

Construction and Application Research of Education Cloud Security System

Shibin Song^{1,2,a}, Junmei Liao^{1,b*}

^ae-mail:591732693@qq.com, * Corresponding author: b48042663@qq.com

¹Sichuan University Jinjiang College, Mei Shan, Sichuan, China

²Sichuan Public Project Consulting Management Co., LTD., Chengdu, Sichuan, China

Abstract—This paper introduces the application status of education cloud, analyzes the security risks faced by education cloud, puts forward an education cloud security system based on the development trend of cloud security technology, and carries out functional verification through a typical case of education cloud network security in a university, providing data support and security policy reference for education cloud network security.

Keywords- Education cloud; Security risk analysis; IaaS; PaaS; SaaS; Safety system research; Application case

1 INTRODUCTION

Education cloud provides information teaching, scientific management and other services for educational institutions, teachers and students in a dynamic deployment and on-demand service model. It is the in-depth application of cloud computing technology in the field of education, providing convenience for traditional education, teaching and educational administration management, and promoting the innovation of traditional teaching and educational administration mode. With the wide application of education cloud, the problem of network security has become increasingly prominent, and the need to build an education cloud security system has become increasingly urgent.

2 EDUCATION CLOUD SECURITY RISK ANALYSIS

As a key technology of cloud computing, virtualization not only improves the efficiency of cloud infrastructure, but also brings many new problems. The higher the degree of application of education cloud and the larger the amount of data, the higher the network security risk [1]. The success of the cloud computing model depends on powerful and reliable virtualization and distributed computing technologies, which rely on the physical layer composed of computing, storage, network and other devices. In the cloud computing information system, the commonly used storage media include hard disk, disk, tape, printer paper, optical disc, etc. Using these

storage media to store and exchange data greatly facilitates data transfer and exchange, but also brings great security risks to the cloud information system. The physical security of cloud platforms mainly includes security risks such as natural risks, operational risks and personnel risks [2].

2.1 Risk of leakage of students' sensitive information

During the deployment and operation of an education cloud system, students should be informed of how to protect private information and the legal obligations to use the platform. In order to prevent network vulnerabilities from malicious attacks, it is necessary to do a good job of basic network security protection of the platform.

2.2 Risk of maliciously tampering with teaching information

Teachers with legitimate user accounts may be responsible for deliberate destruction of teaching. Legitimate accounts are not properly kept, leading to account leaks, and others illegally log in to the education cloud platform database to load malicious information or tamper with teaching content.

2.3 Teaching network security risks

In the education cloud platform, only legitimate protocols and licensed services are allowed for login access and data transmission, which may face network intrusion and malicious attacks.

2.4 Data security risks of teaching information system

The education cloud uses encrypted data to achieve a certain degree of confidentiality in the process of data transmission, but the integrity of the data cannot be guaranteed.

2.5 Risk of malicious SQL attack [3]

Attackers use system vulnerabilities to construct legitimate SQL conditions to directly enter the business database system at the back end of the system to perform unauthorized data reading and writing, and successfully bypass or cheat the user authentication of the website. After successful entry, attackers tamper with, load information and maliciously spread bad content, and plant backdoor programs that seriously affect the normal operation of the system and lead to system crash.

3 CONSTRUCTION OF EDUCATION CLOUD SECURITY SYSTEM

The security of cloud computing information system equipment should consider the security control of equipment placement, power supply, equipment maintenance and disposal [4]. The network security of education cloud must build a strict security system from two levels of technology and management. Solving the information infrastructure from the technical level is the key element to ensure the security of the platform. The secure infrastructure should be based on the self-planning and construction of the education cloud and focus on on-demand

configuration, and the openness and dynamic reconfiguration should be emphasized in the system construction process [5]. In order to reasonably grasp and deploy resources on demand, problems existing in resources should be solved from the aspects of dynamic reconfiguration, real-time monitoring and automatic deployment. The talent team, mechanism and operation and maintenance at the management level are the key elements to ensure the safe operation of education cloud. Based on the security risks of education cloud, education cloud security needs to make full use of the characteristics of cloud computing platform on the basis of traditional information system security measures, and adopt advanced information security technology to improve the security of cloud computing platform [6]. This study proposes to divide the cloud computing platform boundary and physical resource boundary into three layers to build an education cloud security system, namely, infrastructure layer, platform component layer and application access layer, as shown in Figure 1. The security protection and information security management of the education cloud platform are realized by implementing security event handling policies for each layer and strict management of security logs.

