Design and Implementation of Computer Network Security Defense System Based on Artificial Intelligence Technology

Xiaoyun Qin

Information Center, Guangxi Medical University, Nanning, Guangxi, 530021, China

xyqin@gxmu.edu.cn

Keywords: Artificial intelligence technology; Computer; Network security defense; System design

Abstract: Currently, China is in a critical period of modernization construction, and information technology is playing an increasingly significant role. To improve the defense capability, automation and intelligence level of computer network security, this article explores the design and implementation path of computer network security defense system with the help of the functions and advantages of artificial intelligence technology. It is found that the computer network security defense system consists of a network infrastructure layer, an intermediate layer, and an application layer. It is recommended to further improve the functions of intrusion detection and alarm, intelligent control processing, expert assisted decision-making, and other related functions with the help of artificial intelligence technology, hoping to provide assistance in enhancing the responsiveness, response, and defense capabilities of computer network security defense systems, effectively reducing the probability of computer network security risks.

1. Introduction

Network security risks have always been an important factor restricting China's information construction, not only reflected in the frequent occurrence of various network security stories, but also in the potential threats to personal privacy security and enterprise information security. It can be seen that strengthening network security risk management is the key to operating computer network systems and leveraging information technology efficiency, and it is also an essential part of China's modernization construction [1]. In recent years, the country has attached great importance to cybersecurity issues and has formulated a series of online behavior guidance manuals and risk management mechanisms from a legal perspective. Although it can resist certain external network security risks, it is difficult to cope with the constantly emerging new network security risks due to outdated risk defense methods. The machine learning, big data analysis, and other functions of artificial intelligence technology can timely identify potential security risks in computer network systems, making it a good way to deal with various security risks.

2. Architecture Design of Computer Network Security Defense System Based on Artificial Intelligence Technology

The computer network security defense system is a security monitoring system composed of a network security firewall and various antivirus software. It has the functions of filtering abnormal data information, protecting the stable operation of computer systems, monitoring the overall running status of computers, and timely detecting and eliminating various viruses. It is necessary to build a computer network security defense system because network viruses can spread freely between networks and computers, attacking system running programs. By utilizing machine learning, big data analysis, decision guidance, and other functions in artificial intelligence technology, an efficient computer network security defense system can be established to enhance its operational flexibility and functional scalability [2]. The system architecture is mainly divided into the following three levels:

  DOI: 10.25236/iwmecs.2024.023

2.1 Network Infrastructure Layer

The so-called network infrastructure level refers to the infrastructure level (hardware devices and software systems) in the entire computer network security defense system. This level is the foundation for the stable operation of computer network security defense systems, providing necessary network connections, data transmission, data processing, and collection services for the system's functionality. By building a solid network infrastructure and flexibly handling various raw data streams during computer system operation, such as data logs, system logs, and alert information feedback from firewalls. In addition, the network infrastructure level is also responsible for tasks such as data format cleaning and unified formatting processing of the entire computer network security defense system, providing reference data for the previous network system operation.

2.2 Network Intermediate Layer

The intermediate layer of the network is the core of the computer network security defense system, responsible for tasks such as data processing, task deployment, and operation supervision. [3] The main functions of the intermediate level in the network include: mechanized learning and simulation training, task reception and deployment, network security risk and threat detection. The intermediate layer of the network receives data information uploaded by the basic layer of the network, generates a "neural network", and deploys tasks to various links of the system to promote the normal operation of the computer network security defense system. In addition, the intermediate layer of the network is also responsible for real-time monitoring of the operation status of the computer network system. Once abnormal behavior or data is detected, security warnings are issued in a timely manner, and complex data information uploaded by the network infrastructure layer is converted into actionable instructions to deploy tasks for various system departments in the network application layer and maintain the security of the computer network environment.

2.3 Network Application Layer

The network application layer, also known as the network skills layer, refers to the user interaction interface in computer network security defense systems. The main technical functions are to provide graphical user interfaces, assist security management personnel in monitoring the real-time operation status of computer networks, check for security risks, generate analysis reports on network systems in a timely manner, and utilize various visualization tools to provide computer network system detection reports and analysis results to system users, such as computer network security status, security risk monitoring checklist, historical network security accident analysis report, etc., providing technical support for creating a stable and secure network environment, as shown in Table 1.

Table 1 Architecture of Computer Network Security Defense System Based on Artificial Intelligence Technology

Layer	module	Function Description
Network infrastructure layer	data collection	collect network traffic data, system logs, and alert information from other network devices
	data preprocessing	clean, format, and prepare the format network infrastructure layer required for data analysis of the collected raw data
	data storage management	provide efficient data storage and management solutions for processing and analyzing large amounts of data
network intermediate layer	AI model training	train machine learning models to identify abnormal behavior and predict potential network threats

	Real-time data analysis	real-time analysis of network data using AI algorithms for threat detection and behavior recognition
	threat detection	run various security algorithms to detect and alert network security threats
	API interface	provide interfaces for system integration and data exchange with other systems
network application layer	Graphic User Interface (GUI)	provide an intuitive interface for monitoring network status, viewing alerts, and generating security reports
	real-time alerts	display real-time network security alerts to enable network administrators to respond quickly
	report generation	generate and display network security reports based on analysis results
	user input processing	support users in developing security policies and response measures
	permission management	manage system user permissions to ensure the security and compliance of operations

3. Implementation of Computer Network Security Defense System Function Based on Artificial Intelligence Technology

3.1 Intrusion Detection and Alarm Function of Defense System

The construction of a computer network security defense system based on artificial intelligence technology is mainly aimed at real-time monitoring of system status and network environment, and preventing various network security risks. Therefore, it is particularly important to improve the intrusion detection and alarm functions of the defense system. By utilizing the system's functional modules, real-time monitoring of the computer system's operational status and user behavior can be achieved, and potential security risks and abnormal actions can be identified based on the pre-entered risk list. By relying on machine learning algorithms to analyze known security risks and abnormal behaviors, such as anomaly detection and classification analysis, the timeliness and accuracy of risk identification in computer network security defense systems can be enhanced.

