Research on Omnidirectional Multi-angle Information Security Technology under Cloud Computing and Big Data Environment

Tang Chao[a], Zuo Wentao

Guangzhou College of Technology and Business, Guangzhou 510800, China

tangtao@126.com

Keywords: big data environment; cloud computing; information security technology; research.

Abstract: At this stage, with the rapid development of China's economy and society, information technology has begun to integrate into people's production and daily life, and has gradually become an irreplaceable important technical means in people's production activities. Among them, the level of improvement of social development level by big data technology and cloud computing technology is very obvious. Through the application of cloud computing technology and the promotion under the big data environment, it can provide more convenient and convenient guarantee for people's life, enabling people to quickly complete the processing of matters and the inspection of information in the information environment. But in essence, big data is an open Internet environment. Cloud computing technology is also an important technology derived from the open Internet environment. Therefore, we need to focus on security issues in the application process. In this paper, the author will use the relevant theoretical knowledge to conduct a comprehensive analysis and research on the comprehensive multi-angle information security technology under cloud computing and big data environment.

1. Introduction

In recent years, the rapid development of data science and cloud computing technology has brought about a significant change in the basic architecture of information networks and information systems, as well as the system architecture. While these information technologies provide people with unlimited convenience, they also bring about very serious security risks. In the big data environment, various types of network intrusion methods are constantly appearing, which seriously jeopardizes information security and is of vital interest to people. Caused very serious damage. In view of this situation, many researchers at home and abroad have begun to study technical measures to improve information security performance under the technical environment of big data and cloud computing. The core of research on information security technology in cloud computing and big data environment is to use the way of improving system architecture, and based on this, establish a comprehensive multi-angle protection model to effectively prevent the open Internet environment. Information threats. I will discuss this in the following.

2. Problems faced by enterprises in information security in the context of cloud computing and big data

In the new social development environment, due to the intensified market competition, the information transmission volume and transmission rate between enterprises have also been greatly improved. In the informationized market environment, the quantity and quality of information held by enterprises largely determine the core competitiveness of enterprises. Driven by this development environment, enterprises urgently need to upgrade their information management level and build an information security management system, which will take the lead in the fierce market competition. However, from the perspective of construction and development, although many enterprises pay more and more attention to information security, their information security awareness still stays at a

  DOI: 10.25236/mmmce.2019.052

relatively shallow stage. In the information security management work, there is no deep security awareness and information used. Security technology has certain irrationality, which has led many companies to be attacked by hackers. A large amount of information leaks has brought a very serious negative impact on the economic benefits of enterprises. Based on the above analysis, we can see that many enterprises in China still have very obvious problems in information security work. They do not pay enough attention to information security management work, and have insufficient protection for core internal information. At the same time, internal information of enterprises Safety management personnel lack professional literacy and lack professional safety management capabilities. Therefore, it is difficult for enterprises to ensure efficient transmission of information in a confidential state during security management [1].

Under the support of big data technology and cloud computing technology, many enterprises have a certain degree of deviation in the understanding of information security technology. In the process of information security technology construction, there is no technical environment that combines big data and cloud computing. Therefore, in the future construction of information security technology, enterprises should make full use of the technological advantages brought by cloud computing and big data environment to provide a very high security index for the internal information of enterprises. At the same time, enterprises need to realize in the construction process that the realization of information security transmission is a gradual and systematic process. In the actual construction process, the enterprise follows the actual technical conditions of the enterprise, starting from the overall and detailed perspectives, and then improving from the root cause. The overall level of construction of the enterprise.

3. Cloud computing and information security protection under the big data environment

3.1 Data encryption principle

From the perspective of most enterprises, the internal core data of an enterprise often contains a large number of commercial secrets. If these data are directly transmitted, it will easily lead to the leakage of data during the transmission process. Therefore, the primary protection of information security technology The way is to encrypt the data. After many years of practice and development, the principle of data encryption has become the most widely used information security protection method. The more common encryption methods are private key encryption, public key encryption, etc. [2]. These methods can be encrypted according to the security requirements of users to ensure that the data content maintains a high degree of privacy during transmission. At the current stage of cloud computing technology and big data technology booming, data encryption has become the primary way for many enterprises to protect information security.

3.2 Content-aware encryption principle

Under the support of big data and cloud computing environment, information security technology has begun to develop to the intelligent level. The automatic protection and encryption of data information has become the main demand of enterprises in the development process of the information age. The specific technical principle of automated encryption is to embed content-aware software in the enterprise's data management system, so that the data is converted into a specific format that can be understood by the system, and then the corresponding automated encrypted password is set in it to prevent the information from being transmitted. A leak occurred in the middle. In this way, when users use software to transmit information and data, they can use sensitive signals to control information in an all-round way. This information can be automated to some extent, avoiding the hacker's unrestrained from the source. Attack [3]. The security factor of this information encryption mode is very high. When the data leaves the cloud platform for transmission, the content-aware software can encrypt it at the first time, which not only improves the efficiency and quality of data encryption, but also fully guarantees the data. Security, while the process of information interpretation is more systematic and standardized, which has brought great obstacles to

the cracking work of hackers.

