Research on Computer Network Security Analysis Modeling Based on Artificial Intelligence Technology

Baicheng Zhong
Shandong College of Information Technology, Weifang, Shandong 261000, China
18353617033@163.com

ABSTRACT

Computer security technology is essential to people's daily use. The high frequency of hackers and virus intrusion has brought a crisis to the privacy of users. Artificial intelligence technology is gradually progressing, and its application in computer information technology is relatively extensive. Diversified artificial intelligence technology will provide technical support for the supervision and prediction of computer network security. In daily life and production, more and more intelligent products have appeared and occupied an important position. The application of artificial intelligence technology to the computer network security management process can effectively use the more efficient computing power of artificial intelligence technology and its powerful learning and imitation capabilities to further improve the computer system. This paper constructs a model for computer network security analysis, and puts forward suggestions for the future research of computer network security.

CCS CONCEPTS

• Information systems~Information systems applications~Process control systems

KEYWORDS

Artificial intelligence; computer network security; virus invasion

ACM Reference format:

Baicheng Zhong. 2020. Research on Computer Network Security Analysis Modeling Based on Artificial Intelligence Technology. 2020 International Conference on Aviation Safety and Information Technology (ICASIT 2020), October 14--16, 2020, Weihai City, China. ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3434581.3434709

ICASIT 2020, October 14–16, 2020, Weihai City, China

ACM ISBN 978-1-4503-7576-4/20/10…$15.00
https://doi.org/10.1145/3434581.3434709

1 Introduction

Due to the continuous improvement of the scientific level, the related technologies of artificial intelligence have also achieved remarkable results. At present, computer information technology is becoming more and more popular, and artificial intelligence technology has shown more and more positive significance in the process of computer network security management [1]. Nowadays, artificial intelligence technology has become one of the most worthy research topics in the progress of science. Both at home and abroad, it has been given high enough attention and extremely extensive use. In daily life and production work, more and more intelligent products have been produced [2]. What is inconsistent with the rapid development of computers is the research on computer network security. The faster the computer network develops and the more frequent software updates, the worse the computer network security. Hackers will look for vulnerabilities in the software installed on the computer to attack, and then obtain the information saved in the computer [3]. Due to the accelerated advancement of Internet technology, the old model is no longer applicable to the current Internet environment, and the security of the computer space has been threatened [4]. Channels and technologies for invading computer networks have become more advanced, and corporate secrets and personal privacy may be leaked. The research on computer network security management is imminent. With the help of artificial intelligence technology in computer security management, it will be able to give full play to the superior computing level and the excellent learning and imitating characteristics of artificial intelligence technology, effectively improve computer security management, and improve the efficiency and efficiency of computer analysis of data, and security Guarantee [5].

Due to the continuous improvement of scientific level, artificial intelligence technology has made great progress, computer information technology has become more and more popular, and artificial intelligence technology has also shown more and more positive significance in the work of computer information security management [6]. The application of artificial intelligence in the computer information security management stage has become more extensive. Due to the rapid improvement of artificial intelligence technology, it has effectively promoted the continuous development of computer information security management technology [7]. The role of artificial intelligence technology in computer information security management is unprecedented and

has a wide range of applications. Computer security incidents are increasing, and hacker attacks happen from time to time. A new security model must be established to ensure network security and reduce the incidence of accidents indefinitely. The modeling research of computer network security analysis is becoming more and more important. Only by improving the security of computer network can people's privacy not be leaked [8]. This article analyzes the computer information security management resources and the reasons that may have a negative effect on security, and creates a computer information security analysis model to provide certain support for the development and research of computer information security management.

2 Computer network security analysis

2.1 Performance of computer information security management

In the early days of computer development, due to the poor continuity and regularity of network data, it increased the difficulty of computer analysis of the authenticity of data. This also makes the intelligence of computer information security management extremely important. The proposal of artificial intelligence technology not only greatly promotes the processing of text, pictures, and videos, but also brings computer networks closer to the way of thinking of the human brain, and makes a significant contribution to the liberation of labor. More and more fields are inseparable from the use of computers. There is no doubt that computers have indeed brought us a lot of convenience and convenience, and many benefits. However, in addition to its benefits, some drawbacks cannot be ignored [9]. With the emergence of more and more cyber crimes, in order to more effectively ensure the security of user information while effectively curbing cyber crimes, keen insight and rapid response capabilities are necessary functions for computers. The intelligent management system is established based on artificial intelligence technology. It mainly has the functions of automatically collecting information and network fault diagnosis, which also greatly guarantees the user's information security.

The improvement of the security level of computer information systems not only ensures that stored data will not be stolen, but also includes the protection of personal privacy and company secrets. The ability of artificial intelligence to efficiently process data has greatly improved the efficiency of human work when using computers, and promoted the overall plan to be completed more efficiently. It is not to be underestimated for the overall development of the entire computer network. The driving effect of [10]. All technological advancements are closely linked to equipment support, and these two technologies support each other. Perform technical inspections on rotating drum equipment to meet work requirements, store work information and ensure information security management. The level of computer technology has promoted the popularization and progress of artificial intelligence technology, and the improvement of artificial intelligence technology is also crucial to the improvement of computer information security management. Artificial intelligence technology has a very positive meaning in computer information analysis, and its importance cannot be replaced. The data resources on the Internet are huge but not continuous. They are irregular and elusive. Therefore, artificial intelligence must be introduced into computer network technology to strengthen supervision and quickly and accurately find target information from network data resources, thereby ensuring information security.

