IJETCR Open Access

ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Volume 3; Issue 2; Page No. 176-180

Security in Cloud Using Virtualization

Mr. Anil Kumar, Mr. Pradeep M

Department of Information Science and Engineering, Channabasaveshwara Institute of Technology, Gubbi, Karnataka, India.

anil.kumar@cittumkur.org, pradeep.m@cittumkur.org

ABSTRACT

Virtualization is a foundational elements of cloud computing and helps deliver on the value of cloud computing. Cloud computing is the delivery of shared computing resources, software or data-as a service and on demand through the internet. Virtualization became important again as a way to improve system security and helps delivery on the value of cloud computing. In this paper we address the security risk induced by virtualization are analyzed and classified. Where we presented divide and conquer idea for security risk of private cloud computing virtualization can be reduced.

Index Terms: three ways integrity check algorithm, cloud service provider, Third party auditor, message digest.

INTRODUCTION

The rapid development of cloud computing has brought a series of non-traditional security threats, and put forward a new and higher demand to information security. Now it is an urgent need that increasing the security synchronization technology research efforts for the development of cloud computing technology and application, which can provide support of security technology, products and infrastructure. From the cloud computing industry and application, despite the world's IT (Information Technique) companies have launched many of its cloud-computing products, but because of security problem is not resolved, related to a spate of security incidents, combined with the popularity of the concept of cloud computing, people to deepen understanding of cloud computing, security has become the greatest concern in the use of cloud computing or migrating to cloud computing, cloud computing security. This bottleneck problem is not solved, cloud computing would be difficult for industrial upgrading and application. Therefore, cloud computing security research has important practical significance.

Generally, a cloud is discussed in terms of services. The menu of services is being enriched as SaaS (Software as a Service), PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) have been invented as part of XaaS. Cloud computing is a promising computing paradigm which recently has drawn extensive attention from both academia and industry. By combining a set of existing and emerging techniques from research areas such as Service-Oriented Architectures (SOA) and virtualization, cloud computing is regarded as such a computing paradigm in which resources in the computing infrastructure are provided as services over the Internet. As promising as it is, cloud computing is also facing many challenges that, if not well resolved, may impede its fast growth. Data security, as it exists in many other applications, is among these challenges that would raise great concerns from users when they store sensitive information on cloud servers. These concerns originate from the fact that cloud servers are usually operated by commercial providers which are very likely to be outside of the trusted domain of the users.

Virtualization became important again as a way to improve system security and helps delivery on the value of cloud computing. It enables business to reduce IT cost while increasing the efficiency, utilization and flexibility of their existing computer hardware.

Academic also focus of cloud computing security, has organized several international conferences on cloud computing, research on cloud computing technology, deployment, policy and security issues. Berkeley cloud computing white paper [5] listed 10 facing of cloud computing problems and opportunities. The article [6] discussed on the cloud storage, proposed the ideas of cloud storage system structure and involved the relevant issues, such as the storage security, but did not give the appropriate solution. The articles [7] and [8] analyzed the privacy, security and credibility issues caused by cloud computing, and discussed some possible ways to enhance confidence and security. The article [9] for the security implications of cloud and risk assessment, gave a

Corresponding author: Mr. Anil Kumar

quantitative framework.

The paper [10] presented a security system framework for the cloud, and discussed of four kinds of security stack service mode of cloud computing. The paper [11] reviewed on the security issues of cloud computing service delivery model, revealed a variety of security risks faced by the transmission cloud computing services. The paper [12] gave a model of cloud computing security based on AIS (Artificial Immune System), and claimed that based on this security model can be more effectively prevent malicious software attacks. The paper [13] in order to enhance the cloud of virtual machine (VM) security, proposed a measure framework of virtual machine operation. In this framework, there is a module in virtual machine to transmit the operation of virtual machine to a trusted virtual machine, by comparing with a good reference table prepared in advance to determine whether the virtual machine in a normal state of operation. The paper [14] by analyzing the status quo of cloud computing security, pointed out that the current cloud computing security challenges and enhance demands is an opportunity to cloud computing, and from the user and cloud computing provider point of view gave the issues in the next step should focus on cloud computing security.