3.3 Format encryption principle

The technical environment of cloud computing and big data has very high requirements on the stability of the user information transmission process. The format-preserving encryption principle can control the format and type of information and data as a whole, so that the perceived level of data content can be obtained. Substantial improvement. The core of the format-protected encryption principle is to implement the encryption algorithm by using sensitive data through blocks to encrypt the data on a large scale. Improve the stability of data transfer in an all-round way. Through the application of the format-protected encryption principle, enterprises can easily transfer long-length strings and save data to the same type in the same format [4]. Although the principle of format-protected encryption has been developed to some extent in the context of big data and cloud computing, there are still some problems in the implementation of this technology principle. The most typical one is that the function of cloud service is encrypted. In the process, it will be hindered. The access key must be obtained during the access process, and the plaintext data is needed in the process of accessing the key. The conflict in the encryption process seriously hinders the format encryption technology. It is played there, so in the future research process, how to reflect the functional completeness of data and the absolute security of data in the big data environment, further research and analysis by relevant departments and staff.

4. Cloud computing and key technologies in the big data environment

From the perspective of relationship nature, cloud computing technology is a new efficient and practical data transmission and processing method proposed in the big data environment, and it is used as an extension of parallel computing, distributed computing and network format computing. Cloud computing technology appropriately expands the original independent computing mode to form a parallel, data-centric computing model, which ensures the efficiency and stability of the computing process. The corresponding storage structures in cloud computing mainly include the following Several.

4.1 Iaas layer

The Iaas layer is the underlying structure in the cloud computing structure. It integrates and processes large amounts of data by constructing and arranging distributed state data centers. Based on cloud data and application service centers, the Iaas layer provides high quality and large enterprises. The number of resources. From another perspective, the Iaas layer needs to schedule hardware resources through the principle of on-demand distribution, in this way to provide personalized and customized services for enterprises. In view of the above characteristics, the security research of the Iaas layer mainly focuses on how to establish a low-cost data storage and processing unit under the premise of ensuring efficiency, thereby improving the ability of virtualization and de-dispersion technology to enable enterprises to provide STable service [5].

4.2 PaaS layer

The PaaS layer is the upper structure of the Iaas layer and is based on resources such as computing, storage, and the Internet provided by the Iaas layer. The PaaS layer can provide strong support for applications in the upper-layer cloud platform. The main storage technologies include GFS technology, HDFS technology, and so on. At present, under the condition of increasing data size and data complexity, enterprises have put forward higher requirements for data analysis and processing capabilities of the PaaS layer under various application scenarios. The security requirements of the PaaS layer are mainly concentrated in the following aspects. The first aspect is interface security. Because the technical environment of cloud computing is relatively open, in order to keep resources such as servers, storage boards and the Internet in the running process, For good scheduling management, the system needs to provide an open API interface. In this way, the running and

managing bottle of the cloud computing can issue commands to the script through the API interface, thereby implementing control over the device and issuing the policy. In this link, we can use the authentication mechanism or encryption key to solve the above problem [6]; the second aspect is the security of the database. From the perspective of access control, the database should be maintained during the operation. The complexity of the password, and restrict the login behavior of the illegal user. The verification password should be replaced within a certain period of time. The user who legally accesses the database should set the corresponding authority and perform the account with redundant and abnormal status for a period of time. Clean up. In the aspect of security audit, the audit work of the database needs to be deployed separately, and the behaviors, resource utilization status and core commands of the users in the database should be recorded in all aspects.

4.3 SaaS layer

The SaaS layer is a top-level structure that provides access services and is widely used in government departments and large enterprises. The government and relevant departments of the enterprise need to deploy the smart service software in the server of the cloud machine room. Users can obtain relevant service information through the Internet, and enjoy the convenient experience brought by smart management. The convenience requirements of the SaaS layer are mainly divided into the following points. The first point is the security of multi-tenancy. In this level, isolation is required to ensure the independence of the resource use process. Each user is accessed through the access control list. The boundaries of the access are controlled. It should also be noted that some of the applications in the SaaS layer are relatively sensitive to the data collected and generated. Therefore, some important core data needs to be encrypted during use, which will be more in the actual management process. Users participate in the management work. On this basis, a complete centralized identity authentication system can be established to prevent illegal access in the system. The second point is the security of the application. In general, we can deploy the web application. The form of the device provides the necessary security protection for the SaaS layer, thereby centralizing the security management of related application data.

5. Conclusion

In summary, cloud computing technology and big data technology are the mainstream technologies in the information environment, playing an increasingly important role in people's production activities and daily life. Therefore, in the process of actual use, we need to deeply explore its security performance to solve the security threats in the open information environment, so as to better enjoy the convenience brought by the information age.

References

[1] Shang Yongqiang. Discussion on Omnidirectional Multi-angle Information Security Technology in Cloud Computing and Big Data Environment[J]. Science & Technology Communication, 2018, 10(23): 142-143.

[2] Wu Weiqiang. Research and Practice of Omnidirectional Multi-angle Information Security Technology in Cloud Computing and Big Data Environment[J]. Communications World, 2017(14): 45-46.

[3] Shao Xiaohui, Ji Yuanxiang, Le Huan. Research and practice of all-round multi-angle information security technology in cloud computing and big data environment [J]. Bulletin of Science and Technology, 2017(1).

[4] Zhu Xiaoyan. Application of Big Data and Cloud Computing Technology in Financial Work [J]. China Finance, 2016(22):48-49, Total 2 pages.

[5]WANG Xin, ZHOU Xiaomei. Research and Simulation of Big Data Rational Diversion

Technology in Cloud Computing Environment[J]. Computer Simulation, 2016(3):292-295.

[6] Liu Jiawei. Information Security Technology in Cloud Computing and Big Data Environment[J]. Electronic Technology and Software Engineering, 2019, 148(02): 219.