During the operation of the system intrusion detection and alarm function module, once attack behavior or abnormal data is detected, timely warnings are issued to reduce the adverse effects of potential risks. At the same time, with the aid of artificial intelligence technology, the detection cycle and content are automatically adjusted to ensure that the computer network security defense system can flexibly adapt to complex and changing network environments. It is necessary to pay attention to strengthening the automated learning function of this functional module, and use algorithm models in artificial intelligence technology to improve the accuracy of network security risk detection and the timeliness of early warning. In addition, leveraging the automation and intelligence advantages of artificial intelligence technology, we continuously enhance the risk prevention, risk identification, risk detection, and response capabilities of computer network security defense systems.

3.2 Intelligent Control Processing Function of Defense System

The computer network security defense system built based on artificial intelligence technology should include intelligent control processing function modules to facilitate refined management, timely execution of various security defense strategies, and enhance the operational security and stability of the computer network system. With the help of decision algorithms and real-time big data analysis technology, it can dynamically guide the intermediate layer of the network to adjust

security defense strategies, and maximize the security of computer network systems. Once there is a security risk in the computer network system, this intelligent module can quickly and accurately report environmental information and risk status to the intermediate layer of the network. At this point, the intermediate layer of the network outputs operational instructions to the network application layer based on the risk characteristics, ensuring the security and stability of the computer network environment. This efficient and automated defense processing function can improve the responsiveness, response, and defense capabilities of computer network security defense systems.

3.3 Automatic Tracking and Analysis Function of Defense System

The computer network security defense system built based on artificial intelligence technology should also focus on the precise identification and efficient governance of network security risks, and improve the automatic risk tracking and analysis functions. By utilizing artificial intelligence algorithms and analysis techniques, various complex events in the operation of computer systems can be traced along the path of network risk attacks. In addition, with the data integration function of this module, a computer network security risk database is built to provide data support for personnel to query attacker behavior paths, analyze harmfulness, etc. System users can use the automatic tracking and analysis function in the defense system to timely discover the risk movement path, risk triggering reasons, and risk harmfulness in the computer network environment. Then, with the help of machine learning algorithms, it is possible to predict risks or the next actions of attackers in a reasonable manner, and prepare for network security risk prevention in advance. The computer network security defense system should also integrate data technology, integrate the data information generated during the operation of the network infrastructure layer, intermediate layer, and application layer, and provide data support to improve the risk response and attack response capabilities of the computer network security defense system.

3.4 Defense System Expert Assisted Decision-making Function

The computer network security defense system built based on artificial intelligence technology also needs to leverage the decision-making assistance function of artificial intelligence technology and create an expert assisted decision-making section for the defense system. By utilizing artificial intelligence technology and expert system principles, based on the operating principles of computer network systems, more accurate assessment and analysis solutions can be provided for system users to detect security risks. Embedding a knowledge base in the expert assisted decision-making function module of the defense system should include various network security rules, national network security management regulations, attack modes with different risks, corresponding attack strategies, and analysis of typical network security incidents to enhance the system’s assisted decision-making function. With the aid of natural language processing technology, security analysis and query services can be provided for system users. With the support of data and intelligent technology, various risks can be explained to users in detail, automatically generating attack response measures, risk assessment analysis reports, and computer network system repair suggestions. Relying on continuous learning, knowledge base updates, and other technologies, it is necessary to continuously improve the content of the expert service decision-making module of the defense system, update the security threat list in a timely manner, and provide technical support for the decision-making function of computer network systems.

4. Conclusion

In summary, with the innovative progress of information technology in China, computer network systems have been widely used in social production and life, bringing many convenient advantages while also increasing the probability and harmfulness of network security risks. Based on this, it is necessary to actively explore the construction and functional implementation path of computer network security defense systems under the new situation, and use defense systems to ensure the stable operation of computer network systems. Artificial intelligence technology plays a significant

role in the construction and application of computer network security defense systems. It can not only efficiently handle various basic repetitive tasks, but also achieve round-the-clock detection of network systems, timely risk tracking, and flexible adjustment of security defense strategies. In this regard, relevant technical personnel and units should start from the network infrastructure layer, intermediate layer, and application layer, improve functions such as intrusion detection and alarm, intelligent control processing, and expert assisted decision-making, enhance the responsiveness, response, and prevention capabilities of computer network security defense systems, and maintain the network environment in China.

References

[1] Leng Bin. Design and Implementation of Computer Network Security Defense System Based on Artificial Intelligence Technology [J]. Information recording materials, vol.25, no.11, pp.91-92+95, 2024.

[2] Wang Gang, Peng Qian, Duan Hongjun, etc. Design and Implementation of Computer Network Security Defense System Based on Artificial Intelligence Technology [J]. Heilongjiang Science, vol.15, no.18, pp.70-73, 2024.

[3] Lu Baichuan. Design and Implementation of Computer Network Security Defense System Based on Artificial Intelligence Technology [J]. Information and Computers (Theoretical Edition), vol.36, no.16, pp.115-117+121, 2024.