Related work

At present, there still did not have the unification cloud computation definition, NIST defined the cloud computation essential characteristics, the service models and the deployment models, has certain representation, specific as shown in Figure 1[15].

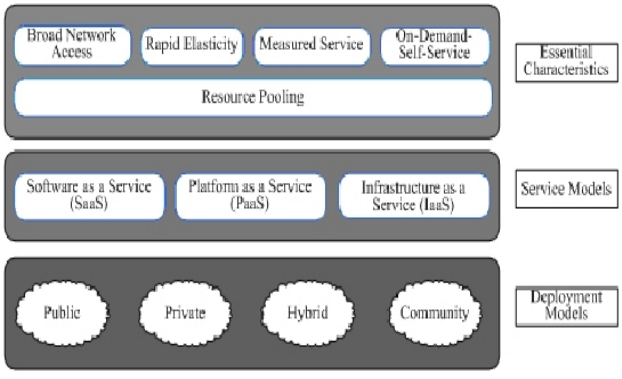
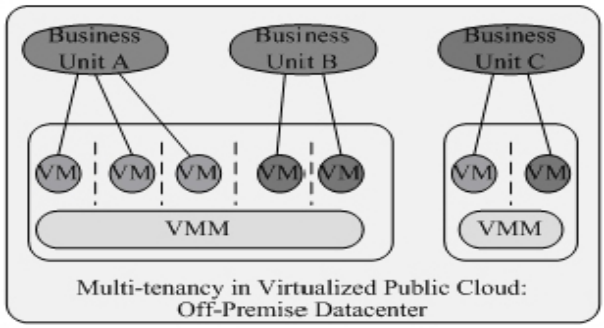
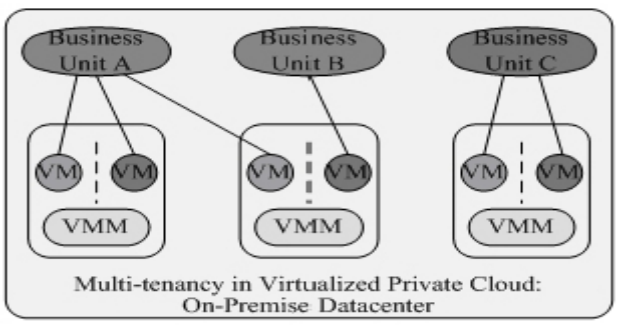


Figure 1:. Cloud computation essential characteristics, the service models and the deployment models defined by NIST

The position independency in a certain extent, namely the user beyond control or is unable to know that uses the resources' accurate physical location, but virtualization may assign the position in the high abstract stratification plane (e.g. country, state, province, or data central). Refers to the different existing literatures, there are large differences about the virtualization definition. In the virtualization vigorous development's stage, there did not have the strict standard and the definition defines the virtualization. It is usually thought that the virtualization isrefers to the computer parts operate in the hypothesized foundation, but not in the real foundation, and the virtualization is one solution to simplify the management and optimized resources. Virtualization technology assigns flexibly workload different physical machines to achieve resource sharing, is a method that running multiple virtual machine operating systems independent in a physical machine [16], shown in Figure 2, where VM is the virtual machine, and VMM means the virtual machine monitor. The main purpose of virtualization is to simplify the IT infrastructure, and it can simplify access to resources and resource management. Users access the resource through the standard interfaces supported by the virtual resources. By using the standard interfaces, when the changes happen on the underlying physical resources, the case does not affect the user's use. At the same time the overall management of IT infrastructure can be simplified, virtualization reduces the coupling between the user and resource, so the user does not depend on specific physical resources. By using this loose coupled relationship, managers can make the management on IT infrastructure in the base of influence the user minimum. Today's virtualization technology includes microprocessor virtualization, file virtualization and storage virtualization.



