International Journal of Computer Applications Technology and Research
Volume 5– Issue 2, 56 - 60, 2016, ISSN:- 2319–8656

A Security Model for Virtual Infrastructure in the Cloud

Roya Morshedi
Department of security
Information Engineering,
Central branch, University of
Malek ashtar
Tehran, Iran

Abstract: Accordin to easily manage cloud computing, flexibility and powerful resources on space, provide great potential for improving cost efficiency. Cloud computin capabilities through the efficient use of shared hardware resources increases. Properties mentioned above, incentive agencies and other users of their programs and sevices in this space with a series with a series of threats and risks are also met.
This ensures higher accuracy virtualization and cloud infrastrure components of the virtual machines is. In this regard, particularly for initial design thesis developed a new model called cloud protectionsystem, it is suggested and shown that the proposed model, can increase supply security in the cloud. And packets received by sources and do not be discarded. How to test this architecture, in terms of effectiveness and efficiency in the fight against offensive attacks mentioned above, partly expressed and tools for simulating and measuring the efficiency of the system may be useful, recommended.
Keywords: cloud computing, service levels, virtiuation, model

1. INTRODUCTION

Today, cloud computing is widely used in industry and education. Part of the benefits of a cloud environment, including economic and cost, large capacity, the availability of all places, convenience and access to resources is based on demand, has caused business owners to do their work in this environment instead. References in this environment, on-demand and user requests from multiple sets of resources provided or is released. Preparation of allocation based on demand and are affordable. Consumers, whether ordinary people or organizations no longer need to invest heavily in technology to build their information technology and in this case, users of the resources in the cloud environment and the use to which they pay respectively. On the other hand the cloud could be released as soon as a source by a particular user, use the (reusable resources), resulting in greatly improved utilization of resources. Ease of use is a clear advantage Dygrfzay and other customers to use this space requires special expertise in particular technologies are not cloudy.we can service and Web services, virtualization and multi-tenancy refers reqest via the Internet to customers are clear.the use of physical resources. Virtual multi-processing and process separately from different users on the same physical machines are allocated. However, these resources are logically separate and cause the cloud to be multi-tenant. Despite the benefits that provides a cloud environment, this environment is not free from risk and security risk.[5] Security is one of the biggest barriers that slow the spread of the use of cloud computing.the hold. All processing and data management processes and applications within the field of administrative organization is done. On the other hand the organization of the executive management and infrastructure services and cloud services do not have. security measures cloud service providers, in general, the organizations are transparent and not visible. The presence of a large number of users who do not belong to the organization, increased concerns in the organization. Cloud service providers should rely on users but it may not be mutual trust. The reasons mentioned above, causes the customer to insert their digital assets in the cloud and therefore are doubts about the choice of this medium without relish Grdnd.dr fact, honesty, integrity, confidentiality andIt is clear that despite all the positive and negative aspects, is a comprehensive system and thus increase the protection of nodes in the cloud Karchalsh is controversial.[5] The identification of possible threats and to establish security procedures and services to protect against attacks on the operating system, is very important. Current cloud computing virtualization to provide load balancing between the nodes and physical nodes. That is, if you need to create a new virtual machine or dynamic migrations of virtual machines, load on the network divided between the existing nodes. Virtual machines on the Internet, in the form of different methods can use virtualization technology to filter and separation of data and resources and at the same time, also provide a higher degree of confidence. In particular, virtualization can be used as a security component Grdd.k·h including application virtualization to provide monitoring on a virtual machine, allowing easier management of multiple security cluster and the server mentioned compound.[8] It may seem that the issue is system virtualization for the past decade, however, has a history of more than forty years, basic research has been done in this regard in the 1960s. But in the last decade, significant progress has been made in the virtualization In principle virtualization system using a software layer that surrounds the operating system or its surroundings and the behavior of the input and output The hardware system is expected to provide a Sazd.nrm software to do this is called the hypervisor or virtual machine monitor. It seems that virtual machine monitors are equivalent to the host operating system, but not so in terms of hardware are separated. For virtual systems, virtual environments called virtual machines that may be installed inside or on platforms. Since a virtual machine hardware is not affiliated, may be more virtual machines on the same hardware and the same unit to be installed. A virtual machine is the logical equivalent of a physical hardware and more virtual machines on a single hardware logically separate spaces and can be used in a network as separate systems. The isolated virtual machines mentioned the concept of security is very important. A system-dependent security concepts in the real world is not just a theoretical concept based on factors such as factors and assumptions, implementation details and user preferences can be changed. System virtualization is also not an exception.[6]

