Attack Threat and Response Strategy of Network Security in the Background of Artificial Intelligence

Songli Wu, Zili Wang

Zhumadian Vocational and Technical College, Zhumadian 463000, China.

Abstract: In recent years, information technology has been continuously updated, bringing brand-new technology experience to people. Artificial intelligence technology, is a relatively novel technology, has a significant role in the national economic growth and social development. The Internet is the basis of artificial intelligence technology, and the Internet has the characteristics of virtual nature. Therefore, the application of artificial intelligence in people's production and life can not only promote social progress, but also may have a greater impact on network security. Under the interference of many factors, the network security is threatened by many attacks in the background of artificial intelligence.

Keywords: Artificial Intelligence; Network Security; Attack

Introduction

With the deepening of the market economy system, the development speed of artificial intelligence technology is accelerating. At the same time, the technology and big data and the Internet and other continuous integration and penetration, so that people's production and life have undergone earth-shaking changes. In the sustainable development of artificial intelligence technology, artificial intelligence home appliance system has become an indispensable part and plays a significant role in the development of artificial intelligence technology. When people use artificial intelligence technology in their production and life, they may be threatened by network security problems. The update and development of artificial intelligence technology will inject new vitality into network security, but it also brings great challenges.

1. Threat analysis of network security attacks in the background of artificial intelligence

Threat analysis of network security attacks in the background of artificial intelligence Based on the background of artificial intelligence, network security is facing the threat of attack. One is the threat of denial-of-service attacks. This threat is a common threat during the construction of the AI network[1]. With the abundance of the network connection hardware equipment, the threat factors increase accordingly. Distributed construction of network equipment makes the network faced with a huge threat of denial of service attack, which has a great impact on the network security control effect. Second, malicious code security threats. Under the background of artificial intelligence, the network attacks in all links will damage the security of network operation. Especially in a single link of the network attack, the code under the malicious code programming attack means has a strong survival ability, which will affect the network security.

2. Network security defense technologies in the context of artificial intelligence

2.1 Intelligent social engineering attack techniques and anti-malicious code attack techniques

There are more types of network security defense techniques in the context of artificial intelligence [2]. Intelligent social engineering attack techniques, is one of the more common techniques. This technique is used to protect personal privacy data through the effective use of expert system methods, neural network methods, etc. to intelligently identify and process the process of virus attacks spread by computer worms or distributed by spam. Through the analysis of this technology, it is mostly applied in new phishing attacks where the attack targets are emails and social networking sites, and the attack form is code transmission carrier. In addition, with the development of artificial intelligence technology, malicious code survivability continues to increase. When new threats emerge from malicious code, the anti-virus engine needs to be continuously optimized and upgraded to counter malicious code products. The degree of optimization and upgrading of the anti-virus engine is closely related to the ability to resist attacks. Around the deep learning theory, malicious code attack technology can bring its advantages into full play [3]. TRPAI technology is a new technology developed by Tencent, which is based on deep learning to achieve the detection and killing of malicious code. Compared with machine learning, malicious code attack technology is able to learn automatically, identify key features of malicious code, and add or remove them intelligently.

2.2 Intelligent packet filtering firewall technology and vulnerability data mining technology

Based on the background of artificial intelligence, intelligent packet filtering firewall and vulnerability data mining technologies are also relatively new technologies. The intelligent packet filtering firewall technology effectively combines the Internet of Things and artificial intelligence technology, etc. By combing the network layer access control table ACL, the packet is analyzed from an intelligent perspective and filtered multi-functionally to achieve the purpose of controlling the forced access to internal and external network communications. Through the analysis of this technology, it is clear that this technology is based on information such as the packet source address, the port number used by the packet, and the packet destination address when judging the feasibility of packet passage. In general, the filtering host of this firewall system can run two processes, one of which is the filtering process; the other is the configuration process. The former can effectively filter and forward packets, and can transmit alarm information to the monitoring host in real time. The latter has the role of modifying the configuration of the filtering host itself or improving the filtering rules of the filtering host . Intelligent vulnerability data mining technology is based on the premise of identifying and analyzing defects intelligently without human intervention, and accomplishing unintended functions by exploiting the defect. Essentially, the technology is based on big data technology for intelligent mining of security vulnerabilities.

