Application of AI Technology in Defense of Big Data Network Security

Yinda Chen¹, *, Xuanrui Gao², Xuechen Wu³

¹College of the Environment & Ecology, Xiamen University, Xiamen, Fujian, 361101
²School of Telecommunications & Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing, Jiangsu, 210023
³School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing, 400065

*Corresponding author: yindachen@xmu.edu.cn

Abstract. Artificial intelligence technology is a new technology based on computer science and technology, combined with Internet technology. It has been widely used in all walks of life. With the development of information technology, the coverage of the Internet is wider, more and more users are involved, and the transmission and sharing of information is more and more convenient. This makes people's request for information security rise to a higher level. The arrival of the big data era has put forward higher requirements for the security protection of the information technology security personnel for the complex data. Artificial intelligence technology can solve this problem well in the application of big data security defense. Artificial intelligence technology can not only enhance the security of network information, but also will change the way people live in the future with the wider application in the network, which will profoundly affect people's life in the information age.

Keywords: artificial intelligence; big data; network security defense.

1. Introduction

With the rapid development of China's economy, people's living standards are also improving [1]. People's lives are showing more diverse needs. Nowadays, the Internet has become an indispensable part of people's lives. The integration of Internet and big data technology makes it easier for people to process massive data [2]. The development of artificial intelligence technology has brought more possibilities to network information security. It can make the application of network security technology more perfect, improve the efficiency of information security, and at the same time, to a certain extent, improve China's relatively bad network information security and protect the environment [3]. Promoting the construction of network information security in China.

2. Analysis of the current situation of China's network security defense against the background of big data Era

With the improvement of information technology in China, China has entered the era of Internet information in the past few years [4]. The Internet has developed more and more widely in recent
years, and its technical support has been more in place. The speed of information transmission has also been improved qualitatively [5]. At present, China's Internet is in the state of integration of acceleration and artificial intelligence. Technicians in the industry have also invested in the great projects to improve the network environment in China, so as to build our original imperfect network information security environment [6].

Network information security is not only related to the vital interests of China's Internet users, but if security measures are not in place, it is likely to cause user privacy leakage, and it will also have different effects on China's economic development, because once the user's information is not properly protected, and privacy leakage incidents occur, people's confidence in the Internet will decline [7]. The development of the Internet will also have a negative impact. In recent years, China's Internet has accelerated the pace of construction. Based on the experience of western developed countries, it has formed the Internet Ecosystem under the background of socialism with Chinese characteristics, and has helped to the development of all walks of life [8]. Making the network information security become an important topic that China urgently needs to study and solve, because "Internet +" can bring a broader platform for the application of AI technology, so that AI can infiltrate into every corner of every household and even society, which will inevitably bring greater challenges to the work of network information security defense [9]. We can often see the news of user information leakage, and even some users' privacy information is not properly protected, resulting in the theft of Internet bank, causing serious economic losses and mental damage to users [10]. Therefore, strengthening the management of artificial intelligence in the field of network information security defense under the background of big data has become an important task of our current network construction.

3. Advantage analysis of AI technology

3.1. AI technology has strong learning ability
The application of any network technology must rely on the network platform. Artificial intelligence, as the representative of advanced technology, needs to improve the support of the network platform in the process of merging with the Internet. After the introduction of AI technology, the network information security defense work is compared with the traditional network information security work. Because of its strong learning ability, artificial intelligence technology has presented a dynamic management mode against the background of big data. The information security defense work will gradually become passive and active from the past passive protection information, and resist external attack mode, and gradually turn to active prediction. With the development of artificial intelligence technology, network security defense work will break through the limitations of traditional information protection work, and make security work more efficient. At the same time, with the powerful learning ability of artificial intelligence, the construction of information security database will also be more rapid, and the technical personnel will have more accurate identification of dangerous information.