2. RELATED WORKS

Issues related to information security and cloud computing in 2011 by "David Frisbee and Vyramvlyab and their colleagues" of engineers, computer engineers and electronics departments Intel was introduced and after the public cloud concepts and challenges in this environment to store storage, transfer and secure computing, a scenario to perform calculations provide securely. Then in 2012, "Shankar Syram and Yvgamankalam" from the University of Tamil Nadu in India that the security problems in the storage and use of open source tools and their resource requests and caching as a solution to the problems mentioned proposed and The use of monitoring tools and virtualization is also useful to know. 2013 can be a turning point in examining issues related to the subject of this paper is that this year at least articles published in journals that went perfectly valid to mention them. In this year, "Gabor pack and Lvnth Attaché and Bnkasa" from the University of Budapest will focus on security issues with hardware virtualization and the concepts relating to the different types of network virtualization and storage services, to expression threats associated with virtualization and Countermeasures notes.explains. Most research in this area in 2015 by "Vasylakv- Ali manifestations and Athanasius" was performed at the University of North Dakota to legal challenges, communication and architecture as well as virtualization refers issues and ultimately "Flavio Lombardi and Roberto Di Pyytrv and colleagues "in 2010, an advanced protection system to maintain the accuracy of the information presented in virtualization.

3.CLOUD COMPUTING

The first question that arises, in relation to the concept of cloud computing and forming part of this environment. In response to this question, the definition provided by the National Institute of Standards and Technology as an academic institution in America, visit We (1 and 5). This definition is widely accepted. It defines cloud computing as follows:

Cloud computing model to provide easy access based on user demand through the network change and configuration set of computing resources (eg, networks, servers, storage, applications and services) that can be accessed with minimal need resource management or the service provider to directly intervene, quickly provided or released (left) is. Essential features are divided into 6 categories that include:

Row property	Row
On-demand access	4.1.1
widespread access network	4.1.2
Resource	4.1.3
The rapid expansion	4.1.4
measured service	4.1.5
Several rental	24.1.6

Table1. The essential characteristics of cloud computing

4. LAYERS AND SERVICES IN CLOUD COMPUTING SERVICE

National Institute of Standards and Technology services provided by cloud services is divided into three categories, namely: 1. software as a service,2. platform as a service 3. Infrastructure as a Service.

4.1 software as a service

This service enables users to use the cloud service provider and run applications on the cloud, it is. Tvanndbh Users access these applications through Web browsers Nmaynd.ayn the possibility of an application does not provide service and only software distribution model to be put on the Internet and users can use the software that do not have ownership of it, according to usage, to pay the costs.

4.2 platform as a service

Applications that is owned by a user, the need for a framework for the implementation and management. This framework includes integrated development environment, the operating system layer resources (time execution engine that will run the software), and is. As the above services by the service provider. This service, control over the user's operating system and applications to the cloud does not pass.

4.3 Infrastructure as a Service

The service provided by the service provider cloud hardware structure implies that includes network, storage space, memory, processors and other computing resources. These resources are available online and via the Internet Bashnd.frahm the cloud service to all service control layer.

