Design and Application of Network Security Vulnerability Detection System Based on Artificial Intelligence

Fang Qian*, Jue He, Jiawei Zeng

（Ultra High Voltage Transmission Company of CSG Co., Ltd., Guangzhou, Guangdong 510663, China)

cgy67006931@126.com

Abstract. In order to understand the design and application of network security vulnerability detection system, a design and application research of network security vulnerability detection system based on artificial intelligence is proposed. In this paper, firstly, aiming at the high false alarm rate of network security vulnerability detection methods, an automatic network security vulnerability detection method based on artificial intelligence is designed to improve network security. The network flow table items are obtained, and the discrete function of the feature sample classification subset is established. The obtained discrete degree value is taken as the basis of the normal behavior set of network information. On this basis, the network information features are extracted, the network security situation is described, and the network information is evaluated. From the perspective of artificial intelligence, this paper analyzes the law of network vulnerabilities and realizes automatic detection of vulnerabilities. Practice has proved that this detection method can reduce the false alarm rate of network security vulnerabilities and has high feasibility.

Keywords: Artificial intelligence; Network security; Vulnerability detection

1 Introduction

With the continuous improvement of social informatization, network security issues have become increasingly important. Among them, the automatic recognition of network security information plays a crucial role in solving network security problems, but this field has not received sufficient attention. The traditional network security information Automatic identification system often has some problems in actual operation, which may have a negative impact on network security, and even lead to economic losses. When the Automatic identification system of network security information collapses due to various reasons, people are most worried about the risk of data loss. The traditional network security information Automatic identification system has the following three main problems: information leakage, malicious virus implantation and malicious program destruction. These issues may lead to security vulnerabilities in the network, allowing malicious attackers to obtain sensitive information, manipulate the system, or disrupt the normal operation of the system. Artificial intelligence technology

A. Rauf et al. (eds.), *Proceedings of the 3rd International Conference on Management Science and Software Engineering (ICMSSE 2023)*, Atlantis Highlights in Engineering 20,
https://doi.org/10.2991/978-94-6463-262-0_87

is an effective means to ensure network security and protect network security information from malicious attacks. In the context of Big data, due to the continuous maturity of artificial intelligence technology, its application in the field of automatic identification of network security information is increasingly widespread. Therefore, this paper focuses on the use of artificial intelligence technology to improve the network security information Automatic identification system. By integrating artificial intelligence technologies such as neural networks, automatic recognition of network security information is achieved, thereby improving the efficiency of the system and fundamentally improving the accuracy of network security information. This method can help prevent information leakage, detect and block malicious software, and prevent malicious destructive behavior, thereby enhancing network security protection capabilities[1-2].

2 Design of automatic detection system for network security vulnerabilities based on artificial intelligence technology.

The network security vulnerability detection system based on artificial intelligence is a system that utilizes machine learning and data analysis techniques to dynamically discover vulnerabilities and potential threats in network systems. This type of system typically uses a large amount of data to train algorithms, enabling them to identify patterns and behaviors of network attacks, thereby helping to protect the network from potential security threats. Network attack refers to the act of attempting to access, interfere with, destroy, or steal data or resources in the network without authorization. The following are some common types of network attacks:

1. DDoS attack (distributed denial of service attack): Attackers use a large number of computers or devices to send a large number of requests to the target server, resulting in server resource depletion and preventing legitimate users from accessing the service.

2. Malware: includes malicious software such as viruses, trojans, worms, and spyware that can run on user devices and cause damage to systems, data, or user privacy.

3. SQL injection attack: The attacker accesses, modifies or deletes data in the database by inserting malicious SQL code into the input field of the application.

To protect the network from these attacks, the following are some recommended security actions:

1. Regularly update and maintain the system: Ensure that all operating systems, applications, and security software are updated in a timely manner to fix known vulnerabilities.

2. Network firewall: use network firewall to monitor network traffic and prevent potential malicious traffic and attacks.

3. Access control: Implement strict access control policies to restrict users' access to sensitive data and system resources.

Network security is an evolving field, so it is crucial to continuously update and improve security operations to adapt to new threats and vulnerabilities.

The automatic detection system for network security vulnerabilities is based on artificial intelligence technology and mainly involves research and design in three aspects: user interface, information collection and analysis, and vulnerability detection.

Through the research and design of these three aspects, the network security vulnerability automatic detection system can provide comprehensive security protection and ensure the absolute security of computer networks. The user interface enables managers to easily configure and manage the system. The information collection and analysis module can obtain key network status and behavior information, while the vulnerability detection module can automatically detect and identify security vulnerabilities, thereby ensuring network security. Such a system can improve network security, reduce the risk of vulnerabilities being exploited, and protect computer networks from potential threats.

(1) User interface

The normal operation of the network security vulnerability automatic detection system also requires users to configure its related parameters. Only in this way can the network security vulnerability automatic detection system play a more critical role in the application, so the user interface must be set in the network security vulnerability automatic detection system. Users can log on to the automatic detection platform of network security vulnerabilities at any time according to the account password registered in advance, and after passing the detection of the automatic detection platform of network security vulnerabilities, users can make a detailed understanding and analysis of the monitoring data at this stage according to their own rights[3].