2.2 Causes of negative effects on computer information security management

2.2.1 Computer network software and network vulnerability

Viruses can attack computer networks and hackers can invade other people's computer networks because of loopholes in the computer network or loopholes in the software installed in the computer network [11]. Judging from the transient and dynamic performance of the current network, network management and system assessment work have great pressure in this regard, and the integration of intelligent technology has indeed effectively alleviated this problem. Data information is the object of protection of computer networks, so the entire computer network system is a carrier of information technology. Software and network vulnerabilities refer to defects in hardware, software, or protocol implementation and security design. In this case, some illegal users can log in to the system without authorization and conduct malicious damage. When new computer network systems developed by related companies are put on the market, professional staff should perform system inspections to prevent defects during system installation.

2.2.2 Malicious attacks by hackers and viruses

Hackers use superb computer network technology, constantly attack other people's network, get a lot of information from other people's computers, so as to obtain a lot of profits. Some hackers attack other people's computers not for profiteering, but just for showing off. Some virus software will detect the weakness of computer network and take strong attack against this disadvantage. When the system is invaded, users can't use the information normally and can't operate the system. They can only let the virus invade their private information. Malicious programs, viruses, Trojans and other tools are also commonly used by hackers to maliciously tamper with and steal users' data, and viruses or Trojans can also affect the connectivity of computer networks and affect the normal use of users' computers. The use of artificial intelligence can improve the intelligent degree of firewall and monitoring system, realize the effective isolation of internal network and external network, and more effective identification of viruses, so as to effectively resist network intrusion and make users as far as possible free from virus attacks.

3 Computer information security management modeling based on artificial intelligence technology

After the construction of intelligent firewall, it can identify information data through probability operation, mathematical statistics, memory identification and intelligent decision. Computer

network security is the goal pursued by enterprises and countries all the time. Training professionals to learn information technology, strengthening the analysis and research of network security, adopting mathematical methods and selecting appropriate mathematical models according to the actual situation. The most important factor affecting computer network security is malicious attacks from hackers and viruses, and people cannot guarantee that they will never be attacked by hackers. Therefore, in order to improve the security of computer network, it is necessary to set the access rights of computers, and the important information in computers must be accessible only by administrators [12]. Improving the system management ability in computer network in time plays an extremely important role in users' feelings of using the Internet.

In order to implement the decision of the decision-making level, it also needs a management level to manage the daily work and an execution and maintenance level to be responsible for executing the safety plan and decision. This forms a hierarchical information security organization directly led by the CIO, as shown in Figure 1.

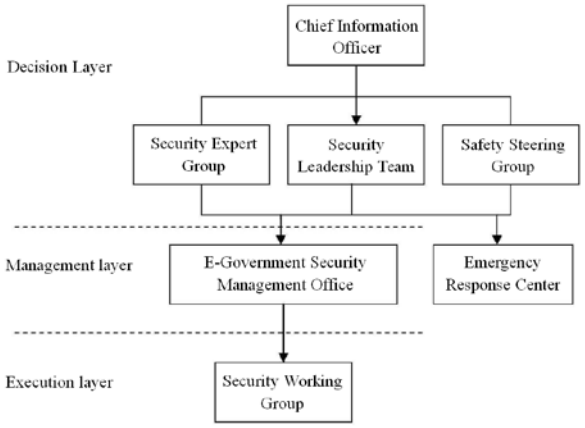

Figure 1 Hierarchical information security management structure

The shared nature of computer network data allows different industries in various fields to share computer network information. For computer crime, the energy-based probability model defines the probability distribution through the energy function:

$$\ln(D_i) = a + \sum_{j=1}^{n} b_j \ln(p_j) + r_i \ln(Y) + u \quad (1)$$

By being a polynomial kernel function:

$$D_i = a + \sum_{j=1}^{n} b_j \ln(p_j) + r_i \ln(Y) + u \quad (2)$$

As the social relationship between nodes increases, the shortest path between nodes and the average distance of the entire network are decreasing (see Figure 2).

Based on the characteristics of big data analysis, artificial intelligence technology will play an important role in the process of analyzing various information data, classifying and managing these data. The significance of smart firewalls can be demonstrated in the prevention of hacker intrusion, effectively reducing malicious virus attacks, and significantly improving the monitoring and management of local area networks, thereby fully avoiding attacks from malicious viruses and Trojan horses. Intrusion detection is the main component of the intelligent firewall, and the second protection method of the firewall to improve the security of the computer network. There are still many potential dangers in computer networks. The malicious intrusion of criminals may crash the computer network and lose important data, causing huge losses to individuals, companies, and the country [13]. The use of artificial intelligence technology in computer information security management can make computer systems more humane and intelligent. At the same time, computers will be able to bring higher-quality services to humans and better meet people's needs. Through artificial intelligence technology, data mining can be performed on network data to more accurately detect memory overflow and other problems, so as to intelligently ensure the smooth operation of the network. Improving computer security management techniques, reducing vulnerabilities and maintaining computers and related equipment regularly can ensure the security performance of the computer system to a certain extent.

