have the system to false alarm, as well as avoid the type of warfare to prevent the choice of a difference. Sandbox offers direct access to the secure memory and processing power of the hardware layer processing. And the host operating system sandbox can offer sound system. The following internal devices and media VMM VM. VM VM communication between the secure channel and direct access to the firewall user access (ACL) it. ACL provides work for the medical profession as a communication VM VM service agreements. SLA and ACL VMM two different databases (see Figure 2).

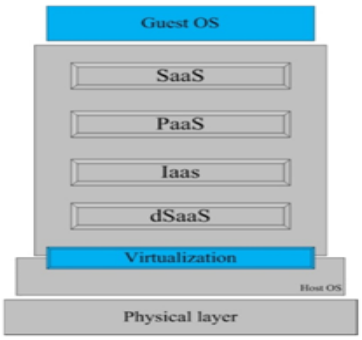

Figure 1. Blue Print of Proposed Idea

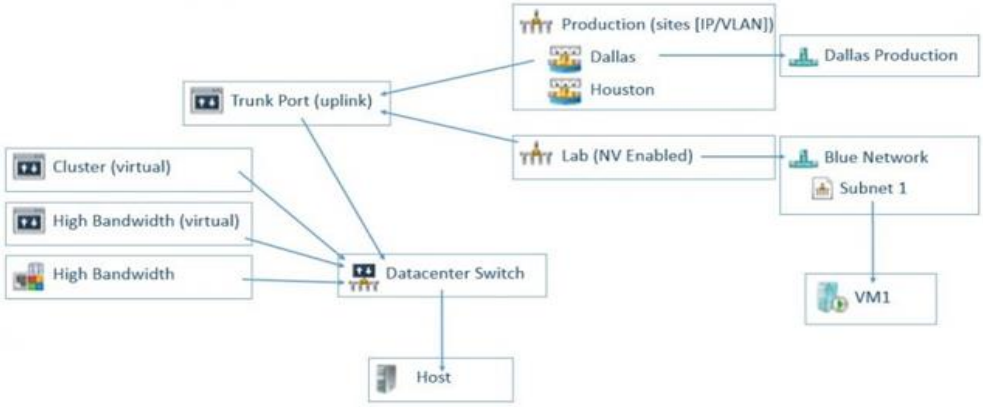

Figure 2. VMM Components

VMM tax system to increase cloud providers to fill responsible planning. Even the use of data from the operating system. The data should have a code of conduct. For maximum safety in the VMM library drive, record VMM. The directory signature of all people. Through this sign all normal process is not difficult to understand quickly. Administration is concerned manner in terms of what is needed by the sandbox and working memory (see Figure 3) to isolate a zone.

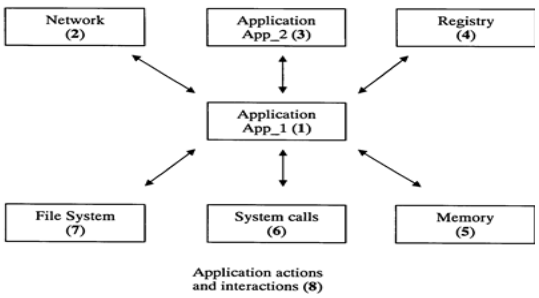

Figure 3. Sand-box Set of Physical Reality

4.1 Information

The model is based on choosing the best IDS system. IDS the proposal does not discuss the only example of IDS, depending on the program and has different IDS can be used. Another hypothesis is based on the cloud backup flyer using this model. All banks usually do not want a fight. It is important that the solutions that meet the general requirements of

information security such as confidentiality, integrity [18]. Encryption is one of the main requirements of confidentiality and authentication. The problem is that the virtualization; Share the main system or the mandatory use of unencrypted user data needed. But without introduction, such as encryption. Figure 2 shows a model consists of two parts: the professional security at module level (HSLA) monitors alarms Host Guest Level Security Analyzer (GLSA) and dust. Progress HSLA World Cup in three forms, physical violence or military targets. Moreover, the relation between the signals of the HSLA VM firewall module. GLSA better information and treatment of guests. GLSA work in normal mode. A silent mode to work as Asset Monitor Virtual Machine (VM BM) feels normal system, use of resources and do not start the process (the new system, not to mention the name of the program). VM Monitor intensity connected to the BM-GLSA. Monitoring the load of the system and compare the results Loges Cloud Manager. Spot HSLA system will be announced. HSLA To the point that the practice decided or not taken. If the choice was for the money cloud control signal. But it was not anti-system begins.