3.2. AI technology has strong fuzzy information processing capability
Artificial intelligence will play a vital role in network information security defense in the rapid development in the future. One of the main reasons is its powerful fuzzy information processing ability. This is also a core technology for artificial intelligence to imitate human's thinking and behavior patterns. The powerful fuzzy information processing ability of AI technology can not only enhance the level of network information security defense, but also in the process of defense. Analyzing and processing complex network information and data, greatly improving the defense efficiency, and through fuzzy analysis to determine the source of information and various attributes of analysis value, so that network information security management becomes more convenient.
3.3. **AI technology has strong ability to help network security defense**

China's current network security environment is very bad, and the information of network users cannot get comprehensive security protection, making the construction of network security defense work difficult to advance rapidly. Network security defense is a systematic project with heavy task and long cycle, and has high requirements for collaboration between departments and personnel involved in network construction. The distribution of population is large and the network coverage is large. In order to achieve better results in network information security defense, it is necessary for the relevant departments to coordinate. With the involvement of artificial intelligence technology, the network information security department can more effectively coordinate various departments and personnel, improve the network information security system, and further enhance the effectiveness of security.

3.4. **The computational cost of AI technology is relatively low**

Artificial intelligence is a technology based on the powerful computing power of a computer. It realizes a more powerful function by simulating human thinking or behavior. It possesses the powerful and ultra high computing power that human beings do not have, and can achieve hundreds of times of computing power in human beings per unit time. If these operations are carried out by traditional computer network systems. It is bound to seriously slow down the calculation speed. With AI technology, the algorithm will be optimized accordingly, the speed will be further improved, and the computation cost will be greatly reduced. In addition, using advanced Internet algorithm, AI can also improve the efficiency of network information processing, and make the network security defense system more perfect by analyzing the network information more efficiently and accurately. And save costs for enterprises.

4. **Application of AI technology in network information security defense**

4.1. **Intelligent firewall technology**

The firewall first appeared as a software for terminal computer virus defense and strangulation. After decades of development, it has formed a software system that exerts influence on network security and ensures more user information security. Nowadays, a perfect firewall system has been able to shield various potential risks and early warning of future security risks. The traditional firewall has been relatively mature. However, because of its lack of support for AI technology, it is impossible to achieve more precise, targeted and efficient defense work. The development of AI firewall technology can solve this problem relatively well. Artificial intelligence firewall technology can better analyze and intercept all kinds of potential threats in the network environment, and prevent malicious attacks from being outlying. Artificial intelligence firewall system can be perfected by learning and updating, simulating human experience. It has better defense effect for some malicious attacks that have occurred.

4.2. **Intrusion detection technology**

The other important function of firewall is to use it to detect hidden dangers in network environment, so as to realize the purpose of eliminating hidden dangers in advance. However, due to its lack of learning ability, the traditional firewall needs to be artificially carried out for database updating such as hidden danger, which makes the workload of technicians very large, and often because of not being timely with new ones. The firewall can not properly cope with some risks. Moreover, the traditional firewall does not possess strong fuzzy information processing capability, making the whole system more insensitive to the intrusion of some risks. With the addition of artificial intelligence technology, the firewall system has the corresponding learning ability and analysis ability, and it will make a quicker response to the invasion of risks. And through the analysis and prediction of high-risk areas, real-time monitoring of the area, to achieve targeted prevention, precision strike.
4.3. Neural network system

Neural network system is a high-level application of artificial intelligence technology. It can realize the comprehensive analysis and identification of information in the security defense system by collecting and monitoring all kinds of information in the network environment. Considerable attention has been paid to network security defense system. Neural network is a large distributed processor composed of many simple processing units. It has the characteristics of information distribution and storage, high fault tolerance and so on. With the development of artificial intelligence technology, neural network system can also realize self-management. Because of the relative independence between neurons, the neural network system will show more prominent advantages in parallel computing. These characteristics of neural networks enable them to play an important role in the defense of network information security, especially in areas such as security identification, classification and processing in defense work. It plays an important role in promoting.

At present, the application of neural network technology has achieved certain results in our network environment, and has played a good role in risk intrusion. For example, DDoS network, computer worm detection, zombie mail detection, software malware installation and other aspects, the neural network system has played a strong role. Some neural network systems can also process graphics. With the development of AI technology, its image processing level has been improved unprecedentedly, and has played an excellent role in resisting external risks. In addition, due to its high fidelity, neural network is also named as the "third generation neural network", which provides more possibilities for the construction of network security environment in China.

Nevertheless, the construction of our neural network system in the network information security is still at a relatively late stage, and there is a certain distance from the western developed countries, coupled with the complex network environment in China, which brings different obstacles to the further development and development of the neural network. However, there is still a long way to go before we can get the perfect construction and use.

