Research on Virtualization Security Service Technology of Cloud Platform

Gao Ruohan, Liu Hui, Qian Hengshun, Li Yan

Nari Group co., LTD. Nanjing, Jiangsu 211100, China

Keywords: security risks, cloud computing platform, IaaS, three-level protection security indicators.

Abstract: When face with the security risks brought by virtualization and other technologies of cloud computing platform, the existing information system security level protection index system in China has obvious deficiencies in both feasibility and effectiveness. By analyzing the security threats of IaaS cloud computing, this paper proposes the corresponding security protection requirements of IaaS cloud computing for IaaS security threats, and designs the IaaS cloud computing security evaluation index model based on the three-level protection security indicators. The analytic hierarchy process (ahp) and fuzzy comprehensive evaluation method are emphasized as the evaluation methods of this index model.

1. Introduction

According to the research of Gartner, the fastest growing scale of global public cloud market is cloud service under IaaS mode, and the expected growth value of its cloud computing service scale will reach 43% in 2016 [1]. In the white paper on cloud computing (2016), China academy points out that the infrastructure as a service model (IaaS) is the main investment project for the information technology construction of China's Internet enterprises in 2015, and will also be the main growth point of the cloud computing market in the next year [2]. Thus, IaaS model is the most widely used service model in the cloud computing market. At the same time, although China's hierarchical protection system divides the security level of information system into five levels from low to high, it can be concluded from the actual protection experience of information system in the market that the protection level of most Internet enterprise information system is usually classified as three levels. Therefore, based on the three-level protection index, this paper studies the cloud computing security evaluation index model under IaaS service mode, which is in line with China's current cloud computing development trend and security needs, and can also provide reference for the formation of cloud computing market access standards.

2. IaaS Security Risks in Cloud Computing

Cloud computing in IaaS mode mainly relies on a virtualization technology that Abstracts the underlying hardware. Hardware virtualization is divided into full virtualization and paravirtualization, the full virtualization is divided into bare-metal virtualization and host virtualization. The difference between bare-metal and host virtualization is whether the Hypervisor is installed directly on the hardware resources or on the standard host operating system. The most common server virtualization technology in a cloud computing environment is bare-metal virtualization, which is as shown in figure 1. The Hypervisor layer consists of the virtual machine monitor (VMM) layer, the kernel layer and the driver layer. For the operating system of the virtual machine running above the Hypervisor layer, the underlying hardware resources are invisible black boxes.

  DOI: 10.25236/mmmce.2019.058

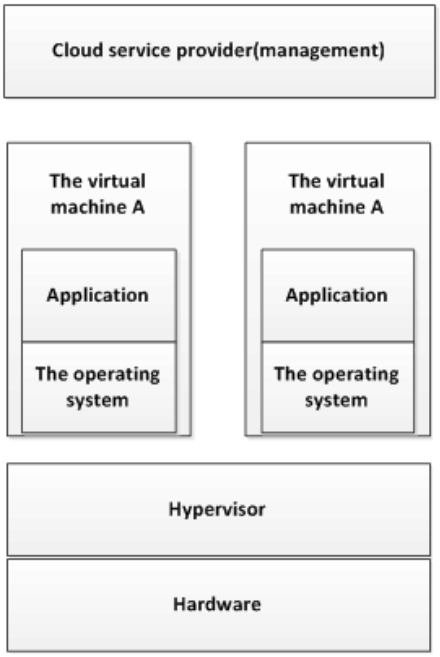

Fig. 1 The bare-metal virtualization

2.1 The Security Risks of Virtualization Technology.

IaaS cloud computing has certain security requirements for Hypervisor, virtual machine VMs and tenant operating system image protection, which are the key components involved in virtualization technology. Muhammad Kazim et al. summarized the security risks and solutions of these three key components [3], as shown in Table 1.

