Journal of Artificial Intelligence Practice (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2023.060604
ISSN 2371-8412 Vol. 6 Num. 6

Research on the Application of Artificial Intelligence Technology in the Field of Network Security

Yang Zhang

Shanghai Xingwei College, Shanghai, 201300, China

Keywords: Artificial intelligence technology; Network security field; Application

Abstract: As an important component of national security, cyberspace security is facing increasingly severe and complex security threats. Cyber security attacks are becoming increasingly large-scale and automated. Security detection needs are expanding from point to area, and network security defense needs are transforming from passive to active. Wider areas of attack, stronger network attackers, and more passive defense methods require people to find network security defense strategies that are different from traditional methods. The application of AI (Artificial Intelligence) technology in the field of network security is an innovation in the traditional network security system, which has important guiding significance for further strengthening network security construction. The use of AI technology to enhance internet defense capabilities and enhance network security is widely anticipated. After using AI technology, network data can be monitored. During the process of network information monitoring, risky data will be prohibited from accessing and alarm messages will be issued to computer users, effectively avoiding the invasion of unknown threats and ensuring the security of internal computer information.

1. Introduction

The rapid development of the Internet and the extensive penetration of Internet technology in various fields of society have made people lament the Internet technology, but at the same time, they also show various concerns about the security problems it brings. Network security threats are showing a new development trend in the new era background. Cyberspace security, as an important component of national security, its security threat situation is becoming increasingly severe and complex, network security attacks are becoming increasingly large-scale and automated, the demand for security detection is expanding from point to surface, and the demand for network security defense is changing from passive to active [1]. Wider attacked areas, more powerful network attackers and more passive defense means require people to find different network security defense strategies from traditional methods. AI involves many fields and disciplines, such as logical linguistics, computer science, neural network science and other disciplines, and thus produces AI, a comprehensive discipline [2]. At present, with the rapid development of science and technology and the continuous improvement of computer network technology, the public has become accustomed to using the network to deal with various matters in life, such as office, entertainment, social interaction, etc., and more and more personal privacy is exposed on the network [3]. The application of AI technology in the field of network security is an innovation of network security

system in the traditional sense, which has important guiding significance for further strengthening network security construction. It is widely expected that people will use AI technology to improve the defense function of the Internet and strengthen network security. The application of AI has a very important role and broad development prospects. Through the deepening and strengthening of technology, it can provide a strong guarantee for network security [4]. The core of AI is algorithms, including traditional machine learning algorithms and non-traditional machine learning algorithms. Among them, traditional machine learning algorithms mainly solve simple application scenarios and structured data. Non-traditional machine learning algorithms mainly solve more complex application scenarios and unstructured data or diversified data [5]. Using traditional network security methods to maintain privacy can no longer meet the needs of the public, and AI technology is another opportunity to provide higher protection in the field of network security. The following is a simple analysis and discussion around the current situation of network security in China.

2. Basic Network Security Situation and the Concept of Artificial Intelligence

2.1. The concept of artificial intelligence

At present, AI technology has been widely applied in multiple fields, and its advantage lies in its fuzzy processing ability for massive data, especially for data that cannot be recognized and processed under artificial conditions. AI technology can make up for the related shortcomings [6]. As shown in Figure 1, AI technology can preprocess unknown problems. This ability to handle unknown problems is due to the fuzzy logic reasoning method of AI technology, which does not rely on accurate data models, but extracts useful information based on the presence of a large number of factors or fuzzy information in the network and conducts inference.

Figure 1: AI Technology

From the technical level, we can see that AI is a modern technology for research, simulation, development and utilization of human brain activities. It is mainly based on human brain activities and intelligent activity laws, and integrates neurophysiology, Cybernetics, computer science, linguistics and other disciplines to carry out systematic development, and ultimately achieve the effect and purpose of replacing human brain thinking with machines. However, unlike human brain thinking, it has significantly higher computational and processing capabilities. Applying it to the field of network security can make network security protection more powerful and efficient [7-8]. Attack behaviors in the network often change their manifestation. When these attack events change, they are difficult to be recognized by traditional network protection systems due to the lack of preestablished rules or patterns that can match them. Machine learning is not about using explicit rules to accomplish specific functions, but about abstracting and inducing knowledge and rules from a large amount of sample data through self-learning, making it more flexible and efficient [9]. After using AI technology, network data can be monitored. During the process of network information monitoring, risky data will be prohibited from accessing and alarm messages will be issued to computer users, effectively avoiding the invasion of unknown threats and ensuring the security of internal computer information.