5. VIRTUALIZATION

Virtual systems are widely used for a variety of applications to protect physical servers, separate from guest operating systems and debugging software is used. There are many other applications for virtualization and virtualization motives and causes many to choose from there. [6]

An advanced operating system like Windows or Linux is very complex suitable tens of millions of lines of code with the desktop version, and thus a greater level of vulnerability and simply is not possible to prove that they are safe. In addition, the operating system a break point to anything in the system (process and data) to turn and attack the operating system, the entire system was destroyed. It is difficult to secure a spot in the complex point of failure, represent a security risk for data processing in the system. In the result of the permanent reduction of hardware costs, most organizations to achieve different operating conditions based on safety , use of multiple physical systems. [8]

The establishment of a physical system to reduce potential security risks due to a failure point is used, increasing efficiency and flexibility. Each physical device need physical space, cabling, power, cooling and management software is. In addition to the above, due to the physical separation, communication costs such as delays of data transmission and storage should also be added. For some problems, solutions

optimization (such as the storage consecutive to improve access to data and energy management to reduce energy costs), but for some of these problems, the cost is so high that it are not justified. Because of the expenses that each physical systems, one of the most important issues that arise, avoiding systems that are used less. Small system applications within the organization can be seen in two ways: [1] desktop machines that rarely use their full potential (ie, systems that operate at night preservation and maintenance purposes, do not do) 2 - or systems and servers that are not currently active. Many organizations are interested in the efficient use of these systems, and in addition to overhead and low cost, highest efficiency in using them. Virtualization is a method in a hardware system allows multitasking operating system and it is possible to perform multiple operations simultaneously provide and increase the efficiency and reduce the cost.
The benefits of virtualization are:
1.srfh direct and indirect cost savings.
2. Use the optimization of hardware resources and improve efficiency.
3. integration of services in one or more servers, which create a centralized management and high security.
4. accelerate the implementation of the various components and rapid creation of new services in order to increase the organization's business.
5. Support of existing systems and services in the organization.
6. integration of hardware resources.
7. creation and deployment of test environments without disruption and without risk.
8. lower maintenance costs and manpower
9.arayh virtual machines instead of physical machines and run different operating systems on a single physical host.

6.MODEL CLOUD COMPUTING SECURITY

A service provider one or more sample runs in the cloud service that this service can be accessed by a group of final service. For this purpose, providing resources from the cloud service provider's rent. Service users and cloud service provider space are not any physical control over the service level agreements signed with other that specifies how to implement cloud services.
Attacks on cloud systems in the scenario may be divided into two parts:
1. Attacks resources
2. Attacks data
These attacks may include the following:
• Prevent access to resources (denial of service attacks)
• misuse of resources to attack
• steal data or change configuration nodes
• leakage of sensitive information
• attacking the components associated with the structure

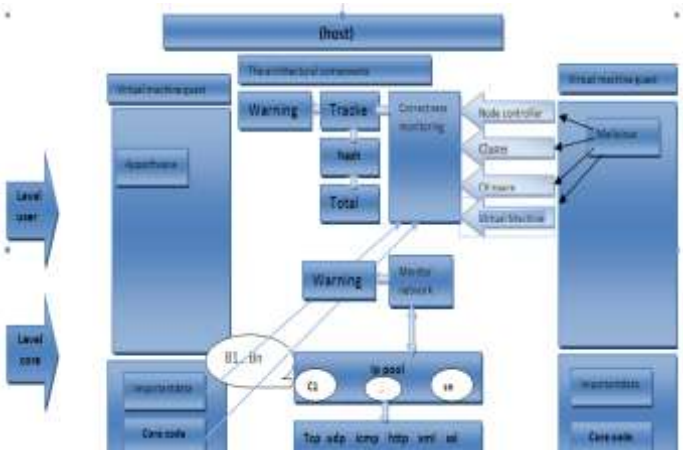
7. Requirements
The main requirements of a system to monitor cloud security we can mention:
Yield property
Efficiency and effectiveness of the system must be able to detect the most common types of attacks and violations of integrity.
System accuracy is better able to avoid negative and positive situations (in this case the attack mistakenly considered to be licensed activities).
Transparency of the system should have minimal visibility into the virtual machine and users are able to detect the presence of possible regulatory system are not
attacker host system, the cloud and other virtual machines should be attempted attack from a guest, be protected and should not be able to change or disable its monitoring system
The ability to expand the system should be expanded on most configuration

Accountability systems should intervene in the cloud and cloud applications, but with data collection and capture must be able to implement policies in response.