(a) Virtualization model in the public cloud



(b) Virtualization model in the private cloud

Figure 2: Virtualization models in cloud computing

Virtualization security framework and access control

Virtualization security could be investigated from 2 aspects: virtual system security and virtualization security management. A virtualization security framework was given as fig 3.

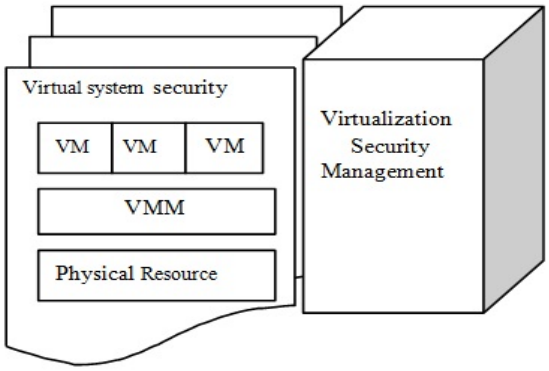


Figure 3: A Virtualization Security framework

Virtualization security framework is organized effectively in two modules which are virtual system security and virtualization security management. Two modules perform their duties without disturbing each other, so that the entire framework can be more efficient.

The virtual system security consists of three layers: The first layer is Physical Resource layer. The second layer is VMM which is the most important layer that should be heavily facilitate with security mechanisms to protect VMs up running. The top layer is VMs that provide virtualization services to consumers.

Access control in virtual environment refers to the practice of restricting entrance to a resource to authorized VM. A well-designed access control policy will make the physical resources being used appropriately and communication between VMs and between VM and VMM more trustworthy. An access control framework for virtual system is shown as fig 4.

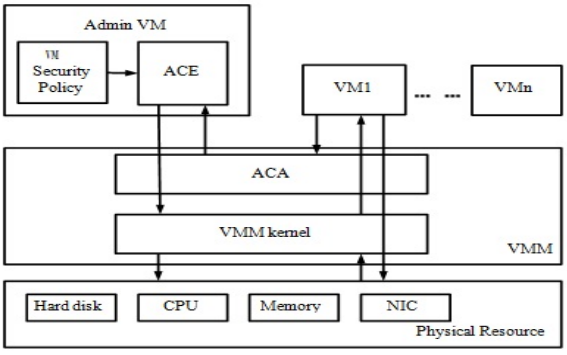


Figure 4: An access control framework.

An access control framework is divided into three layers, namely physical resources layer, virtual machine monitor system layer and virtual machine system layer.

We can see from figure 5, the physical resource layer contains the required hardware resources of the entire structure: hard disk, CPU, Memory, NIC. Physical resource layer can be said that it is the cornerstone of this framework. The above two layers call the hardware resources through the physical resource layer, so that the whole framework run well. This access control framework mainly consists of Access Control Agent (ACA) resided in VMM and Access Control Enforcer (ACE) resided in Admin VM which is in charge of managing the whole virtual system cooperating with VMM. ACE is used to control Guest-VM access behaviors as per its security policy profile. ACA is used to receive or the requests from Guest-VM and then transfer them to ACE. In the access control structure, Admin VM plays an important role as an agent. By Admin VM controlling other guest virtual machines, the security management of the Guest- VM becomes easier in the VMM system. VMM system delivery the work of security policy profile to the Admin VM, and then VMM system controls the Guest-VM according to the requires of the Admin VM. Adding an Admin VM in the access control framework not only help the structure to be built much simpler, but also increase more flexibility of the whole structure.

Risk analysis of virtualization security

Virtualization technology itself is not new, but after being applied to cloud computing, it brings some new security risks and vulnerabilities may be exploited maliciously and may cause major security incidents. Virtualization security has two aspects, one is own safety of virtual technology, another is the introduction of new virtualization security issues. Specifically, we think the following risks of the private cloud virtualization security are worth concerned especially.

