Inmate OS and VMM based Secured Virtualization for Cloud Computing

Parmanand Prabhat, Dept. of Computer Science & Engineering, Himalayan University, Itanagar, Arunachal Pradesh, India.
Dr. Syed Umar Professor, Dept. of Computer Science & Engineering,HMKS & MGS College of Engineering India.

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, Inmate OS, Virtualization, Sandbox

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.

2. Security Threats due to Virtualization in Cloud Computing

Security virtualization is the shift of security functions from dedicated hardware appliances to software that can be easily moved between commodity hardware or run in the cloud. The increased virtualization of the computing and network environments is putting more requirements on flexible, cloud-based security.

2.1 Access Control Vulnerability

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 DoS Weak Point Control

If the number of customers who want to work very young, and the current balance of the system is used to move another workplace. At the same time, to make the changed methods for customers with the industry and to know what measures in the market to avoid that put a lot of resources and virtual platforms. In the event of a disaster, the virtual platform and occasional data loss will come. It is important to restore the virtualization and fast platform and continue to function as a normal process. Symantec data recovery protection solution that can be used for data security and disaster recovery

2.3 Virtualization Platform Vulnerability

VMware has identified several major vulnerabilities this year that have required patches for its entire virtualization product line. In May, VMware issued a security advisory to inform customers of five related vulnerabilities in its virtualization products. The first two vulnerabilities involved a problem with RPC commands in which a guest could crash the VMX process or execute code on the host. The third vulnerability identified an issue where NFS traffic could potentially overwrite memory, allowing code execution without authentication. The fourth and fifth vulnerabilities listed in this advisory involved out-of-bounds memory writes with virtual floppy drives and virtual SCSI controllers. These issues were all addressed by installing the appropriate security patch for each VMware product. VMware's advisory included mitigation advice for customers who haven't yet installed the patch, but it may be a little difficult to implement: "Do not allow untrusted users access to your virtual machines. Root- or administrator-level permissions are not required to exploit this issue."

2.4 Virtualization Platform Vulnerability in Security Management Center

There is some security to design in a virtual environment. Sometimes, however, a security policy, this problem can not be solved. A solution to address the risks associated with part of the new security platform for virtualization. All security systems, such as firewalls, intrusion detection, logging, etc., can help secure the virtual machines. To ensure the integrity and authenticity of the log file support, digital signatures and digital watermark system can also be used with other security procedures. It is important that the virtual machines use VMM of the ed. Thus, the storage system is required to monitor the VM sign written for the device to ensure to ensure the security of traditional networks. The selection is the physical resources of each operating system of the virtual machine and the running applications on one of the VMMs. VMMS the relationship between physical and virtual OS. [4, 11]. Drawing money VMMS OS eliminates the dependency between the physical hardware resources. Therefore independent operating systems simultaneously on the same platform. All MCC has three main functions:

1. The first is insulation. VMMS is responsible for the effective physical resources allocated for each virtual machine. To give another VM, assign some VMMS to each VM. This allows the interaction with the application to VM [11, 13].

2. The second feature VMM Research. VMMS access to the site all physical host resources: CPU and smaller devices. Examine any physical host can be set when saved, copied and sent to the environment [11, 13].

3. In the third part of the VMM response. Administrative instructions to dominate the VMMS equipment. Trade the equipment of the individual virtual machine on behalf of the Inmate operating system and check the quirks of the Inmate operating system and interruptions. All entries / applications from the Inmate operating system of the MCC [11, 13].

A wide range of virtualization resources. Engineering groups with different laws of nature or host multiple virtual servers. Two advantages.

• The first is that data access should be preserved. Cluster contributes to continuous access to data provision, although most of the damage to the system or network.

• Another advantage is the significant increase in aberrations in the system as the number of workers using the [3] system.

Control of the virtual machine that determines the security of the system [14]:

• **Performance:** The system would be able to identify the different types of attacks on the integrity of the damage.

• **Accuracy:** The system will be able (if possible) to False Positives to prevent false identity cardiac infarction when the agent.

• **Elegance:** It reduces the occurrence of VM, SP on potential attackers and is unable to detect a lack of control.

• **Non Sub Vulnerability:** VMM system, cloud infrastructure, and fraternity VM Sword and cause damage to the store, the line cannot be disabled or changed.

• **Setup:** The system will be implemented in all public and private cloud services, the industry as whole cloud models.

• **Dynamic Response:** Identify the attachment system for sharing the cloud, and if you need to be careful, it is necessary to take appropriate action to try to infect the market and/or remote operation of the middleware components.

• **Service:** The system does not access the cloud and enterprise applications; However, this information should be collected in the tower fulfills the provision of billing services.

As a result of virtualization is an excellent opportunity to share with us. However, anyone with the technology can walk virtualization, risking a set of security when connected. One of the biggest problems for the security of virtualization. So

professionals familiar with the show, which has been confirmed for each series virtualized. It is important to create solutions for security problems.