8. THE PROPOSED MODEL

The proposed system, to protect the integrity virtual machine guest and distributed computing, as well as to detect and prevent denial of service attacks that use this virtual machine guest using supervision and monitoring infrastructure components and activities in the network. The proposal, developed and protective methods "When I wear him" to protect against intruders and attacks monitored components such as worms and viruses.we will consider.Takes. In fact, guests can target any type of cyber attack and manipulation such as viruses, scripting, and buffer overflows as well. When the image supplied by the user is visiting, security virtual machine is not fully guaranteed and the guest must be possible to track malicious activity, be monitored. In this model, attackers can cloud users or users of their cloud applications. While victims can service providers running in the cloud or cloud infrastructure or other users. One of the common threats and dangers, it is for an attacker to remotely exploit a weakness in a guest system's software. Some attacks exploit cloud services possible. When a malicious person, the legal action of the other cases within the cloud, as mentioned earlier, can be programmed to learn malicious information . Among other possible attacks in the cloud, denial of service attacks, traffic rate is an estimate and should always be monitored traffic on the network.
In order to protect virtual machines and cloud structure of strikes, the key components that can be targeted or they are affected by the monitor (Monitor), we. To enable or disable monitoring on key core or key components and middleware components, capable of detecting any changes might be in the data or the core code. As a result, we can be sure that the integrity of the core and central component of the risk taken place. In addition, in order to monitor entry points to cloud, cloud to the behavior and health components through logging and periodic review of the countervailing executable files and libraries pay. In order to protect from Denial of service attacks, to monitor sent packets on the network and if it was a certain amount of network traffic to prevent service failures due to denial of service attack, to prioritize packets received the query. If the received packet is less important, and the value stored in the buffer delay in executing or discarding it is presented. The next goal, especially when the image cloud provider offers is unreliable, ensure that the program is running forward, is not able to detect external intrusion detection system. However, due to unknown codes in the intrusion detection systems, determine what extent are detected by using a target virtual machine, simply do not accept. In fact, the presence of a monitoring system can be

measured by the performance of certain functions, be detected. The proposed protection system can do the following protection:
1. protected from attacks from outer space is clear.
2. Protect VMs from attacks that it is aligned.
3. protected from attacks that come from the virtual machines.
4. protected from attacks that enter through the network
The proposed system architecture In addition, the architecture "IC Open the" combined. stored. The proposed system has two monitoring systems is at the same time: [1] authenticity observer on key components and data on the network 2. supervisor And can work in two modes: 1. simultaneously V2- for asynchronous notification. honey reqest 2. In the event of an attack when the moment will be warned and prevented from continuing activities. In this system, the coping storage database stored on the host side, which includes the following components: Total coping vital for the components of the architecture of the home and host kernel code and other necessary data and files are used.low priority act. . It all requirements listed in Section 7 meet.



9. PERFORMANCE

As fitness
Hardware and software required
Minimum hardware and software requirements is included in the table shown below:
Details of host 1 host 2
Athlon 64 4400+ Athlon 64 4400+ processor model
Multi 2 2
Memory 4096 4096
Operating system Ubuntu 8.10 (oecp)
Ubuntu 9.10 (eaucal) Ubuntu 8.10 (oecp)
Ubuntu 9.10 (eaucal)
Linux 2.6.30 Linux 2.6.30 kernel
Virtual machine monitor Kvm 88 Kvm 88
Jdvl- hardware and software requirements
The implementation and evaluation of the proposed system requires the following software:
1. virtualization software like kvm or vmware
2. Network simulation software like opnet
3. The network monitoring software like wireshark
4. application traffic generation and simulation attack

10. Problems and challenges

Due to the lack of a code of attacks on the network as well as the relatively low efficiency and high cost of traffic simulators allows simulation of attacks is not complete.
In addition, to obtain the optimum point for different network traffic packets need to experience high performance and accuracy.
Test Mode, once the attack without implementing the proposed system in terms of when and how to diagnose and test again with the implementation of a monitoring system that we repeated attacks. Then there is the possibility of comparisons.