2.2. Network security situation

Nowadays, the whole global society has entered the era of information and big data, and everyone can no longer be completely separated from the network. Many activities, information and even property have been transferred to the network, and they may be invaded, destroyed and stolen [10]. With the development of computer technology, a new product is derived, which is a new technical science. The theory, method, technology and application system for simulating, extending and expanding human intelligence are analyzed and developed. The proposal and application of AI technology not only reduces the consumption of resources, but also promotes the continuous development of Internet applications. The advantages of AI technology in application can be mainly described from six aspects, as shown in Figure 2.

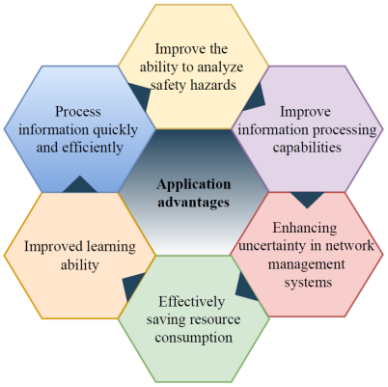

Figure 2: Advantages of AI technology in application

The current situation of network security in China is as follows: when users open computers and webpages, webpages will automatically pop up some strange interfaces or advertising information. Such webpages often have no value but some unorganized information, which has a bad influence on the normal use of users [11]. Typical network attacks include but are not limited to malware, botnets, phishing websites, traffic attacks, spam, etc. These attacks not only cause losses to individual users and enterprises, but more importantly, they will endanger the national economy and even national defense security. The boundary of traditional network security began to blur gradually, and it lost its binding effect. The dangers of zero-day vulnerability network attacks, DDoS, APT and other network attack means are getting higher and higher, and the difficulty of network security protection is increasing day by day. If network security is threatened, it may lead to privacy leakage and property loss, and the consequences may be large or small [12]. In this regard, we must further adopt efficient technology to strengthen network security protection, such as the scientific application of AI technology to the field of network security. Spreading bad information or viruses on the network at will to attract users' attention, bring users an extremely uncomfortable experience, and even cause users' password leakage, data loss or tampering with the network, port failure and so on. These phenomena are extremely unfavorable for the normal development of China's network security, which makes the computer network in an unsafe state for a long time more likely to cause hacker attacks, worms and virus breeding, and poses great danger to China's network security.

3. The specific application of artificial intelligence technology in the field of network security

3.1. Intelligent Identification of Network Access Data

AI technology can use the risk data stored in the security center for comparison, confirm the user's access behavior, and select to prohibit or allow access to the information returned by the security center. When AI technology is applied to network security protection, spam automatic

detection technology can leverage its own advantages. By adopting an intelligent anti-spam system, it can effectively prevent spam from entering the mailbox and achieve full time detection. AI technology can also learn autonomously based on user access habits, monitor high-risk websites that users frequently visit, and have the ability to store and share data information. All of the above advantages demonstrate the level of artificial neural network technology. It can completely establish a complete time series prediction model on its own basis, effectively identify Computer virus, enable us to get accurate protection results, and make an important contribution to the current network security protection. When the user is in a state of departure, they steal data information and forward it to an external database, using extremely covert intrusion methods that are not conducive to detection. So either of these two types of network attack methods will cause huge damage to the computer, causing operating system abnormalities, and causing economic losses to the enterprise. Intelligent abnormal behavior detection technology can rely on the operating environment of computer operating systems to quickly detect abnormal situations and report them to computer users. At the same time, it can also suppress and eliminate abnormal behavior, protect network security, and ensure the security of user information. Once the risk index of some websites increases, users will be reminded and access to relevant websites will be prohibited until the corresponding website risk index decreases to a normal level.

3.2. Intelligent firewall technology

Intelligent firewall technology is a technology that can adaptively adjust the security level based on the specific usage of users. Although it is a basic network security protection method, it achieves the combination of AI technology and traditional firewall technology, giving traditional firewalls the ability to "think". Intelligent firewall technology is an organic combination of AI and firewall technology. Compared to traditional firewall technology, intelligent firewall is a joint application of learning and memory, probability, and decision intelligence, which can effectively analyze and control data. Intelligent firewall is a combination of traditional firewall and AI technology. Its characteristic is that it no longer requires human intervention in setting up too many firewalls, and can even completely eliminate any settings. By analyzing a large amount of data and relevant intelligent learning, it can automatically make network security protection strategies, more effectively identify unsafe access or data up and down, and block and isolate them, Prevent viruses and attacks. Adjust the defense level of the firewall based on the comparison results and provide reminders to users. However, it should be noted that when using some software to retrieve network data, there may also be the phenomenon of activating smart firewalls. However, as users repeatedly allow data access to the software, smart firewalls will remember user behavior, thereby reducing unnecessary operations for users. During operation, it can ensure the transmission of internet data information and provide effective scientific defense against access control, preventing network systems from being invaded by virus information.