4.4. Expert system

As an artificial intelligence system, expert system has developed earlier and is relatively mature today. The expert system mainly consists of knowledge base and inference engine. It is based on the knowledge provided by experts in a certain field, reasoning on it, and making decisions through simulating human thinking and behavior. The expert system can propose solutions similar to experts for problems. It has a relatively high level of expertise in related fields. However, the ability of expert system is largely determined by the amount of knowledge reserves based on the expression constraints of specific rules. With the help of network experts' R&D experience, and by enriching expert knowledge in different fields, the expert system can realize the formulation of self decision making in network information security defense work. It is a feasible development idea for information security protection.

Some early Internet information security intrusion detection systems in China have also tried to use expert systems. With the help of specific detection methods, the expert system can realize the recognition of a part of network attacks by the constraint of the most basic programming conditions, if-then. These early intrusion detection systems are based on specific rules. If we want to make it with the development of network technology and the explosive growth of risk categories, we can still maintain efficient and accurate identification. We need to constantly enrich the identification conditions, which is very bad for the long-term development of network security work of expert system, and will bring more and more trouble to technicians. The expert system's recognition and decision making ability will be greatly improved. For example, the NIDES expert system is a new type of system based on statistical algorithm to identify risks. It embeds corresponding intrusion scene coding inside the system, enabling the system to audit users' behavior by means of statistics with powerful computing power. In order to form different behavior models for different users, and then identify abnormal abnormal behaviors under the unified monitoring system to determine whether the behavior is a risk. It should be noted that it is very necessary to analyze the risk with the normative
behavior model, because the NIDES expert system is based on the statistical model to judge. The accuracy of statistical methods depends on the accuracy of data. The accuracy of data depends on the model framework and conditions that restrict the data. Therefore, when establishing a similar artificial intelligence network information security defense expert system based on statistical methods, we should analyze the scientific nature of the constraints so as to improve the accuracy of the whole system for risk analysis.

4.5. Spam network security defense

Nowadays email has become an indispensable part of people's life. From the development of business work to the verification of personal identity registration, it needs to be realized by email. With the expansion of network scale and the surge of Internet users, the use of email is increasing rapidly. This is a huge platform for some criminals to get access to email. It is possible to injure people's privacy information. Especially in the context of big data, the application of AI technology can play a very good role in the defense of bad emails. For example, it can categorize email from some sources into high-risk categories through big data analysis. By sending these e-mails to the user's mailbox and isolating them, it fundamentally eliminates the possibility that users may click on links, resulting in the leakage of personal privacy information. After analyzing millions of email users, artificial intelligence technology can form email risk reports to help technicians manage the mail. More accurate tracking and elimination of spam can improve our network information security environment.

5. Conclusion

With the continuous development of science and technology in China, network information security and defense technology has also brought great changes with the introduction of artificial intelligence technology. Artificial intelligence technology combines its own advantages and network security defense work, by improving the level of firewall technology, improving the accuracy of intrusion detection technology, and improving the expert system. The level of network information security defense work in China has been raised to a new level.

References

[1] Mei Xin Yue. Research and design of network security management system based on big data [J]. science and technology innovation, 2019 (24): 85-86.

[2] Huang Huamei. Computer network technology [J]. China new communications, 2019,21 (11): 58.

[3] Ding Chen. Practice of big data and artificial intelligence technology in risk management of bank network security -- log security audit analysis business [J]. China informatization, 2019 (05): 66-68.

[4] Wei Ning. Application of big data and artificial intelligence technology in computer network [J]. electronic technology and software engineering, 2019 (08): 12.

[5] Zhou Xin. Application of AI in computer network technology under the background of big data era [J]. information and computer (theoretical version), 2019 (08): 113-114.

[6] Yang Bin. Application of AI technology in big data network security defense [J]. computer products and circulation, 2019 (03): 142.

[7] Guo Yonghe, Liu An, Li Jing, Zhang Yahao, Cheng Jie. Research on network security technology and application based on data driven key technology of network security. 2019 (02): 31-32.

[8] Gao ting. Application of artificial intelligence in computer network technology in the age of big data [J]. electronic technology and software engineering, 2019 (01): 6.

[9] Zhang Chee. Application of AI in the computer in the era of big data [J]. China new communications, 2019, 21 (01): 95.

[10] Yang Changqing. The effective use of AI in computer network technology under the background of big data era [J]. information and computer (theoretical version), 2018 (23): 140-142.