Information Security Detection and Analysis Based on Big Data and Artificial Intelligence Technology

Xiuzhuo Wei, Rui Ma, Lei Mu, and Huinan Zhao(✉)

Changchun Humanities and Sciences College, Jilin, China
278838061@qq.com

Abstract. Under the background of big data and cloud computing, computer network security is facing new security threats, and big data also provides a big data foundation for the application of artificial intelligence technology in computer network security detection system. This paper studies the application of artificial intelligence technology based on big data in computer network security detection system design, in order to provide some intellectual support for the application and promotion of artificial intelligence technology in computer network security detection system design.

Keywords: big data · Artificial intelligence · Network security · detecting system

1 Introduction

With the deep application of computer information technology in various industries, especially the wide application of cloud computing related technologies, such as cloud storage and cloud computing services provided by various cloud computing service providers, the network security of cloud computing has been paid more and more attention [1, 2]. However, from the current situation of the development of network security technology, the related early warning technology, secure access technology and corresponding network monitoring technology are relatively lagging behind, which makes the use of existing network security systems to defend against various intrusions show a high rate of missed detection, so the traditional computer network security detection system can no longer meet the needs of network security detection systems under the background of big data and cloud computing services [3, 4]. In recent years, the emergence of artificial intelligence technology has provided practical solutions to many practical problems in various industries. Because artificial intelligence technology characterized by machine learning and deep learning can mathematize complex practical problems and realize very complex nonlinear fitting ability, it has very good performance in many practical problems.

At present, the vast majority of network equipment users do not have the knowledge and protection awareness of network security, which is particularly obvious among

K. Hemachandran et al. (Eds.): ICAID 2023, AHIS 9, pp. 304–310, 2023.
https://doi.org/10.2991/978-94-6463-222-4_32

ordinary network users, and they have a certain awareness of network security protection among network users in relatively professional fields, but this awareness is relatively weak [5, 6]. The lack of knowledge about network security and the weak awareness of network security provide opportunities for network intruders. According to statistics, most network intrusion incidents are caused by the weak awareness of network users.

Based on this, this paper studies the design of computer network security detection system based on big data and artificial intelligence technology, with a view to using the current artificial intelligence technology to solve the network security problems under the background of cloud computing services to some extent.

2 Design Method

2.1 Overall Setting

In the design process of network information security detection system, we need to pay attention to its system analysis ability and detection ability. In order to ensure the efficient use of network information security detection system and improve the management level of network information security, most enterprises will design the network information security detection system through B/S system architecture [7, 8]. Through the efficient use of the Internet, the network security is detected, the template design is implemented by computer system detection, and the man-machine interaction between the system and users is realized by web, and the data is restored by means of system detection. At the same time, the system operation behavior is recorded by computer logs and then stored in the database of the system. In the network information security detection, the main concept is the monitoring setting, which needs to be completed through the hub. When the designed network information security monitoring system is not equipped with the corresponding hub, the switch can be used instead. For the network information security monitoring system, the purpose of monitoring setting is to monitor the internal relations and functions of different templates in the system, so as to ensure that the network information security monitoring system has reasonable use functions.

2.2 System Protection

When designing the network information security detection system, it is necessary to establish the corresponding firewall. For firewall, it is an important defense means of network information security detection system, which can effectively protect the occurrence of attacks, and use firewall to establish corresponding isolation areas, so as to avoid the security threat of risk behavior to the whole system and effectively protect the security of the whole system. When designing the network information security detection system, you can also set the corresponding hardware firewall [9, 10]. Using the hardware firewall can not only strengthen the information protection ability of the system, but also help the system to centrally manage information, and also enable the computer to record logs according to the protection operation. After the firewall is established, it is necessary to install related equipment with intrusion detection ability to ensure that the system can detect illegal intrusion in real time. At the same time, by installing equipment with intrusion detection ability and combining it with firewall, the security protection ability of the

whole system can be effectively improved. By installing intrusion detection equipment, it can not only help staff find security loopholes in the system in time, effectively prevent important data from leaking, but also help staff to formulate problem solutions in less time.

2.3 Hardware Virtualization and Network Data Acquisition

Virtualization of hardware can not only save a lot of hardware investment, but also provide good data interactivity for the design of network security protection system based on big data and artificial intelligence. Because this function can realize the virtualization of hardware, the cost and flexibility of the system have been greatly improved [11]. At the same time of hardware virtualization, data are collected, stored and transmitted for the system, and these data are transmitted quickly, which provides great convenience for sending them to the artificial intelligence network security detection system for analysis. Moreover, due to the role of principal component analysis and sparse sampling in artificial intelligence technology, many unimportant data are filtered out, which greatly improves the collection efficiency of effective data, and at the same time greatly improves the response speed of identifying network intrusion behavior.

