Research on New Virtualization Security Protection Management System Based on Cloud Platform

Zihong Li¹, Guangxu Liu¹, Yijie Dang¹, Zhijie Shang¹, Nan Lin¹

¹State Grid Information & Telecommunication Branch, Beijing, China, 100761

*Corresponding author e-mail: Lizihong@sgit.sgcc.com

Abstract. As an emerging product under the condition of informatization, the utilization of cloud platform in many industries has brought fundamental changes to the production and business model in related fields. The cloud platform provides rich and diverse utilization services to terminals through multi-dimensional integration of different IT resources. With the in-depth utilization of cloud platform, the security problems it faces are becoming more and more prominent. The traditional network security protection means have been difficult to effectively adapt to and deal with the security threats under the new situation of cloud platform utilization. As a prominent part of building cloud platform, the construction level of virtualization security protection system will have an intuitive impact on the security of cloud platform. At present, the virtualization security protection management system under cloud platform is facing direct threats from virtual machine deployment, virtual machine communication and virtual machine migration. Based on this, this paper studies the virtualization security protection management system of cloud platform from the perspective of virtualization security tech, so as to ameliorate the stability, reliability and security of cloud platform.

Keywords: Virtualization Security Protection, Cloud Platform, Informatization

1. Introduction
The in-depth utilization of cloud computing platform in various fields has changed the operation mode of relevant industries to a great extent. The cloud platform organically integrates information resources represented by networks, servers and software, so as to provide information services to customers in the form of overall packaging [1]. The service resources provided by the cloud platform can be easily accessed and used by users, so it can bring higher utilization value to users. The utilization of cloud platform virtualization tech not only brings the innovation of enterprise and industry information business architecture, but also introduces new information security risks and challenges. This requires cloud computing related service providers to formulate targeted virtualization security protection schemes and management systems based on the typical characteristics and practical needs of virtualization information security protection, so as to provide more effective support for more extensive and in-depth utilization protection of cloud platform.
With the increasingly severe threat of network security, cloud platform operators are not only improving resource utilization, but also actively improving the security of cloud platform [2]. In the process of providing information services, the security threats faced by the cloud platform are mainly manifested in unauthorized malicious access, modification and damage to the cloud platform. Secondly, the cloud platform is also facing internal and external security threats, mainly in malware attacks. The clustering and layering characteristics of cloud platform make the traditional security protection measures unable to effectively deal with the security attacks and threats against cloud platform. Therefore, according to the virtualization characteristics of cloud platform, focus on improving the security and stability of cloud platform, so as to strengthen the stability and robustness of cloud platform.

In addition, as an prominent system providing systematic services, cloud platform plays an prominent role in its security, information integrity and availability. The cloud computing platform fully integrates several aspects of virtualization tech, as shown in Figure 1 below, and realizes the prominent transformation of cloud platform in the safe operation of virtualization. On the one hand, the new virtualization security protection management architecture based on cloud platform supports the practical requirements for data collection, storage and forwarding; On the other hand, it supports structured and unstructured multi-level security situational awareness.

![Diagram](image)

**Figure1.** Integration elements of cloud computing platform virtualization tech

In short, with the deepening utilization of cloud platform, in order to effectively deal with the severe security situation faced by cloud platform, targeted countermeasures need to be established according to the virtualization characteristics of cloud platform and new attack methods. Build a new virtualization security protection management system based on cloud platform [3]. While improving the virtualization security service capability carried on the cloud platform, it supports multi-dimensional security mode and realizes the customization and self-service of cloud platform security policy. Therefore, the research on the new virtualization security protection management system based on cloud platform has prominent practical value.

2. Virtualization characteristics of cloud platform and its security threats

2.1. Typical characteristics of cloud computing platform

The typical characteristics of cloud computing platform include virtualization of computing and services and parallel processing of large-scale data [4]. Each physical environment of the traditional security protection model is relatively independent, including security products to protect servers and utilizations. After the virtualization of cloud platform, all virtual machines share resources. The virtualization of cloud platform computing and services makes virtual machines and utilizations likely to move or change at any time. Traditional security software causes resource conflict, reduces the density of virtual machines, and protects the system security through regular scanning, virus database
updating and resident in memory. The virtual machine of the cloud platform needs to have a fully configured client and the latest virus library.

2.2. Security challenges faced by cloud computing platform
The unique characteristics of cloud computing platform, such as data and service outsourcing, virtualization, multi-tenant and cross domain sharing, have brought new challenges to the security of the whole platform. The security and privacy problems faced by cloud platform have become an prominent obstacle to its further utilization. The computing environment faced by the cloud platform makes it more dependent on the network and servers, resulting in greater security and privacy problems and security and confidentiality risks [5]. Firstly, the characteristics of data and service outsourcing of cloud platform make it at risk of privacy disclosure and information theft. Secondly, the characteristics of multi-tenant and cross domain sharing of cloud platform make the establishment, management and maintenance of trust relationship more difficult, and service authorization and access control become more complex.

In addition, the virtualization characteristics of cloud platform make a large number of virtual services rented by users more vulnerable to covert collaborative attacks [6]. Resource virtualization supports the deployment of virtual resources of different tenants on the same physical resources, which facilitates malicious users to implement side channel attacks with the help of shared resources.

2.3. Challenges of cloud platform virtualization security management protection
The security challenges and threats faced by the cloud platform under the new situation make the traditional and single means of security management and protection unable to effectively meet and adapt to the security protection requirements under the new system. Safety control needs to be carried out in multiple dimensions and levels such as policy, tech and supervision. Secondly, the traditional security management system, such as encryption mechanism, security authentication and access control, cannot effectively meet the security protection needs of cloud platform [7]. In addition, the establishment of multi-dimensional and multi-level privacy security system, fully homomorphic encryption algorithm, dynamic service authorization protocol and virtual machine isolation strategy has become an prominent measure to carry out cloud platform security protection.

