10.18686/aitr.v2i2.4016

Design Strategy of Network Security Defense System Based on Big Data and Artificial IntelligenceTechnologies

Boyuan Hu

Fort Hays State University, Hays, Kansas 67601-4099

Abstract: In the context of the big data era, the Internet has become a crucial tool in people's daily life and work, and continuously changing their way of life, which is of great significance. However, with the rapid development of big data technologies and artificial intelligence tech-nology network security issues have become increasingly severe, the design of network security defense system based on big data technologies and artificial intelligence technologies has become a prominent research area. In this paper, we will analyze the design strategy of network se-curity defense system based on big data technologies and artificial intelligence technologies, so that big data technologies and artificial intelligence technologies can play a vital role in network security defense and ensure the security and stability of the network system.

Keywords: Big data technology; Artificial intelligence technology; Computer network; Network security; Network security defense system

Introduction

In the context of the big data era, big data and artificial intelligence technologies have been widely applied to various industries and have achieved better results. At the same time, network intrusion technology is also advancing with the development of computer technology, and the network intrusion methods have also undergone major changes, seriously threatening people's personal privacy and property security. Therefore, it is necessary to fully combine the current situation of network intrusion in the era of big data to develop the design of network security defense system based on big data technology and artificial intelligence technology, in order to enhance security for the computer network, and to protect personal privacy and property security.

1. Analysis of the current situation of network security in the context of the big data era

1.1 Rapid development of network invasion technology

In the context of the big data era, more and more people have begun to carry out the study of artificial intelligence technology and big data technology, effectively mastering network technology. However, some of these people who carry out the learning of big data technology and artificial intelligence technology have insufficient knowledge of the law or their own ethnical principle, and apply the learned technology to conduct website attacks for profit. This misuse has accelerated the advancement of network intrusion technology under the auspices of big data technology and artificial intelligence technology, which has increased the security risk of computer networks and made computing network security face more serious challenges.

1.2 More ways of network intrusion

Big data technology and artificial intelligence technology have driven advancement of the Internet of Things and the mobile Internet, resulting in increase complexity in the computer networks. Apart from conventional terminals such as computers, mobile phones and tablets, an array of intelligent terminals are connected to these networks. While these intelligent terminals bring greater convenience to people's daily life and work, thereby effectively improving people's quality of life. However, they also introduce vulnerabilities for network breaches and offer new avenues for cybercriminals, which leads to a surge in hacker intrusion techniques targeting computer networks.

2. Functional requirements analysis of network security defense system based on big data and artificial intelligence technologies

2.1 Infrastructure layer virtualization function requirements

Under the background of big data and artificial intelligence, the infrastructure layer of the network security defense system not only requires more advanced hardware facilities, but also a robust virtualization function. The virtualization function of the network security defense system can enhance the utilization of big data and artificial intelligence technologies, enabling more efficient distribution and sharing of com-

puter hardware resources. This, in turn, creates optimal conditions for improved performance of the computer system.

2.2 Demand for middleware layer management functions

The main function of the middleware layer of the network security defense system based on big data and artificial intelligence technologies is to streamline the processing of the input and output data flow. This enables a more scientific allocation of various data resources within the system, facilitating effective control of the access security of the computer network system. Furthermore, it enables the real-time monitoring of the system's operational status, so as to ensure high degree of stability and security. Therefore, when designing the network security defense system based on big data and artificial intelligence technologies, it is essential to enhance the middleware layer with more high-quality application functions such as load balancing, security detection and resource allocation.

2.3 Application layer service function requirements

The primary role of the computer network security defense system based on big data and artificial intelligence technologies is to offer users computer network security defense services. Therefore, in the process of designing computer network security defense system, it is necessary for the system to provide users with relevant services more conveniently, swiftly and reliably. The system should include functions such as user registration, user login, access authority control, authority allocation, system intercommunication, intrusion detection, system backup and data recovery to cater to the users' needs effectively.