2.4 The Establishment of Anomaly Detection Model

Firstly, through the virtualization function of the network layer, the number information of each node corresponding to the detection system is collected when a network intrusion event occurs. Through the collection of multiple sample parameters, the data information of the sample space of a large number of nodes with network intrusion in the network detection system is accumulated, which can completely express the behavior of network intrusion in the detection system. However, these characteristic space data detection systems which represent the network intrusion behavior are usually too complete [12]. Although using these data to build an artificial intelligence network detection security detection system can also achieve a relatively high recognition rate, this process requires the operation of a large amount of data in the detection system, which may consume a lot of time and greatly reduce the response speed of the system. In order to improve the response speed of the system, it is usually necessary to sparse the high-dimensional features. The detection system selects several representative features to represent the network intrusion behavior, so that the network detection system based on artificial intelligence will have a relatively high response speed. In addition to ensuring high efficiency, the operation of the system also needs to be sensitive to the risks of information security to ensure that the intrusion threat to user data can be detected in real time. Therefore, on the basis of data mining algorithm, this paper establishes an abnormal data detection model to detect and identify abnormal traffic. The detection model designed in this paper is shown in Fig. 1.

Usually, the network security detection system can effectively detect the network intrusion or the virus Trojan intrusion, but it has not carried out the next operation [13, 14]. This link is to take further measures after discovering the network intrusion and the invasion of virus Trojan. In this link, the network security detection system can adopt technologies such as path retrieval and abnormal activity monitoring to search the viruses

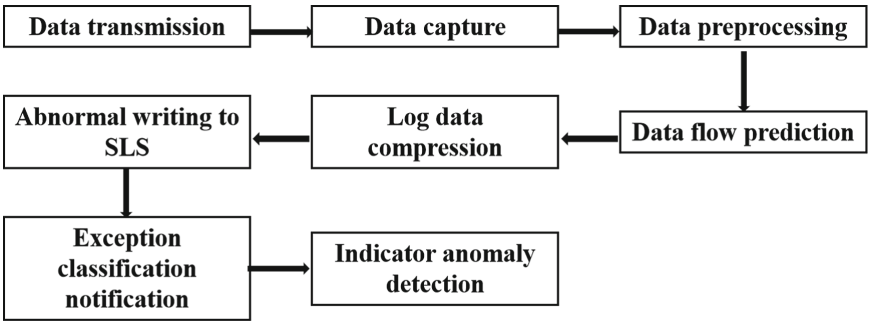

Fig. 1. Network security vulnerability detection model

in the system step by step according to the directory and finally find the location of the virus, and give users a warning based on the situation and harm degree of the virus, and finally further deal with the virus and Trojan to ensure the security of the network system.

3 Experimental Results and Analysis

In order to realize efficient network information security detection and evaluation, this paper designs a new system based on information fusion and the above methods. In this paper, the system designed in this paper is tested experimentally, and the detection and evaluation performance of the system designed in this paper are analyzed. The experimental preparation and results are as follows.

3.1 Experimental Preparation

Set up the hardware framework needed by the system, and select the CPU2400MHZ data acquisition server, the CPU 2400 MHz. 1 TB hard disk anomaly detection server, the ram54kbit.luts6900 FPGA system circuits, and the user training computer with i7700 kCPU.8G memory. The corresponding hardware system combination test is carried out to ensure that the system designed in this paper has a stable hardware foundation. After the hardware connection test, it is determined that the hardware running framework of the system designed in this paper is stable and can provide a solid hardware foundation for the system [15, 16]. After testing the hardware function, this paper uses an independent computer as the attacker, simulates some network attack instructions, and carries out network attacks on user computers with different IP. The attack mode settings are shown in Table 1.

According to the above attack instructions, carry out security attacks. Record the running time and results of the system designed in this paper.

3.2 Experimental Results and Analysis

After the attack computer is connected with the user computer, the data acquisition server, the security detection server and the database server, the attack instruction is sent through

Table 1. Parameter Table of Network Attack Settings

Serial number	Attack type	Number of attacks
1	IP Sweep	50
2	Sad mind rpc	50
3	Remote-to-Root	50
4	DDoS	50

the attack computer [17, 18]. In order to ensure the rigor of the experiment, this paper joins the traditional vulnerability detection and evaluation system, runs the designed system and the traditional detection and evaluation system on the user's computer respectively, and records the corresponding attack detection data. The specific attack detection results are shown in Table 2.

As shown in Table 2, the system designed in this paper has obvious advantages in anomaly detection compared with the traditional system. The system designed in this paper is obviously superior to the traditional system in the performance of risk assessment. With the extension of the attack time, the evaluation values of the two systems for the risk rate have increased steadily, and the traditional system can not accurately evaluate the risk rate, and the evaluation rate is only half of that of the system designed in this paper.

Comprehensive analysis of the above experimental results shows that the system designed in this paper has obvious practical significance in the process of detecting and evaluating users' network information security [19, 20]. The system has high efficiency and stability in detecting network attacks, can improve the detection efficiency of abnormal situations, and the error of detection results is extremely small. At the same time, the system can also ensure the accuracy of computer security state evaluation.