Risks of Resource Access Control

First, when resources are unified into the same logical platform to storage and use, there is no fixed security border and isolation, the user can only see the logical storage location, do not know the specific storage location of information, this information may be in the off-premise storage infrastructure, which there is the possibility of leakage of secret information, including the infrastructure manager and control the infrastructure by using the vulnerability of virtualization platform might extract the secret information. Second, when the virtualization platform is attacked, the administrator's privileges may be stolen and used maliciously, for example for some users to upgrade or delegated authority, these rights run away will lead to secret information loosing the control.

Risks of DOS Attack

Virtualization services have a risk to slow or even stop when a large number of applications and even unlimited use virtualization platform for processing. This is similar to a traditional network, when a server or a group of emergency visits, the server will reduce the speed of response, processing business is slow, in particular, a large flow of cases and the application layer DDoS (Distributed Denial of Service) attacks, cause server downtime and service is stopped. DDoS has a greater risk and use potential at virtualization platform. Due to the virtual platform is designed to provide each user with the necessary service, when an excessive number of users or malicious applications were a lot of services, it will take up too many resources and make the virtualization platform cannot run effectively, thus all users will be affected. For the former, that the excessive numbers of users are normal using virtualization platform, you can expand the virtualization platform and increasing the resources to resolve. But for the latter, i.e. a malicious application that was a lot of services to take up a lot of damage for the purpose of unlimited resources, which for any kind of high-performance virtualization platform is not affordable, can be very destructive. In addition, this behavior is similar as Botnet in Internet, the malicious users apply a large number of services to attack other virtualization platform and as a result all virtualization platforms will denial of service.

Risks of Virtualization Platform in Building Network

The network connect client with sever is based on the software hubs usually. If two clients are the members of same network, which share the same virtual interface, then the two clients can see the server and all traffic of the client end because the traffic of two networks connected by a virtual switch machine is through the same physical network card. For all client ends of a server, all other client ends and servers share the same software stack. Network stack sharing is a major problem of virtualization security, if all the client ends and the server share the same network software stack, the attacker can access to the entire stack by only attack a computer of clients.

Risk of Virtualization Platform's Security Management

The virtualization platform built in private cloud is physical isolation with Internet, thus the library of viruses and Trojans for the virtualization platform cannot update rapidly, and the vulnerabilities of virtualization platform cannot be repaired in time. Internet environment will always produce new viruses and Trojans, Internet-based business can update security software through accessing Internet servers in real time and ensure obtaining the latest security services. For the private cloud, in the LAN (Local Area Network) environment, there is a "time poor" in updating virtualization platforms virus and Trojans library and fixing the vulnerabilities, this bring a risk for the security of the virtualization platform. There is a qualitative change between the management of virtualization platform and that of traditional network, this bring a new kind of risk for virtualization platform, namely the management risk. In the virtual world, all the concepts is change from hardware to software, the system administrator of managing the virtual switching network cannot any longer use the simple tools for monitoring and troubleshooting. The administrators cannot approach the virtual machines, plug into a laptop computer, add a network splitter, make a port mapping, or view the statistics of a virtual device. All of these skills and knowledge about virtualization beyond the capabilities of the general network administrator, and the virtualization technique conceal the software controller, GUI (Graphical User Interfaces) of management, dedicated kernel module and the binary systems, so the general network administrator cannot see them. Only the designers, developers and senior administrator of virtualization system know how to implement effective manage, thus increasing the cost and difficulty of management.

SOLUTIONS OF VIRTUALIZATION SECURITY RISKS

For virtualization security, the appropriate technical measures can be used include: encryption and integrity checking of virtual memory image files, isolation and reinforcement of virtual machines, access control of virtual machines, vulnerability checking of virtualization, monitoring of virtual machine, security migration of virtual machine, and so on. In the face of a wide range of infrastructure, a wide range of services, and large user groups in virtualization environment, the overall strategy of virtualization security solution is to divide and conquer in this paper, namely, according to the user and manipulate objects of different categories take appropriate safety measures.