3. Construction of cloud platform virtualization security protection management system

3.1. Security protection scheme for cloud platform virtualization environment
The architecture of the virtual environment solution is shown in Figure 2 below. Firstly, the cloud platform virtualization environment is facing the problem of resource contention. In order to build agent-free security, have the ability to perceive the virtual environment, and establish the security tasks distributed based on the overall resources of the virtual machine, it can effectively avoid resource contention.
Secondly, aiming at the problem of protection gap during the real-time startup of cloud platform, it is necessary to establish a security virtual machine deployed based on virtual machine and use the latest threat feature library in real time, so as to identify security threats in real time and offline. In addition, aiming at the protection blind spots between cloud platform virtual machines, a virtual environment aware security solution integrated with virtualization platform is established to effectively eliminate the protection blind spots [8]. To solve the problem that individual virtual machines on the cloud platform are difficult to manage effectively, it is necessary to integrate with the virtual environment management platform VMware vCenter, so as to effectively detect virtual machines with insufficient security level.

3.2. **Cloud platform desktop virtualization security protection scheme**

The architecture of cloud platform desktop virtualization security protection is shown in Figure 3 below. With the help of IDS/IPS, known zero-day attacks launched through security vulnerabilities are detected and prevented. Secondly, use web utilizations to protect web utilization security vulnerabilities. Use virtual patches to provide patch free protection measures when patch updates cannot be provided in time in the user environment [9]. In addition, the firewall is used to reduce the attack level, prevent DoS attacks and defects, and realize monitoring scanning. Using virus killing software to detect and intercept malware. Detect malicious and unauthorized changes in prominent system directories, files and registry entries through integrity monitoring. Log audit is used to optimize and identify prominent security events from massive data.
4. Utilization of virtualization security protection management system of cloud platform

4.1. Functions of virtualization security protection management system of cloud platform
The design of virtualization security protection management system of cloud platform needs to be carried out from the dimensions of access security, design security, host security, multi-tenant resource isolation and data storage security. The virtualization security protection system of cloud platform needs to establish DDoS attack defense, intrusion defense, and vulnerability analysis and situation awareness [10]. The implementation formula of container virtualization tech is shown in formula 1-2 below. In addition, the virtualization security protection management system of the cloud platform can provide traffic traction and services, realize centralized platform management, provide permission management and development interfaces, and provide cloud security function services. In which, $L$ is the container engine and $D$ is the container, so as to ensure the consistency between the execution environment of the hosted utilization and the previous definition.

$$L = C_{group} + N + \text{CI}_{\text{root}} + V$$  \hspace{1cm}(1)

$$D = L + \text{AUFX} + L = C_{group} + N + T$$  \hspace{1cm}(2)

4.2. Utilization of virtualization security protection management system of cloud platform
The cloud platform introduces network traffic into the virtual service chain or virtual machine according to the user service chain and virtual machine configuration, and processes the returned traffic and sends it to the user. Secondly, provide differentiated security protection services according to the personalized strategy of the cloud platform. In addition, the access point equipment realizes user differentiation, drainage and diversion, and ensures the availability of the network. The virtualization security protection management system of the cloud platform provides traffic traction and services, centralized management of the platform and cloud security function services.

5. Conclusion
In summary, build a new virtualization security protection management system based on cloud platform. While improving the virtualization security service capability carried on the cloud platform, it supports multi-dimensional security mode and realizes the customization and self-service of cloud platform security policy. By analyzing the virtualization characteristics of cloud platform and the security threats it faces, this paper studies the trend and challenges of cloud platform virtualization security management and protection. Through the research on the construction of cloud platform virtualization security protection management system, this paper analyzes the security protection
scheme of cloud platform virtualization environment, and finally studies the construction scheme and utilization function of security protection of cloud platform virtualization environment.

References
[1] Gu Ziwei. Research on Virtualization security under cloud computing tech [J]. Wireless Internet tech, 2015 (19): 89-90.
[2] Hu Yang, Hu Xin. Research and analysis of cloud security based on Trusted Computing [J]. Information network security, 2013 (S1): 10-12.
[3] Li Anqi, Zhang Lei, Zeng Zhangfan, et al. Cloud computing helps military information security [J]. Computer science, 2016, 43 (B12): 170-173.
[4] Liang Jiliang, sun Jiayan, Han Hui. Security and credible defense system in the era of big data [J]. Cyberspace Security, 2018, 9 (12): 35-40.
[5] Pan Lin, Chen Ping, Yu Han, et al. Design of trusted security cloud protection system [J]. Science, education and culture, 2016 (1): 176-178.
[6] Shi Haibin, Zhong Zhujun. Cloud security system construction based on SDN and nfV [J]. China financial computer, 2015 (11): 26-28.
[7] Wang Gang. Multi region secure cloud computing architecture based on SDN tech [J]. Information security research, 2015, 1 (1): 86-91.
[8] Wang Xiaodi, Zhang Yunyong, Liu Dy, et al. Research on security tech of cloud computing virtualization [J]. Telecommunications Science, 2015, 31 (6): 1-5.
[9] Wei Yin. Network information security tech based on cloud computing environment [J]. Network security tech and utilization, 2018 (1): 58-59.
[10] Xie Ying. Research on security protection tech of cloud computing data center [J]. Journal of Southwest University for Nationalities (Natural Science Edition), 2018, 44 (06): 70-74.