Table 1 The security risks and solutions of these three key components

element	risk	The solution
Hypervisor	Virtual machine escape attack	Properly configure the tenant virtual machine and its interactions with the host virtual machine
	Consumers rent virtual machines to install malicious user operating systems	Virtual machine file encryption.
	BluePill, Vitriol, Sub Vir and other malicious Hypervisor program attacks	
	vulnerability due to the increased Hypervisor source size	Use systems that guarantee Hypervisor integrity
VMs	The worm attack	User operating system installed anti-virus, anti-spyware programs and other software monitoring can be operated.
	Attacks virtual machine status files	Encrypt the virtual machine state before saving it to a plain text file.
	Denial of service attack	Install fire protection wall agent; Use the VortIO driver of KVM to provide mechanisms such as interrupts and timers.
Virtual machine image	Virtual machine image creep	Use a mirror management system to set up management policies for unnecessary mirrors.
	Virtual machine image patch update	Use the offline virtual machine image patch tool.
	Virtual machine checkpoint attack	Check the document and add the sealing; Enable SPARC mechanism.

2.2 The Virtualization Characteristics and Risks of IaaS Cloud Computing.

In the IaaS model, the resources and applications used belong to the same organization or different organizations by multiple cloud service consumers is called multi-tenancy. It is a significant feature

of virtualization technology. Cloud services under multi-tenant conditions have risks such as visible residual data, operation of malicious tenants on other tenants and so on. Therefore, IaaS cloud computing also has certain security requirements for resource isolation between tenants, protection of tenant data, and supervision of tenant operation behavior.

3. Evaluation Methods

3.1 AHP.

AHP (Analytic Hierarchy Progress) [4] makes factors which are related to the decision objective qualitative become criteria, scheme such as level, and build the AHP Hierarchy model which is as shown in figure 2. Through the pairwise comparison of the importance degree of a certain relevant factor at the same level, the quantitative method of the importance degree of the hierarchical factor to the target factor is obtained by calculating the importance degree of the hierarchical factor from the bottom layer to the top layer.

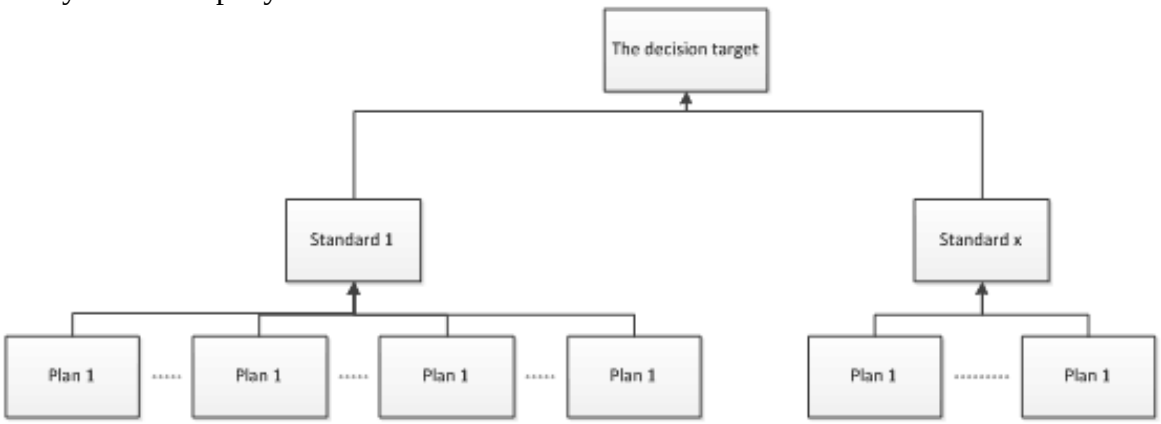

Fig. 2 The AHP Hierarchy model

3.2 FCE (Fuzzy Comprehensive Evaluation Method).

Fuzzy Comprehensive Evaluation [5] is a comprehensive evaluation method that converts qualitative evaluation into quantitative evaluation index by counting the frequency of the qualitative evaluation of the indicator elements in the same indicator set appearing in the evaluation set of each grade. When using FCE to calculate the quantitative evaluation results, it is necessary to determine the weight vector of each fuzzy index element. For the same decision-making, if the hierarchical model constructed by AHP method is taken as the tree structure of fuzzy index set in the FCE evaluation process, then the weight vector calculated by AHP method can be used as the index factor weight needed in the FCE evaluation process.

