DOI:10.18686/ahe.v7i31.11500

Computer Network Security Defense System Based on Artificial Intelligence Technology

Hui Zheng

Zhangzhou Vocational Institute of Technology, FujianZhangzhou, 363000

Abstract: With the rapid development of modern technology, the importance of computers is increasingly valued by all sectors of society, widely popularized and applied in various social fields. However, the application effect of traditional computer network security defense systems is not good, not only has potential security threats and vulnerabilities, but also the problem of data leakage is severe, making it difficult to achieve the expected risk resistance effect. In response to this, an innovative computer network security system based on artificial intelligence technology is proposed, and the architecture design of the system is clarified from the general user backend management module, administrator user backend management module, and system security protection module. The system testing results indicate that the system can monitor all network data packets entering and exiting the PC, effectively intercept hacker attacks, and evade network security attack events. It has broad application prospects in the field of computer network security.

Keywords: Computer; Network security; Artificial intelligence technology; Data leakage

1. Overview of Artificial Intelligence Technology

Artificial intelligence technology is a technology that simulates human intelligence and can be divided into computer vision, speech recognition, natural language processing, machine learning, and big data according to functional types. Specifically, computer vision mainly imitates the human visual system to recognize, analyze, and understand images and videos. Through a machine vision method that integrates image processing, feature extraction, target tracking, and recognition, it can convert the information contained in images and videos into usable digital information, providing strong data support for many fields. Speech recognition can transform human language into text information that can be processed by computer programs, playing an indispensable role in smart homes,

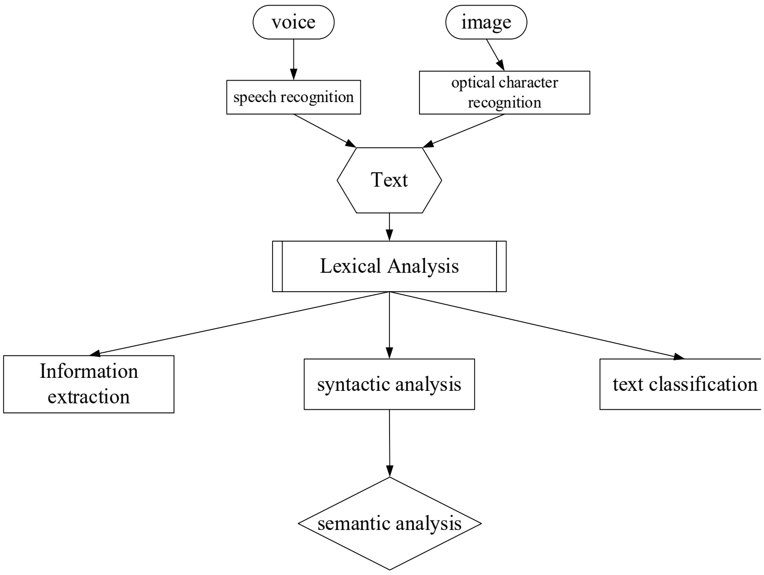

Figure 1 levels of natural language processing smart customer service, and voice assistants. Natural language processing has functions such as text classification, language modeling, semantic analysis, and machine translation, which can transform massive language data into practical information and provide users with excellent services. According to the granularity of the processing object, natural language processing roughly includes four levels: speech analysis, lexical analysis, syntactic analysis, and semantic analysis, as shown in Figure 1. Machine learning includes SVM, decision trees, logistic regression, and neural networks, which can train machines using a large amount of data, helping to improve self-learning ability and optimize knowledge structure. It has become a fundamental way to accelerate the development of computer "intelligence". Big data is a large-scale, complex structure, and high-dimensional dataset that facilitates data storage, processing, analysis, and visualization. It is a key component of artificial intelligence technology. Overall, artificial intelligence technology has become an important branch of modern society and has broad application prospects.

2. Architecture design of computer network security defense system based on artificial intelligence technology

2.1 General user background management module

The computer network security defense system based on artificial intelligence technology advocates b/s architecture. Taking HTML5 as the core, CSS3 as the foundation, and JavaScript as the main tool, it completes the functions of web page structure layout, web page effect rendering, and front-end verification. In terms of the background management module for ordinary users, ordinary users can set a login entry on the home page of the system platform. When logging in for the first time, you need to enter personal information, such as user name, password, telephone number, e-mail, etc., to obtain facial features. After uploading to the background, you can log in only after being approved by the administrator. Ordinary users can also scan the two-dimensional code first, use the system to read the face information, and then compare it with the existing face information in the database. Through, you can access the background management interface of ordinary users to manage personal private data. If the comparison is not successful, it will be sent to the senior administrator of the system through text message or e-mail to achieve the early warning function of illegal intrusion.