Table 2. Attack detection results of two systems

Serial number	Attack type	System alarm times		Assess risk rate	
		This text	Tradition	This text	Tradition
1	IP Sweep	50	30	0.97	0.90
	Sad mind rpc	48	27	0.92	0.78
2	IP Sweep	50	28	0.90	0.89
	Sad mind rpc	50	16	0.78	0.68
	Remote-to-Root	47	9	0.81	0.69
3	IP Sweep	50	32	0.76	0.96
4	IP Sweep	50	30	0.84	0.54
	DDoS	49	27	0.71	0.41

4 Conclusion

Under the big data and cloud computing, the network security situation has undergone new changes, and the network intrusion behavior is more hidden and diversified. However, big data and artificial intelligence technology also provide data and method basis for the monitoring of network intrusion behavior. In the future, artificial intelligence technology based on big data analysis will definitely play an important role in computer network security detection, and will be gradually popularized and applied.

References

1. Soualmi, A., Alti, A., & Laouamer, L. (2022). An imperceptible watermarking scheme for medical image tamper detection. International Journal of Information Security and Privacy (IJISP), 16.
2. Yang, G. K., Mendoza, B., Kwon, O., & Yoon, J. (2022). Task-specific feature selection and detection algorithms for iot-based networks. Computer and communication, 10(10), 15.
3. Karampidis, K., Rousouliotis, M., Linardos, E., & Kavallieratou, E. (2021). A comprehensive survey of fingerprint presentation attack detection. Journal of Surveillance, Security and Safety, 2(4), 117-161.
4. Han, K., Li, Y., & Xia, B. (2021). A cascade model-aware generative adversarial example detection method. Tsinghua Science and Technology, 26(6), 800-812.
5. Yu, W., Huang, X., Yuan, Q., Yi, M., & Li, X. (2021). Information security field event detection technology based on satt-lstm. Security and Communication Networks, 2021(3), 1-8.
6. Li, R. Q. (2022). Research on key security detection method of cross domain information sharing based on pkg trust gateway. Journal of Interconnection Networks, 22(Supp 01).
7. Araujo, F., Ayoade, G., Al-Naami, K., Yang, G., & Khan, L. (2021). Crook-sourced intrusion detection as a service. Journal of Information Security and Applications, 61(2), 102880.
8. Zhang, Y., Zhang, Z., Huo, L., Xie, B., & Wang, X. (2021). Image saliency detection via two-stream feature fusion and adversarial learning. Journal of Computer-Aided Design & Computer Graphics, 33(3), 376-384.
9. Zhang, J., Pan, L., Han, Q. L., Chen, C., Wen, S., & Xiang, Y. (2022). Deep learning based attack detection for cyber-physical system cybersecurity: a survey. Journal of Automation, 9(3), 15.
10. Millar, S., Mclaughlin, N., JMD Rincon, & Miller, P. (2021). Multi-view deep learning for zero-day android malware detection. Journal of Information Security and Applications, 58(3), 102718.
11. Ning, Z., Wang, T., & Zhang, K. (2022). Dynamic event-triggered security control and fault detection for nonlinear systems with quantization and deception attack. Information Sciences, 594, 43-59.
12. Wang, Y., Peng, C., Liu, D., Wang, N., & Gao, X. (2022). Forgerynir: deep face forgery and detection in near-infrared scenario. IEEE transactions on information forensics and security(17-), 17.
13. Liu, Z., Fang, Y., Huang, C., & Han, J. (2022). Graphxss: an efficient xss payload detection approach based on graph convolutional network. Computers & Security (114-), 114.
14. Peng, H., Cheng, D., & Wang, H. (2021). Phishing website detection method based on cnair framework. International Journal of Information Privacy, Security and Integrity, 5(1), 18.
15. Singh, N. B., Singh, M. M., Sarkar, A., & Mandal, J. K. (2021). A novel wide & deep transfer learning stacked gru framework for network intrusion detection. Journal of information security and applications (Sep.), 61.

16. Bisgin, H., Mohsen, F., Nwobodo, V., & Havens, R. (2021). Enhancing malware detection in android application by incorporating broadcast receivers. International Journal of Information Privacy, Security and Integrity, 5(1), 36.
17. Samantray, O. P., & Tripathy, S. N. (2021). An opcode-based malware detection model using supervised learning algorithms. International Journal of Information Security and Privacy, 15(4).
18. Ring, M., Schlr, D., Wunderlich, S., Landes, D., & Hotho, A. (2021). Malware detection on windows audit logs using lstms. Computers & Security, 109, 102389.
19. Chen, H., Meng, C., & Chen, J. (2021). Ddos attack simulation and machine learning-based detection approach in internet of things experimental environment. International Journal of Information Security and Privacy, 15(3), 1-18.
20. Albahar, M. (2021). A hybrid model for fake news detection: leveraging news content and user comments in fake news. IET Information Security, 15(5).