3. Counter strategies for cyber security attack threats in the context of artificial intelligence

3.1 Strengthen artificial intelligence risk management and network security ecological management

In the context of artificial intelligence, in order to effectively deal with the threat of cybersecurity attacks, artificial intelligence risk management and cybersecurity ecological management can be strengthened. On the one hand, strengthen artificial intelligence risk management. In the prevention of AI risk, the security of AI For exampletechnology can be scientifically assessed, and AI can be used to realize the enhancement of defense technology and improve network security management. At the same time, based on the work responsibilities of national government departments, in-depth analysis of AI network attacks, AI offensive and defensive technologies to the ground. On the other hand, strengthen the management of network security ecology. Network security governance cannot be achieved without the joint efforts of multiple parties including universities, government and enterprises. Relevant departments and organizations should strengthen cooperation, form a multi-resource system combining industry, academia and research, improve the sharing of resources, and form a management model that is group-oriented and combined with prevention and control. Enterprises should give full play to the advantages of human resources and data resources, and apply artificial intelligence technology in a practical and reasonable manner. Individuals should strengthen their awareness of cybersecurity, clarify the importance of protecting personal privacy through conscious learning, and scientifically distinguish the authenticity of online information.

3.2 Improve network security knowledge system and network security related system

When dealing with cyber security attack threats in the context of artificial intelligence, it is necessary to improve the cyber security knowledge system and cyber security-related systems. Strengthen the emphasis on technologies such as cloud computing and big data, integrate various technologies together, obtain a large amount of dynamic data, and build a real-time cybersecurity knowledge system to fundamentally enhance the defense capability of cyber attack threats. The data in this system can be divided into different structures. One of them is structured data. Such data can unify the representation of cross domain knowledge and improve the accuracy of cross domain knowledge on the basis of forming a network security ontology model. Second, semi-structured and unstructured data. This kind of data is more difficult to extract, so when extracting data, we can use category or joint marking method to reasonably extract the required data. In addition, improve the system related to network security. Usually, the system has a binding and normative role . When building AI-based networks, the state should scientifically respond to AI cybersecurity threats. While controlling network security threats, AI technology is reasonably applied, and under the premise of following national laws and regulations, the system related to the application of AI technology is improved, and the application process of AI technology is sorted out to ensure that the application of AI technology is based on evidence.

3.3 Targeted improvement of cyber threat control

In the context of artificial intelligence, the threat of cyber security attacks should be targeted to improve the level of cyber threat control. First, prevent the threat of denial-of-service attacks. As the scale of artificial intelligence networks continues to expand, the threat of denial of service attacks is on the scale of development. When dealing with network security threats, it is important to prevent and control the threat of denial-of-service attacks in a timely manner. From a certain point of view, denial of service network attack threats, in fact, belong to a single link threat. Thus, during the construction of AI networks, node protection technology should be reasonably applied to threat defense. Based on the existing network technology, incorporating node encryption technology can improve the level of security, encrypt the transmission of node area messages, and improve the level of information security protection. In the case of data locking protection, different forms of keys can be locked, which can guarantee information security. Second, address the threat of malicious code attack. Generally speaking, the attack of malicious code has a covert nature. Therefore, when dealing with such threats, it is necessary to pay more attention to malicious code mining. In-depth analysis of malicious code characteristics, effective control of malicious code.

4. Conclusion

In the era of Internet+, artificial intelligence technology has penetrated into various industries and has made remarkable achievements. Artificial intelligence has the characteristics of a double-edged sword, which may bring unlimited challenges and risks while safeguarding network security. Therefore, in the context of artificial intelligence, it is necessary to fully strengthen the attention to the defense capability of network security attacks. On the basis of clarifying the total threat to network security in the context of AI, the article deeply analyzes the network security defense technology in the context of AI. At the same time, the response strategy of cyber security attack threat in the context of artificial intelligence is studied from the aspects of strengthening AI risk management and cyber security ecological management, improving cyber security knowledge system and cyber security related system, and improving cyber threat control level in a targeted manner. Strong through this study, the foundation for the future improvement of China's cybersecurity level is laid.

References

[1] Fang BX, Shi JQ, Wang ZR, et al. Security threats of artificial intelligence-enabled cyber attacks and countermeasure strategies [J]. China Engineering Science, 2021, 23(3):7.

[2] Zhao YH, Chen Y. Research on the design of network security defense system in the context of big data and artificial intelligence [J]. Information Recorded Materials, 2022, 23(10):176-178.

[3] Song Z, Sun Q. Global critical information infrastructure security challenges and countermeasures in the context of artificial intelligence[J]. Information Security and Communication Privacy, 2022, 24(006): 2.