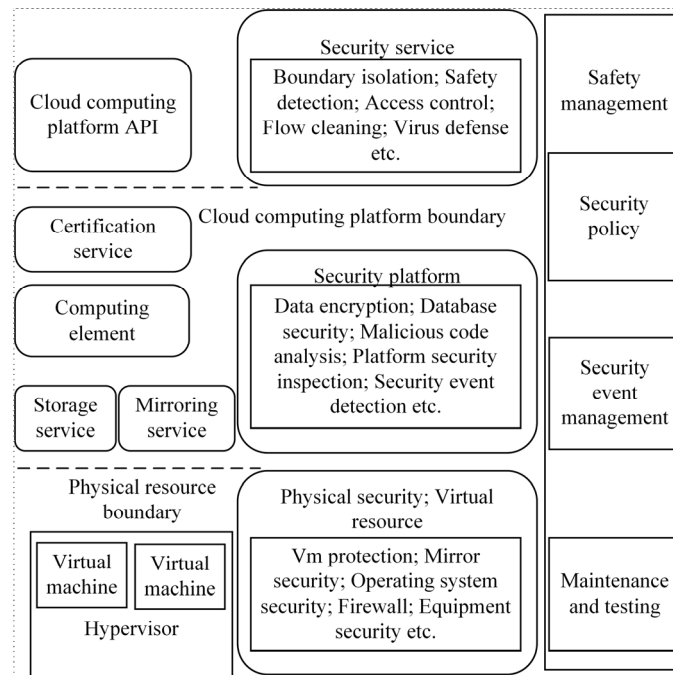


Figure 1. Education Cloud security architecture

3.1 Infrastructure Layer

Security protection measures at the infrastructure layer mainly involve physical device security, network security and virtualization security [7]. Physical device security involves geographic and physical environment security. The protection of the physical environment where cloud computing platforms are located includes fire prevention, waterproofing, anti-static, lightning protection, etc. Physical machine security is directly related to VM security. In terms of network security, authentication, authorization and access control must be implemented by

means of IPS and firewall. IDS can be deployed to detect network attacks and realize automatic timely alarm. To prevent the education cloud platform from DDoS attacks and prevent a large number of resources from being controlled by attackers, a traffic monitoring system is deployed for the data traffic entering and leaving the education cloud platform. Deploy a malicious code protection system to protect the physical server system and Hypervisor from intrusion. Communication between physical machines or virtual machines in the education cloud platform enables traffic monitoring and malicious code prevention to prevent network intrusion from spreading. Virtualization security prevents virtual machines from being invaded through physical machines and prevents virtual machines from horizontally attacking other virtual machines or vertically penetrating the operating system and virtual machines hardware to ensure the normal running of the dedicated machine OS.

3.2 Platform Component Layer

The security protection measures at the platform component layer are to ensure the security of various operations and data processing processes throughout the life cycle of the cloud [8]. Among them, the authentication and authorization process involves the application of encryption algorithms and key management, and can use public key infrastructure (PKI) or universal Unique identification code (UUID) for authorization and authentication. Storage services involve the whole life cycle of data generation, transmission, storage, use, migration, destruction, backup, and recovery, and perform data security management such as data classification, classification, identification, encryption, audit, and destruction[9]. Disaster recovery backup establishes and maintains a backup storage system in the same city or another location, utilizing physical separation to ensure the system and data's defense against catastrophic events.

3.3 Application Access Layer

Application security measures at the access layer require user identity authentication, strict access control policies and rights management to filter visitors, and effectively monitor the communication inside and outside the security zone. The abnormal traffic detection and analysis system is used to analyze and filter traffic [10]. The Web application firewall checks traffic based on preset security rules and analyzes traffic statistics, monitors the geographical distribution, application composition, and change trend of cloud computing platform traffic in real time, and generates statistical tables. Security zones are business premises which require protection by the cloud service provider and physical areas that contain protected information processing facilities. Security management provides security policies to ensure service continuity, manage and evaluate security events and logs. The manager of the cloud computing platform can be equipped with a special security management organization and management personnel to ensure the normal operation of the education cloud platform system.