2.2 Administrator user background management module

The administrator user background management module mainly completes the management of ordinary users and administrator users, the assignment of permissions, and the management of confidential information. Administrator users can add, delete and assign permissions to them through the super administrator preset in the background of the system. The registration process is to scan the QR code first, and then carry out face recognition. Further, the collected facial features are compared with the facial features stored in the database. If they pass, the next step is to enter the user name and password and enter the administrator user background management interface for corresponding management. If the comparison is not successful, it will be sent to the senior administrator of the system through text message or e-mail to achieve the early warning function of illegal intrusion.

2. 3 System safety protection module

The system security protection module mainly adopts a combination of intelligent firewalls and intrusion detection methods to achieve system security protection. The functional implementation of the system security protection module lies in optimizing the computer network security defense system using artificial intelligence technology. For example, technologies such as natural language processing and machine learning can detect and intercept viruses and trojans, protecting computer network security defense systems. At the same time, an expert system can also be used to build an intrusion detection system based on artificial intelligence technology, to identify and detect illegal intrusion and attack behaviors in computer network security defense systems, prevent, intercept, steal, tamper with, and destroy relevant privacy data in the system, and report it to the system administrator.

3. System testing

3.1 Test method

Build and layout a network environment, test whether the computer network security defense system based on artificial intelligence technology has effectively played the relevant module functions, and whether the system's related performance and design are reasonable. Specifically, penetration testing is conducted by the developers of the privacy and security management system, by integrating artificial intelligence technology into the computer network security defense system to verify the information monitoring function of the system. Penetration testing, as a supplement and verification of network security level protection, can provide strong support for risk assessment and conclusion formation in security assessment. It is an important measure to test the rationality of computer network security defense systems based on artificial intelligence technology. Penetration testing is mainly divided into three categories: first, black box testing. Black box testing, also known as "Zero Knowledge Testing," typically refers to the situation where the infiltrator is completely unaware of the system. The second is white box testing. White box testing, also known as structural testing or logic driven testing, is a test case design method that exports test cases from the control structure of a program. The third is covert testing. Penetration testing refers to the use of professional security personnel to simulate hackers and conduct attack tests on the system from their potential locations, in order to identify hidden security vulnerabilities before a real hacker invades and achieve the goal of protecting system security. In addition, the computers used in the testing environment mainly choose Windows 2000, Pentium TV1.8GHZ, 256M DDR, and the network card uses D_ Link530TX.

3.2 Test results and discussion

Penetration testing can simulate the behavior of attackers, conduct security testing on the target system, discover and exploit potential security vulnerabilities, and effectively verify whether the computer network security defense system based on artificial intelligence technology is effectively monitoring, responding, and recovering information security events. The final results indicate that a computer network security defense system based on artificial intelligence technology can reduce the number of parameter factors in network settings, increase the probability of obtaining hidden virus factor features, filter some data through a series of calculations, thereby reducing the complexity of data classification and quickly detecting viruses.

In summary, the computer network security defense system based on artificial intelligence technology has cleverly redesigned and deployed the server structure by adopting more advanced, scientific, and reasonable technical methods. It can effectively fix security vulnerabilities, avoid network security attacks, and has strong responsiveness. In other words, the performance of computer network security defense systems based on artificial intelligence technology shows significant advantages.

4. Conclusion

As China enters the information age, people's requirements for computer network security defense systems are increasing day by day. The article combines the advantages of artificial intelligence technology and innovatively applies it to the design process of computer network security defense systems. It can not only effectively avoid various forms of network attacks, but also greatly reduce losses caused by data leakage, providing important reference basis for the research of computer network security defense systems based on artificial intelligence technology. The computer network security defense system based on artificial intelligence technology can scientifically process fuzzy information, timely analyze and interpret external uncertain data information, and avoid unknown threats to the computer network. It should be noted that computer network security defense systems based on artificial intelligence technology are still in the initial exploration stage and have not yet been extensively applied and researched in combination with actual situations. This is also the top priority of future research on computer network security defense systems.

References:

[1]Yang P. (2022). Archival Data Rights and System Construction in the Era of Big Data, Archives Communication, (4): 51-57.

[2]Gao De.S, Ji Y. (2021). Research on Personal Information Security Governance Strategies in the Era of Artificial Intelligence, Intelligence Science, (8): 53-59.

[3]Lin W. (2022). Artificial Intelligence Data Security Risks and Countermeasures, Intelligence Journal, (10): 105-111+88.

[4]Cheng J., Li H., Ma K., et al. (2023). Architecture and Key Technologies of Mine Visual Computing System, Coal Science and Technology, (9): 202-218.

[5]Jiang Wan.S, Li B.J. (2020). On the Impact of Artificial Intelligence Technology on Human Social Development, Journal of Xi'an University of Finance and Economics, (1): 23-29.