5. Conclusion and Future Work

The unit has been asked to explain the study divided the safety Cloud, which is useful for both types of work can be installed and night system to improve virtualization. You can use the means to monitor the number of types of safety at work. Well distributed and to ensure the safety of the workload guests inch contact to the minimum security. This is very important because a cloud management functions can be transferred in a VM. Insight provides a sandbox environment, together with the risk assessment or defensive attack. Thus, a system that is able to deplete the illegal process and even make it right. To evaluate a model for future work and I want a solution that will be held on Eucalyptus [23]. Eucalyptus is not the same story in terms of performance and safety. Ensuring choose the safety of food from a series of attacks against the weak eucalyptus change called signature wrapping attacks scripting attacks on sites and especially hospitals script. The goal is to be realistic and distribute development platform open to send Computing Language (OpenCL).

References

[1] L McLaughlin. Cloud Computing Survey: IT Leaders See Big Promise, Have Big Security Questions. FA Bazargan, Y Chan Yeob, J Zemerly. *Understanding the security challenges of virtualized environments*. In Internet Technology and Secured Transactions (ICITST). International Conference for. 2011: 67-72.
[2] Blate, Alex, Kevin Jeffay.Gini in a Bottle: A Case Study of Pareto's Principle in the Wild. *International Journal of Computer Networks and Communications Security*. 2013; 1(1).
[3] J Hoopes, Virtualization for security: including sandboxing, disaster recovery, high availability, forensic analysis, and honeypotting Syngress. 2008.
[4] J Sahoo, S Mohapatra, R Lath, Virtualization: A survey on concepts, taxonomy and associated security issues. Bangkok, 2010: 222-226.
[5] SJ Vaughan-Nichols, Virtualization sparks security concerns. Computer. 2008; 41: 13-15.
[6] E Ray, 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.
[7] JW Rittinghouse, JF Ransome. Cloud computing: implementation, management, and security: CRC, 2009.
[8] K Ren, C Wang, Q Wang. Security challenges for the public cloud. *IEEE Internet Computing*. 2012; 16: 69-73.
[9] L Xiangyang, Y Lin, M Linru, C Shanming, D Hao. *Virtualization Security Risks and Solutions of Cloud Computing via Divide- Conquer Strategy*. In Multimedia Information Networking and Security (MINES). Third International Conference on. 2011: 637-641.
[10] PA Karger, DR Safford. I/O for virtual machine monitors: Security and performance issues. Security & Privacy. *IEEE*. 2008; 6: 16-23.
[11] L M Kaufman. Can a Trusted Environment Provide Security. Security & Privacy. *IEEE*. 2010; 8: 50-52.
[12] K Nance, M Bishop, B Hay. Virtual Machine Introspection: Observation or Interference. Security & Privacy. *IEEE*. 2008; 6: 32-37.
[13] F Lombardi, R Di Pietro. Secure virtualization for cloud computing. *Journal of Network and Computer Applications*. 2011; 34: 1113-1122.

[14] CP Pfleeger, SL Pfleeger. Security in computing: Prentice hall, 2003.
[15] TF Lunt. A survey of intrusion detection techniques. *Computers and Security.* 1993; 12: 405-418.
[16] B Mukherjee, LT Heberlein, KN Levitt. Network intrusion detection. *IEEE Network*. 1994; 8: 26-41.
[17] SN Dhage, BB Meshram, R Rawat, S Padawe, M Paingaokar, A Misra, *Intrusion detection system in cloud computing environment*. Presented at the Proceedings of the International Conference; Workshop on Emerging Trends in Technology. India. 2011.