4 EDUCATE CLOUD SECURITY APPLICATION CASES

Taking the education cloud of Zhejiang University in China [11] as an example, the typical application of Tianchi experiment cloud computing platform in the security compliance

construction scenario of teaching information system is analyzed in detail from the aspects of case overview, demand analysis, scheme design, deployment and implementation, and case effect, and the effectiveness of the education cloud security system proposed in this study is functionally verified.

4.1 Case Overview

In 2018, Zhejiang University adopted Alibaba Cloud technology framework to build a set of cloud computing platform. At present, the cloud computing platform has been completed and put into use, which mainly provides cloud resource services for various faculties and departments of Zhejiang University and other universities in Zhejiang Province, supports the teaching information system and educational administration system, builds Zhejiang University's own education cloud, and builds a cloud ecosystem in the education industry. However, in the early stage of education cloud planning and construction, security construction was not fully considered, especially security construction on the cloud. In order to solve the security risks existing in the teaching business system and prevent the leakage of teaching information and data, Zhejiang University plans to establish and improve cloud security construction and comprehensively build the service capability of the cloud ecosystem.

4.2 Requirement Analysis

The education cloud of Zhejiang University in China needs to meet the security protection of the educational administration system on the education cloud, the security compliance requirements of the educational administration system on the cloud, the unified management and on-demand distribution of cloud security resources, and the security independent management and self-service of cloud tenants (the department's own system).

4.3 Scheme Design

China Anheng Information Company adopted Tianchi hyper-converged cloud security solution to help Zhejiang University build a privatized cloud security resource pool in the cloud room. The security capabilities provided by the cloud security resource pool include: comprehensive vulnerability scanning, next-generation cloud firewall, Cloud We application firewall, web tamper prevention, cloud fortress machine, cloud database audit, EDR, and cloud comprehensive log audit. Personnel security measures include detailed understanding of the information of internal personnel with access rights to the cloud infrastructure platform, adhering to the principle of personnel security management, reasonable assignment of responsibilities, implementation of personnel security training and other effective measures to strengthen personnel security; When deploying security-related work, there must be two or more people present for each work to avoid mishandling; Each security staff member cannot hold a security-related post for a long period of time, which would preserve the competitiveness and mobility of the post. This solution provides security service capabilities for tenants on the education cloud, and realizes cloud security capabilities as a service. Tenants on the cloud can log in to the Tianchi Cloud Security Management Platform to apply for cloud security services based on their service requirements to ensure the security of the cloud service system.

4.4 Deployment Implementation

The education cloud deployment structure of Zhejiang University in this scheme is shown in Figure 2. The Zhongtianchi Hyper-converged appliance connects to the core switch of the Zhejiang University Education cloud computing platform in off-line mode. It uses policy-based routing to pull inbound and outbound traffic from the cloud computing platform, and cleans and protects inbound and outbound traffic based on the security capabilities of the cloud security resource pool. Security measures are taken for physical hosts, host operating systems, VM operating systems, hypervisors, and applications to ensure cloud platform virtualization security. In the cloud computing environment, the security protection of physical facilities and the environment is mainly for environmental consideration, access control, monitoring, personnel identification, and illegal behavior detection.

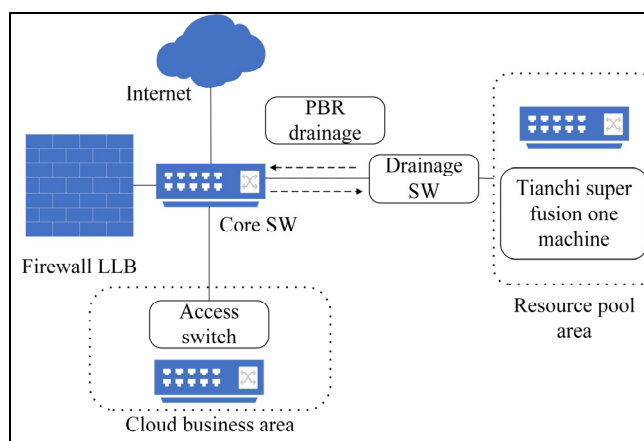


Figure 2. Education cloud deployment structure of Zhejiang University in China

4.5 Case Effect

The construction and application of the education cloud computing platform of Zhejiang University in China has improved the security capability of the cloud computing platform itself, built a unified security resource pool, formed a cloud security operation management center, and strengthened the security of the cloud computing platform itself. Simplify Hypervisor code, optimize code quality, reduce code vulnerabilities, and simplify Hypervisor functionality. It provides good isolation for virtual machines to prevent malicious virtual machines from using the vulnerabilities of the Hypervisor to threaten other virtual machines. It enhances the security of I/O operations on VMS. I/O operations require VMS to interact with external devices and are simulated by the Hypervisor. If the simulation goes wrong, it affects all virtual machines on the entire platform. It provides multiple security services to solve the security problems of cloud business systems, realizes the dynamic allocation and on-demand use of cloud security resources, realizes the unified management of cloud security, and creates cloud security value-added services.