3.3 Establish a Hierarchical Model.

With the security of IaaS platform as the decision-making target, the index elements of the IaaS cloud computing security evaluation index model are decomposed into the criteria layer and scheme layer, and the hierarchical structure model as shown in figure 3 is established. The first layer is the evaluation target that is IaaS platform security; the second and third layers are assessment criteria corresponding to assessment categories and assessment subcategories.

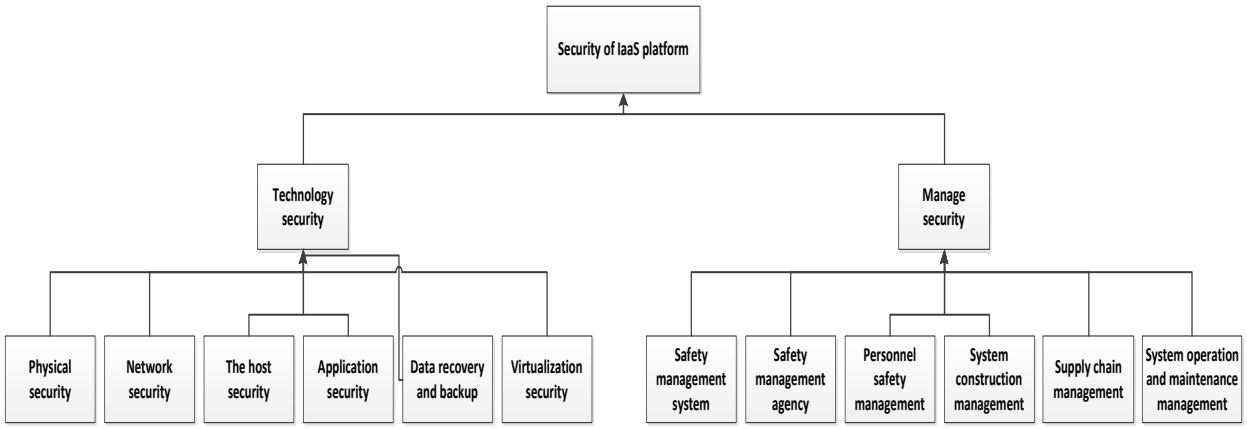

Fig. 3 The hierarchical structure model

4. Summary

According to the experience of grade protection evaluation in China, IaaS cloud computing currently enjoys the highest utilization rate among the systems that need to be managed and protected according to the requirements of grade three protection. This paper only proposes an index model for the security assessment of cloud computing platform provided by IaaS cloud service providers from the perspective of three-level protection security requirements. But this type of cloud computing platform is only part of the cloud computing environment information system, it only studies its safety evaluation index model which is not enough, and when the AHP-FCE evaluation method is used for statistical calculation of evaluation data, the weight data of each indicator in the evaluation indicator model are derived from the experience judgment of experts, and its sample is small. Therefore, providing tools that can automate the construction of assessment indicator model based on hierarchical protection security indicator system can greatly reduce the repetitive work in the process of model construction.

Acknowledgements

Source of funding: NARI Group Science and Technology Project “Infrastructure Cloud Service Platform Technology Research and Application in NARI cloud”.

References

[1] Ed Anderson, L.L Lam, Yanna D. et al. Forecast: Public Cloud Services, Worldwide, Vol. 13 (2013) No.4, p.2011-2017.

[2] UNCTAD: The Cloud Economy and Developing Countries. Unctad, Vol. 2 (2013) No6, p.20-25.

[3] Latif R, Abbas H, Assar S, et al: Cloud Computing Risk Assessment: A Systematic Literature Review, Vol. 1 (2014) No.276, p.285-295.

[4] Dastjerdi A V, Tabatabaei S G H, Buyya R: A dependency-aware ontology-based approach for deploying service level agreement monitoring services in Cloud, Vol. 4 (2012) No.42, p.501-518.

[5] Saaty T L: How to make a decision: The analytic hierarchy process, Vol. 1 (1990) No.48, p.9-26.