2.5 Detection System

Network Intrusion Detection System: - identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.

Host-based Intrusion Detection System: - consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.

Hybrid Intrusion Detection System: - combines one or more approaches. Host agent data is combined with network information to form a comprehensive view of the network. An example of a Hybrid IDS is Prelude.

2.5.1 IDS Coverage

IDS Property Casualty Insurance Company provides property and casualty insurance brokerage services. The company offers home and auto insurance, as well as long term care insurance and disability income insurance. The company was formerly known as Wisconsin Employers Casualty Company and changed its name in 1986.

3. Inmate OS and VMM Based Secured Cloud Computing Model

In order to meet the needs of security measures, as a cloud computing solution is an effective control, while a few passive surveillance activities. The architecture provides a new dimension to the public cloud model (see Figure 1), allowing the system to detect unauthorized processing. Integrity Summary, the data systems included in almost all changes in the system. Raise the head in the clouds for VMM to avoid the default registration in the payroll function.

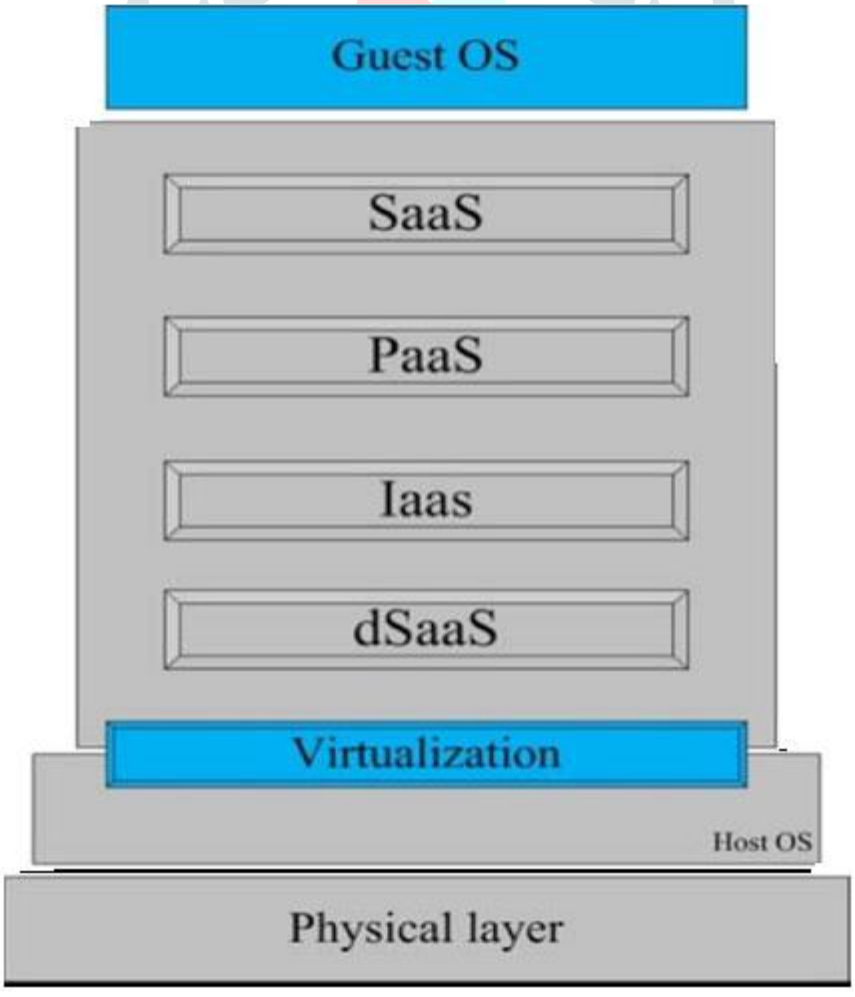

Figure 1. Secure virtualization proposed for CC

Need the complete solution for all IDS VM units, which only works in traffic, and if you find any anomalies, see to reach the firewall where the middleware devices and VMM client. VM intervention concerns is closed, and close all processes. But transparency in the sandbox will continue to respond to illegal activities. Staying active helps to make the process of false alarms, as well as the type of attack should be avoided and avoid choosing the difference. Sandbox offers direct access to the secure memory and processing power of the processing equipment layer. A host operating system that will be the sandbox, to start the process. The following mean VM VMM units. VM-VM communication between the secure channel and direct access to the firewall service access control list (ACL). ACL with the possibility that VM communications operators VM work arrangements.SLA and ACL VMM Two separate databases.