3. Network security defense system design strategy based on big data and artificial intelligence technologies

3.1 Security defense function design

Under the background of big data and artificial intelligence, PCs and mobile terminals are the main sources of network attacks. The scope of network attacks is broader, and many network attack viruses have a longer incubation time. Therefore, in the process of designing a network security defense system based on big data and artificial intelligence technologies, it is necessary to fully integrate the actual situation of the current computer network as the basis for the design of the defense system. The network defense system has a certain degree of initiative to carry out network attacks, to protect the security of the computer network. In the specific design process, it is necessary to fully leverage the advantages of big data and artificial intelligence technologies as well as network security and defense needs in designing security and defense functions. Firstly, the system needs to have the ability to effectively manage the configuration of the system; secondly, it needs to have the ability to manage the users in the system; thirdly, it needs to be able to manage the security policy in the system; fourthly, it needs to be able to carry out real-time supervision and control of the network status; fifthly, it must generate and store the computer network operation logs; lastly, it should be capable of generating the corresponding network operation reports. Only with the above functions can it effectively meet the network security defense requirements in the context of the era of big data and artificial intelligence. The operation of the cybersecurity defense system is illustrated in Figure 1.

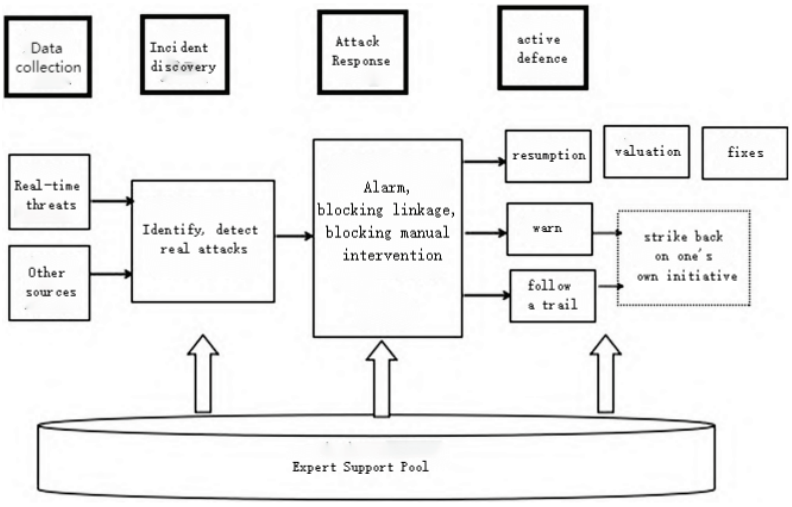

Fig. 1 Operation process of computer network security defense system

3.2 Firewall module design

Firewall is a crucial network defense against attacks for enterprises and individuals during computer network application. Although firewalls have a wide range of applications and can mitigate network attacks effectively, there is a common misconception that solely relying on

firewalls can fully secure a network, which may actually lead to many security issues. Therefore, when designing the network security defense system based on big data and artificial intelligence technologies, it is necessary for the designers to adapt the firewall module to enhance its performance against network attacks comprehensively. Implementing two firewalls can be beneficial: using the first firewall can regulate external users' access rights, and the second firewall to control internal users' network access rights. This dual protection mechanism enhances the defense capabilities of network system, ensuring a higher level of security.

3.3 Transmission encryption system design

The network layer protocol plays a crucial role in digital display data encryption. The encryption methods mainly consist of end-to-end encryption and link encryption in two forms, with the primary goal of utilizing encryption technology to achieve the analysis of the logical location. Among them, the link encryption method involves encrypting all links, and then processing data self-construction and transmission through communication nodes to ensure data protection. On the other hand, end-to-end encryption is more specific, utilizing the OSI model and software programming for data encryption processing. Moreover, the end-to-end encryption ensures that data transmission originates from the data source end, preventing any alterations during transmission, thus improving the security of data transmission effectively. The security of data information can be further reinforced through key management and other means.

4. Conclusion

In summary, this paper analyzes the current situation of network security within the realm of big data and artificial intelligence technologies. It explains the requirement for network security defense based on big data and artificial intelligence technologies, and integrates them thoroughly into the design strategy analysis of the network security defense system. Only by integrating the network security defense needs fully into a scientifically designed strategy for the network security defense system can we enhance the function of the system, and leverage the capabilities of big data and artificial intelligence technologies effectively in network security defense.

References

[1] Song Wuyang, Zhang Ni. Network security defense system design strategy based on big data and artificial intelligence technologies[J]. Network Security Technology and Application, 2022(7):56-57.

[2] Pi Xunxun, Wu Lisheng. Design of network security defense system based on artificial intelligence technology[J]. Wireless Internet Technology, 2023, 20(18):25-27.

[3] Tian Li, Wang Jie, Yu Xiao, et al. Design of network security attack and defense simulation platform based on virtual technology[J]. Information Technology, 2023(8):148-153.