11. WRAP

Cloud computing model to provide easy access based on user demand through the network change and configuration set of computing resources (eg, networks, servers, storage, applications and services) that can be accessed with minimal need resource management or the service provider to directly intervene, quickly provided or released (left) is.Virtual discovery and identification of passive attacks and how to deal with them.

12.REFERENCES

1. Diogo A. B. Fernandes _ Liliana F. B. Soares _ Jo~ao V. Gomes _ M_ario M. Freire _ Pedro R. M. In_acio, Security Issues in Cloud Environments/A Survy, International Journal of Information Security.

2. N.M. Mosharaf Kabir Chowdhury a,1, Raouf Bouta, A survey of network virtualization , Computer Networks.

3. MICHAEL PEARCE, Virtualization: Issues, Security Threats, and Solutions, Acm Computing Surveys.

4. Perez R, van Doorn L, Sailer R. Virtualization and hardware-based security. IEEE Security and Privacy 2008;6(5):24–31.

5. Peter M, Schild H, Lackorzynski A, Warg A. Virtual machines jailed: virtualization in systems with small trusted computing bases. In VDTS ’09: Proceedings of the 1st EuroSys Workshop on virtualization technology for dependable systems, ACM, New York, NY, USA, 2009. p. 18–23.

6. Siebenlist F. Challenges and opportunities for virtualized security in the clouds. In SACMAT ’09: Proceedings of the 14th ACM symposium on access control models and technologies, ACM, New York, NY, USA, 2009. p. 1–2.

7. KELLER, E., SZEFER, J., REXFORD, J., AND LEE, R. B. 2010. Nohype: Virtualized cloud infrastructure without the virtualization. In *Proceedings of the 37th Annual International Symposium on Computer Architecture (ISCA’10)*. 350–361.

8. LI, C., RAGHUNATHAN, A., AND JHA, N. K. 2010. Secure virtual machine execution under an untrusted

management os. In *Proceedings of the IEEE 3rd International Conference on Cloud Computing (CLOUD'10)*. 172–179.

9. STEINBERG, U. AND KAUER, B. 2010. Nova: A microhypervisor-based secure virtualization architecture. In *Proceedings of the 5th European Conference on Computer Systems (EuroSys'10)*. 209–222.

10. SESHADRI, A., LUK, M., QU, N., AND PERRIG, A. 2007. SecVisor: A tiny hypervisor to provide lifetime kernel code integrity for commodity oses. In *Proceedings of the 21st ACM SIGOPS Symposium on Operating Systems Principles.* ACM, 335–350.

11. SHARIF, M. I., LEE, W., CUI, W., AND LANZI, A. 2009. Secure in-vm monitoring using hardware virtualization.In *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS'09).* ACMPress, 477.

12. SIEBENLIST, F. 2009. Challenges and opportunities for virtualized security in the clouds. In *Proceedings of the 14th ACM Symposium on Access Control Models and Technologies (SACMAT'09).* ACM Press, http://portal.acm.org/citation.cfm?doid=1542207.1542209.

13. WU, X. AND MA, W. 2010. Hypervisor based detection and prevention for packed malware. http://www.ece.tamu.edu/~tristanw/files/Wu Xiaojian Ma Weiqin Report.pdf.

14. YUNIS, M. AND HUGHES, J. 2008. Real security in virtual systems: A proposed model for a comprehensive approach to securing virtualized environments. *Issues Inf. Syst. IX*, 2, 385–395.