3.1 Analysis of Sandbox

The model is based on the best IDS Select system. IDS not discussed the proposed solution, the only example of the IDS,

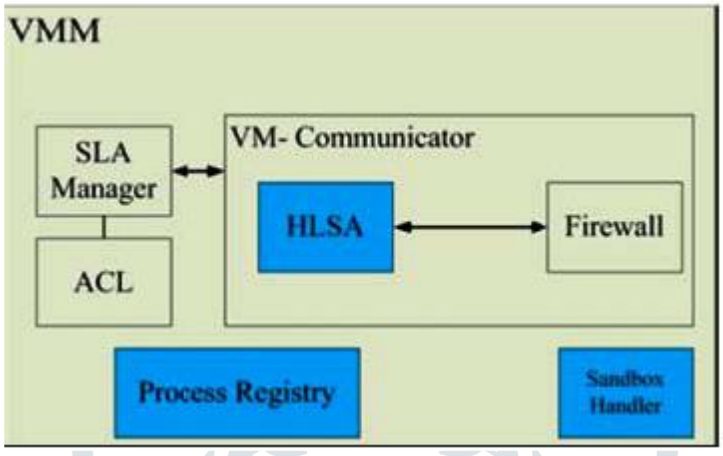

Figure 2. VMM Internal Architecture

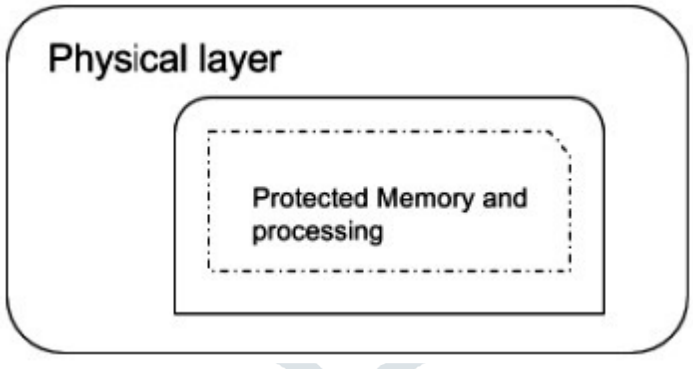

Figure 3. The physical reality series Sandbox

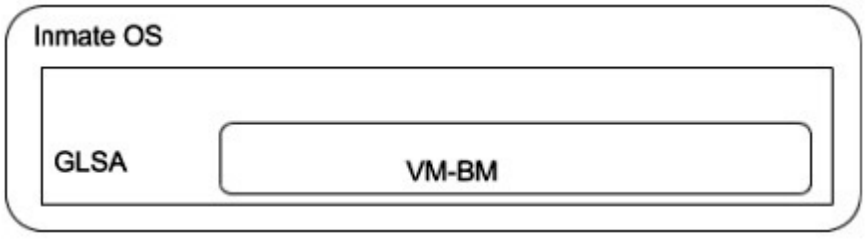

Figure 4. Modules levels of Inmate OS

depending on the application and provide the use of different IDS. Another hypothesis is based on the design of the cloud backup directory using this model. Not all banks generally want a fight. It is important that solutions to general information security requirements such as privacy, integrity [18] are met. Encryption is one of the key requirements for privacy and authentication. The problem is that virtualization; Sharing requires the host system or the mandatory use of unencrypted useful
data. Without introduction, such as encryption. Figure 2 shows a model system consists essentially of two parts: monitoring at

the level of the Business Security Alarm Inmate Security Analyzer Level (GLSA) and Dust for Host (HSLA) alarms. HSLA VM situation report in three forms, physical violence or military targets. In addition, communication between signals from the HSLA

VM firewall module. Glsa information on the best treatment and Inmates. Working glsa in normal operation. A silent operating mode, Virtual Machine Asset Monitor (VM BM) believe that the normal system, the use of resources and do not know the process (not mentioned the new system, the name of the program) to begin with. VM-intensity monitor connected to the BMglsa (see Figure 4). Keeps using the system and the results compare to each other. HSLA spot system will be announced. HSLA To the point that the practice has decided or not taken. If the choice was cloud control signal for money. But it was not to initiate anti-system.

4. Conclusions

The unit has been requested to study to improve the cloud security is distributed, which is useful for both types of work to define, installation and virtualization of the operating system can night. You can use resources to monitor the number of security types at work. Some security and security modules, the relationship between the Inmate operating system is limited to a minimum. This is very important because one of the cloud management functions can be transferred to a virtual machine. Insight provides a sandbox environment, as well as risk assessment or a defensive attack. This allows a system created to kill the illegal process, the law can. To evaluate a model for future work, and I want a solution that will take place Eucalyptus. Eucalyptus is not the same story in terms of performance and safety. Ensure food safety, change in packaging called attacks, cross-site
scripting attacks and in particular script hospitals choose from a series of attacks on the weakness of eucalyptus signature. The goal is to be realistic and to distribute to guide the development platform Open Computing Language (OpenCL).

References

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

[20] Vieira, K., Schulter, A., West hall, C., Westp hall, C. M. (2010). Intrusion detection for grid and cloud computing, IT Professional, 12, p. 38-43.