(2) Vulnerability detection

Vulnerability detection is the focus of the automatic detection system of network security vulnerabilities, and the most important function of the automatic detection system of network security vulnerabilities is to completely detect the vulnerabilities existing in computer networks. In the computer network, there are various factors that cause loopholes, and these factors are not only closely related, but also difficult to handle. Users can quickly detect all the loopholes in the computer network at this stage in time through the automatic detection system of network security loopholes, and solve them quickly according to the actual situation of the loopholes, so as to ensure the absolute safety of computer network operation[4-5].

3 Automatic detection of network security vulnerabilities

After the network security evaluation and the acquisition of flow table items, it is necessary to automatically detect security vulnerabilities, and send the attack vector code HTTP request to the server by combining artificial intelligence with detection methods, and analyze the vulnerabilities according to the HTTP code. With the support of artificial intelligence theory, this paper explores the vulnerability law and analyzes its vulnerability behavior. With the support of the existing network security vulnerability theory, it combines with the actual problems of network vulnerability security to realize automatic detection of security vulnerabilities. After obtaining the judgment result of network information, the corresponding search method is introduced into the security vulnerability detection. Based on the research goal, the fuzzy mathematics evaluation algorithm is applied to realize the evaluation of security vulnerabilities. The letter O is used to indicate the possibility of security incidents, and P is used to indicate the damage caused by loopholes. The threshold value is [0,1], so the risk and possible consequences of security incidents are evaluated by S, which mainly includes three levels: low security, general security and high security, with corresponding values of 0.3, 0.7 and 1.0 respectively, and between 0.3 and 0.7 or between 0.7 and 1.0 means general security[6].

When using random algorithm to evaluate security vulnerabilities, we still need the support of artificial intelligence related theories, and make full use of heuristic knowledge to solve the network vulnerability problem. If system vulnerability is regarded as an important risk factor of network security, then Formula (1) can be used.

$$p = \sum_{i=1} f(a_i - v_i) \tag{1}$$

Represents the probability of a network vulnerability event. Vulnerability factors are represented by, $\sum_{i=1} f$ network security vulnerability factors by ai, and network security information is represented by vi. Vulnerability security and situations corresponding to different levels:

High hazard. The corresponding weight is 1.2, which indicates that the network has lost control;

Harm, the corresponding weight is 0.8, although it has caused certain consequences, but the control right has not been lost;

Low hazard, corresponding to a weight of 0.4, with serious consequences.

As shown in Table 1, it is the possibility level of vulnerabilities, which is mainly based on different levels when judging vulnerabilities. In order to achieve the goal of automatically detecting security vulnerabilities, we can model the network information interaction[7].

Table 1. Description of vulnerability possibility level

Severity grading	Grade weight	Description and explanation
Frequent occurrence	1.2	Frequent occurrence
May occur	0.8	The whole process happens from time to time.
Sometimes it happens.	0.6	The whole process hardly happens.
Rarely happens	0.4	The whole process occurred several times.
Impossible to happen	0.2	Possibility of occurrence or possibility of occurrence

4 Experimental verification

4.1 Build an experimental environment

From the perspective of artificial intelligence, the network security vulnerabilities are automatically detected. By comparison, the experimental environment is constructed, and the network topology of the system is shown in Figure 1.

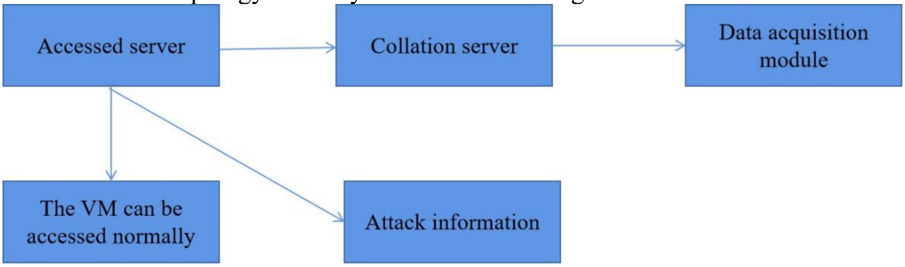

Fig. 1. Experimental Topology Structure

It mainly includes three parts: acquisition module, data processing and calculation module. In order to ensure normal operation, related operations need to be carried out under the action of virtual machine. The server network IP is studied and planned, which is connected with SSH without password, and all components are connected under the action of switches[8].

4.2 Experimental Steps

A total of 500 lines of experimental data are extracted from the experimental software, and the results show that there are security vulnerabilities in 50 lines of code. The detection of security vulnerabilities by traditional methods and this research design method is compared. First, the vulnerable code is given access to the host and supported by network bandwidth. Then collect the data, use the equipment and related parameters in Table 2 to collect the data packet to get the relevant information of the data packet, sort out the experimental data, use the corresponding method to calculate, and embed the data in the program. After packaging the program, check the experimental results.