Table 1 Analysis results of mobile social network system

Network	Node number	Number of relations	Network density	Central potential
Meet information	198	237	0.831	0.346
Mutual information	181	243	0.657	0.355
Weighted summation	187	246	0.691	0.322

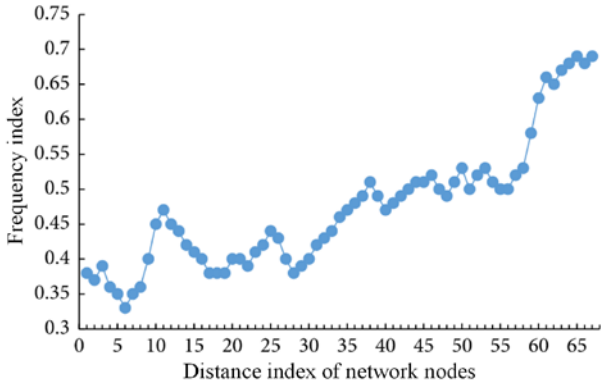

Figure 2 Distance analysis of mobile social network nodes

4 Conclusion

Due to the increasing progress of society and all levels, network technology and information technology are becoming more popular, and people's quality of life and quality have also been improved to a certain extent. In the era of big data, data processing

presents an explosive mode. The joint development of artificial intelligence technology and computer information security management will significantly improve the level of data analysis and effectively deal with the complexity of computer data analysis and security management issues. Currently, fast automatic information retrieval technologies and tools provide important support for the security management of computer network structures, and the subject of evaluation is also devoted to a comprehensive evaluation of the entire information structure on a single host. The improvement and application of artificial intelligence technology is of vital importance in the improvement of network security management. In the context of the continuous advancement of science and technology, the advantages of artificial intelligence in the fields of data analysis, learning efficiency and Internet protection capabilities are increasingly recognized. Only by continuously improving the security performance of computer network can we ensure the privacy of users and reduce the loss of computer users.

REFERENCES

[1] Wang Chenxi, Wang Hao, Wang Quan, et al. Discussion on cybersecurity of medical artificial intelligence products. China Medical Equipment, vol. 33, no. 12, pp. 31-34+39, 2018.

[2] An Keying, Lu Hong. Criminal Law Protection of Cybersecurity in the Artificial Intelligence Era——Based on the Perspective of Cybercrime AIization. Journal of Yunnan Nationalities University (Philosophy and Social Sciences Edition), vol. 181, no. 6, pp. 145 -156, 2018.

[3] Li Xin. Risk Assessment of Wireless Mobile Communication System Based on Artificial Intelligence Algorithm. Modern Electronic Technology, vol. 43, no. 1, pp. 12-15, 2020.

[4] Wang Qianyun. Thoughts on Criminal Regulations for Data Security Crimes in the Background of Artificial Intelligence. Legal Forum, vol. 34, no. 2, pp. 27-36, 2019.

[5] Zhu Guiming, Bin Chenzhong, Gu Tianlong, et al. User preference neural modeling framework based on knowledge graph. Pattern recognition and artificial intelligence, vol. 32, no. 7, pp. 661-668, 2019.

[6] Fu Peng, Lin Zheng, Yuan Fengcheng, et al. Weibo topic tracking model based on convolutional neural network and user information. Pattern recognition and artificial intelligence, vol. 30, no. 1, pp. 73-80, 2017.

[7] Wu Yuanli, Si Guangya, Luo Pi. Application of Artificial Intelligence Technology in Cyberspace Security Defense. Computer Application Research, vol. 32, no. 8, pp. 2241-2244, 2015.

[8] Liao Fangyuan, Chen Jianfeng, Gan Zhiwang. A review of research on defense of critical information infrastructure driven by artificial intelligence. Computer Engineering, vol. 45, no. 7, pp. 181-187,193, 2019.

[9] Qiu Yue, Li Siqi. Research on Security Threat Analysis and Solution Strategies in the Development and Application of Artificial Intelligence. Information Network Security, vol. 213, no. 9, pp. 41-47, 2018.

[10] Wan Qing. Research on route search technology based on adaptive neural network artificial intelligence in ship AIS. Ship Science and Technology, vol. 41, no. 2, pp. 43-45, 2019.

[11] Lin Yilun, Dai Xingyuan, Li Li, et al. The new frontier of artificial intelligence research: generative confrontation networks. Acta Automatica Sinica, vol. 44, no. 5, pp. 775-792, 2018.

[12] Qi Bin, Zou Hongxia, Wang Yu, et al. Research review of adaptive cyber security awareness evaluation system. Journal of Sichuan Armed Forces, vol. 39(011, pp. 140-146, 2018.

[13] Gao Qiqi, Liu Yang. Urban governance in the era of artificial intelligence. Journal of Shanghai Administration Institute, vol. 20, no. 2, pp. 33-42, 2019.