5 CONCLUSION

Online education platforms have developed by leaps and bounds in 2020. In the future, cloud computing applications will continue to be highly respected as an effective way for educational institutions to achieve educational informatization. With the strong support of China's financial sector for education informatization, it is expected that the application revenue scale of cloud computing in the education industry is expected to grow rapidly at a growth rate of about 22% from 2020 to 2025, and the market size is expected to reach 28.5 billion yuan by 2025. Efforts to build an education cloud security system, promote the construction of education cloud service standards and standardize the development path of education cloud, and realize the dynamic deployment and on-demand use of education clouds are inevitable requirements for the construction and wide application of education clouds in China.

REFERENCE

- [1] Huang, K. (2019) Research on security technology of education cloud information resource service platform. *Journal of Hubei Second Normal College*,36(02): 25-29.
<https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTIOAiTRKibYIV5Vjs7iLik5jEcCI09uHa3oBxtWoEibNMKTyG0bfNqnbv4ptMML0gFKQIXZ0jCXWhyr9VIH&uniplatform=NZKPT>
- [2] Gu, H. (2021) Research and construction of security model of education cloud platform. *Information technology and informatization*, 04:193-194. Doi:10.3969/j.issn.1672-9528.2021.04.061
- [3] Fan, X. (2022) Access control model architecture based on data classification and grading system of education cloud platform. *Information security research*, 8(04): 400-407. DOI:10.12379/j.issn.2096-1057.2022.04.11
- [4] Hu, H. (2022) Research on the construction of security protection system of e-government information system, *Computer age*, 10: 147-149. DOI:10.16644/j.cnki.cn33-1094/tp.2022.10.036.
- [5] GAO, Q. (2022) Construction of e-government cloud security audit system based on big data. *Technology economy and management research*, 02:8-14.
https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTIOAiTRKibYIV5Vjs7iJTKGjg9uTdeTsOI_ra5_XQwP0vy2hTI1PZWHxmEEPlaz2vZZtnf1FhSG59b-znVA&uniplatform=NZKPT
- [6] Zhao, H. (2023) Research on the construction and development of government cloud security operation system. *Information and computer (theory)*, 35(04):65-68.
https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTIOAiTRKibYIV5Vjs7ioT0BO4yQ4m_mOgeS2ml3UIm3JTwcW8QPh90-J2XNybZA2nofzCCxq7_XQybHhQ3B&uniplatform=NZKPT
- [7] Zhang, B. (2022) Research on digital government security system. *Telecommunication engineering and standardization*, 35(12):1-7. DOI:10.13992/j.cnki.tetas.2022.12.005.
- [8] Zhong, Y. (2022) Design and implementation of education cloud platform from the perspective of Community: A case study of regional education cloud platform. *Chinese information technology education*, 15:95-98.
https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTIOAiTRKibYIV5Vjs7iM4VjA7s_Xyk4M-4Xrf6_eVTREoq5BXQS6GybrLyjECMQE55DF19qFjfyV2WkdZ1W&uniplatform=NZKPT
- [9] Wang, L. (2019) Construction and application of educational cloud in Heilongjiang Province. *Modern educational technology*, 29(02):107-112. DOI:10.3969/j.issn.1009-8097.2019.02.016
- [10] Wu, D. (2018) The development trend of foreign education cloud and its enlightenment. *Chinese educational informatization*, 11:21-25.

<https://kns.cnki.net/kcms2/article/abstract?v=3uoqIhG8C44YLTIOAiTRKibY1V5Vjs7i0-kJR0HYBJ80QN9L51zrP24e5qqbY7fKdPFO9HXkf4-JghT7FiuPqPw4mIptLJuk&uniplatform=NZKPT>

[11] Miao, C. (2021) Cloud security management and application. People's Posts and Telecommunications Press, Beijing.