3.3. Intelligent traffic monitoring system

In most cases, the virus is lurking in the computer, and when the user leaves or does not use the computer for a long time, it sends information to the outside world through the network in a hidden way. In this case, the traditional network security equipment can't find the abnormality in time, and the loss caused to users is incalculable. When spam enters the system, the system will automatically detect and score it. When the score is below the standard range, the system will delete this information to avoid human misoperation. No matter what kind of virus, it will always cause the change of network traffic when sending data to the outside. Intelligent traffic monitoring system relies on the overall monitoring of computer environment to monitor the call and sending of abnormal data. For example, if the user does not operate through peripherals such as keyboard and mouse, the speed of uploading data by some programs from the background will be limited or even

prohibited. For people who often use e-mail for information exchange, the application of intelligent anti-spam system greatly improves the security of sending and receiving e-mail, and provides a guarantee for users' information security.

4. Conclusions

In summary, traditional network security protection techniques infer rules from known attacks and apply them to identify and prevent their operation. However, the constantly escalating various malicious attacks can bypass this mechanism and cause significant damage to network security, which requires the introduction of a new real-time detection and response security mechanism to replace previous rule-based prevention systems. The use of AI technology to attempt breakthroughs is a relatively new field. In practical applications, AI technology is applied to the level of network security far beyond the aforementioned categories, and there are more unknown technologies waiting for us to explore and discover. China needs to comprehensively strengthen overall planning, closely focus on the overall goal of building a strong online country and maintaining cyberspace security, and further improve and optimize the strategic planning, investment direction, scientific research layout, and talent training plan in the AI field. The effective application of AI can strengthen the security guarantee of the Internet, solve network security risks, and safeguard the construction of network security. The application of AI technology can achieve the transformation from traditional passive defense to active defense, provide users with a more secure internet environment, ensure user information security, and promote the further expansion of internet technology applications.

References

[1] Zhan K. Design of computer network security defense system based on artificial intelligence and neural network [J]. Journal of Intelligent and Fuzzy Systems, 2021, 46(9):1-13.

[2] Guang L F, Lin Z. Analysis of the Application of Artificial Intelligence in Library Computer Network Security [J]. Value Engineering, 2019, 46(18):31-38.

[3] Hua T L L. Computer network security technology based on artificial intelligence [J]. Journal of intelligent & fuzzy systems: Applications in Engineering and Technology, 2019, 37(5):46-57.

[4] Lina L, Liying W, Wenxin L. Research on Artificial Intelligence Technology for Network Security[J]. Modern Information Technology, 2022, 25(14):18-24.

[5] Xie L, Hang F, Guo W, et al. Network security defence system based on artificial intelligence and big data technology [J]. International journal of high performance systems architecture, 2021, 22(34):10-19.

[6] Veiga A P. Applications of Artificial Intelligence to Network Security [J]. 2022, 44(20):26-41.

[7] Zhang S, Zhu D. Towards artificial intelligence enabled 6G: State of the art, challenges, and opportunities [J]. Computer Networks, 2020, 183(4):10-16.

[8] Wang Z, Fang B. Correction to: Application of combined kernel function artificial intelligence algorithm in mobile communication network security authentication mechanism [J]. The Journal of Supercomputing, 2019, 75(9):5965-5975.

[9] Yong Q L. Application Analysis of Artificial Intelligence in Library Network Security [J]. Journal of Physics: Conference Series, 2021, 1744(3):21-26.

[10] Wenjuan H. Application of Artificial Intelligence Technology in Network Security Defense of Big Data [J]. China Computer & Communication, 2021, 33(10):16-24.

[11] Juan Z. The Application of Artificial Intelligence in Library Network Security [J]. China Computer & Communication, 2019, 42(17):61-72.

[12] Haolin X. The Effective Application of Artificial Intelligence in Computer Network Technology [J]. China Computer & Communication, 2022, 12(12):16-23.