(*A*) For the risk 1, for from the LAN, WAN (Wide Area Network) and Internet, different users, its access to different positions and different content, we need to use different security policies. This paper considers that control the number of users is not conducive to the maintenance, since the virtualization platform has all the data and applications under the same standard, it will have different access to the unified management of data and applications are classified under the same security zone, and then take security measures to the security

zone which can avoid the object is encryption protection for each objection. Directory services can be used to manage identities and provide the capability of access control. When the user needs to access the resource of cloud, one-time grant permission for the client, specify the scope of access, and it can only be displayed to access the secure area, other areas is hidden to prevent the user to access, thus can avoid the user which lack of rights to know the path of secret information.

(*B*) For the risk 2, in the special case when the number of users and applications services requests increased dramatically, we need to adopt the workload equilibrium and migration strategy to move to another work area. At the same time, take audit mechanism for users apply services, review each application to prevent a malicious user to apply a lot of resources on the virtual platform. Taking in emergency situations, the virtual platform is outage and loose data by attack, virtualization platform requires a rapid recovery and return to normal working mechanism, where the strategy is to establish the backup of their own and restore mechanism for each security zone, parallel reconstruct without disturbing each other, to restore service. For the data protection and disaster recovery, we can refer to Symantec's data protection and disaster recovery solutions [17].

(*C*) For the risk 3, in each virtualization area we can setup a separate administrator (can be two processes), a process running in a secure area within the real-time, involved in virus and Trojan killing, as well as bug fixes, etc., while another process in an isolated area, communicate with the outside world, updating the virus and Trojan library and obtain the latest vulnerability information, and download those patches stored in a separate isolated "box", the first process to obtain the information of the "box", and the security is maintained throughout the area.

(*D*) For the risks 4, they belong in the virtual platform design problems, added to the virtualization platform security solution does not solve these two problems sometimes. To solve these two problems fundamentally, we need to add some new mechanisms into the virtualization platform design process. Current security policy is mainly audit. In a cloud environment, the physical server is integrated into multiple virtual machines instances on the virtual server. The firewalls, intrusion detection and prevention, integrity monitoring and log checking all can be deployed as a virtual machine as software to increase the protection of virtual machines. Among them, it needs to stress that the log file must be tamper-proof to ensure its integrity and authenticity. We can adopt the digital signature technique the digital watermarking and other techniques to ensure the integrity and authenticity of the log file. For the virtual machine which must use an embedded hypervisor API, we should customize a security mechanism to monitor the flow of VM backboard, where the flow is not visible for the traditional network security monitor equipment.

Conclusion

In this paper, we first we pointed out different of legacy service environment security and CTSE security. Then we propose a virtualization security framework and access control. For the virtualization security problem of private cloud computing, the security risks induced by virtualization are analyzed and classified and then based on the result of risk analysis, for each kind of security risk, some corresponding solutions are presented. Based on the proposed solution, we can effectively solve the risk caused by the current virtualization security and management.

References

1. Cong Wang, Qian Wang, Kui Ren, "Ensuring data storage security in cloud computing", IEEE 2010
2. O Rajitha, Murali Krishna, "Secure dynamic data support and trusted third party auditor in cloud computing" ,International Journal of science & Engineering Rearch, Volume 4, Issue 10, October-2013.
3. Garima, "Ensuring data storage security in cloud using two way integrity check algorithm" ,International Journal of Advanced Research in Computer Science and Software Engineering , Volume 3, Issue 11, November-2013.
4. Xuefeng Liu, Yuqing Zhang, Boyang Wang and Jingbo Yan, "Mona: secure multi-owner data sharing for dynamic groups in the cloud" , IEEE transactions on parallel and distributed system, Volume 24, NO. 6, June- 2013.
5. Kapila Sharma, Kavita Kanwar, Chanderjeet Yadav, "Data Storage Security in Cloud Computing", International Journal of Computer Science and Management Research, Volume 2 Issue 1 January 2013