4.3 Experimental results

The comparison results between the traditional experimental method and the design method of this study are shown in Table 2, and it can be found that the false alarm rate of the traditional method is as high as 48.0%, which is significantly higher than the 18.0% of the design method of this study. The calculation method of false alarm rate is the percentage of the ratio of the number of undiscovered network security vulnerabilities to the number of incorrect types matching to the total number of security vulnerabilities. The automatic detection system designed with the support of artificial intelligence technology has a high detection rate of network vulnerabilities and a low false alarm rate. It can detect network vulnerabilities in time and effectively by using vulnerability detection through the acquisition of network flow items in the interactive process, which is obviously superior to the traditional detection methods. Through the experimental results, it can be found that using artificial intelligence to detect network security vulnerabilities has certain practical significance and promotion value[9-10].

Table 2. Comparison of experimental results

test method	Number of rows where security vulnerabilities were discovered.	Number of rows not found	The number of rows that failed to count correctly.	False alarm rate
Research and design methods	40	8	2	19
traditional method	28	20	61	48

5 Conclusion

Network security vulnerabilities refer to defects or weaknesses in the design, implementation, and use of information technology products, networks, and information systems. These defects or weaknesses may be used by malicious individuals to carry out network attacks, steal information, control or destroy target systems. To address this issue, utilizing artificial intelligence technology to automatically detect security vulnerabilities and grasp their patterns can effectively address network security vulnerabilities, achieve secure operation of the network, and ensure the security of network information. Artificial intelligence technology has the following advantages in detecting network security vulnerabilities:

1. Automated detection: Artificial intelligence technology can detect a large number of information technology products, networks, and information systems through automation, quickly discovering potential security vulnerabilities, and avoiding the tedious and time-consuming manual detection.

2. Learning ability: Artificial intelligence technology can learn and analyze the patterns and patterns of security vulnerabilities through machine learning algorithms, enabling more accurate identification of new security vulnerabilities and timely response and repair measures.

3. Real time monitoring: Artificial intelligence technology can monitor the operational status of networks and information systems in real time, detect abnormal behavior and potential security threats in a timely manner, and thus respond earlier to reduce security risks.

By utilizing artificial intelligence technology to automatically detect security vulnerabilities and taking corresponding security measures in a timely manner, the level of network security can be effectively improved, user privacy and sensitive information can be protected, and losses caused by network attacks on individuals and organizations can be reduced. Therefore, promoting the application of artificial intelligence technology in network security vulnerability detection is of great significance.

References

1. Anne Fül, Nissen, V. , & Heringklee, S. H. . (2023). Knowledge graph-based explainable artificial intelligence for business process analysis. International Journal of Semantic Computing, 17(02), 173-197.
2. Ramlakhan, S. L. , Saatchi, R. , Sabir, L. , Ventour, D. , Shobayo, O. , & Hughes, R. , et al. (2022). Building artificial intelligence and machine learning models: a primer for emergency physicians. Emergency medicine journal: EMJ, 39(5), e1.
3. Zhou, Z. , Yan, C. , & Zhang, C. Y. . (2022). Artificial intelligence biology-biology v3.0. SCIENTIA SINICA Vitae, 52(3), 291-300.
4. Giudicessi, J. R. , Schram, M. , Bos, J. M. , Galloway, C. D. , & Ackerman, M. J. . (2021). Artificial intelligence-enabled assessment of the heart rate corrected qt interval using a mobile electrocardiogram device. Circulation, 143(13)12.
5. Shin, D. . (2023). Embodying algorithms, enactive artificial intelligence and the extended cognition: you can see as much as you know about algorithm:. Journal of Information Science, 49(1), 18-31.
6. Junejo, A. R. , Li, X. , Madiha, H. , & Mohamed, S. . (2022). Molecular communication networks: drug target scalability based on artificial intelligence prediction techniques (retraction of vol 23, pg 1, 2021). Journal of nanoparticle research: An interdisciplinary forum for nanoscale science and technology (5), 24.
7. Tripathy, S. S. , Poddar, R. , Satapathy, L. , & Mukhopadhyay, K. . (2022). Image processing–based artificial intelligence system for rapid detection of plant diseases. Bioinformatics in Agriculture, 61(9)-624.
8. Shen, C. P. , & Muse, E. D. . (2022). Towards an artificial intelligence-augmented, ecg-enabled physical exam. The Lancet. Digital health, 4(2), e78-e79.
9. Envelope, D. U. A. , B, E. D. , C, L. S. , & D, K. S. . (2022). Artificial intelligence as a factor of public transportations system development. Transportation Research Procedia, 63, 2(4)01-2408.
10. Yogesh K. Dwivedi a b Person Envelope, & Envelope, Y. W. C. . (2022). Guest editorial: artificial intelligence for b2b marketing: challenges and opportunities. Industrial Marketing Management, 1(0)5, 109-113.