Application of artificial intelligence technology in network security

Yu Zhou[1], Yijie Liang [2]

[1] Southwest University, Chongqing, 40000, China

[2] Chongqing Yucai Secondary School, Chongqing, 40000, China

Abstract. Artificial intelligence technology has shown significant application advantages in cyberspace security, especially in the fields of the Internet of Things and system security. It enhances threat identification and risk assessment through self-directed learning and pattern recognition. Artificial intelligence technology is currently applied in many fields, such as firewalls, junk advertising, and computer security monitoring, and has played an important technical support role. The future development prospects of artificial intelligence technology are very broad. If integrated with computer network security technology, it can effectively reduce various dangers and improve computer network security. This study summarizes the concept, development, and cross-field application of artificial intelligence and focuses on its application advantages in network security. The paper further puts forward the cyber security strategy based on artificial intelligence technology. It emphasizes that the use of artificial intelligence technology can effectively improve the efficiency of network defense and automatic processing of intrusion. Finally, the conclusion points out the importance of artificial intelligence technology in network security and looks forward to future development.

Keywords: Artificial Intelligence; Network Security; System Safety.

1. Introduction

In today's digital age, the security of cyberspace has become the focus of global attention. With the rapid development of Internet technology, the complexity and concealment of network attacks are increasing, and the traditional network security defense means have been unable to cope with the increasingly complex network threats. In this context, the application of artificial intelligence (AI) technology has become an emerging trend in cyberspace security. AI technology, especially machine learning, and deep learning has revolutionized the field of cybersecurity due to its excellent data processing capabilities and pattern recognition characteristics. The application of AI technology in cyberspace security is mainly reflected in the prediction, identification, and response to cyber-attacks. By analyzing vast amounts of network data, AI can learn and identify various cyber-attack patterns, enabling early warning of potential threats. In addition, AI can dynamically adjust security policies based on real-time data, improving the flexibility and efficiency of network defenses. However, the application of AI in network security also faces challenges, such as algorithm transparency, control of false positive rates, and defense against adversarial attacks. This paper aims to explore the application strategies of artificial intelligence in cyberspace security, analyze the advantages and challenges of AI technology in improving network security defense capabilities, and propose corresponding solutions. Through in-depth research, the research is expected to provide new perspectives and approaches to the field of cyberspace security to deal with increasingly complex cybersecurity threats.

2. Application advantages of artificial intelligence technology in network security

2.1. Concept and development of artificial intelligence technology

Artificial intelligence (AI) technology, since its birth in the middle of the 20th century, has experienced a leap from theoretical exploration to practical application. The core of AI is to simulate the process of human intelligence, including the ability to learn, reason, and adapt. Early on, Turing's

"Turing Test" and McCarthy's concept of "artificial intelligence" at the Dartmouth conference laid the foundation for the development of AI. Subsequently, from simple expert systems to complex neural networks, AI technology has made remarkable progress in mimicking human intelligence. Especially in recent years, with the improvement of computing power and the explosion of data, AI technology has ushered in a new development climax. Intelligent systems such as IBM's "Deep Blue," "Watson," and Google's AlphaGo, etc. have made breakthrough achievements in their respective fields [1].

2.2. Multi-field application of artificial intelligence technology

The application of artificial intelligence technology has penetrated into every corner of society, greatly improving the efficiency and intelligence level of all walks of life [2-3]. In the medical field, AI analyzes medical images through deep learning to assist doctors in disease diagnosis, especially in early cancer recognition, showing higher accuracy than humans. In addition, AI accelerates the discovery of treatment plans and new drugs by analyzing big data in personalized medicine and drug development. The transportation industry is also undergoing an AI-driven transformation. Self-driving cars use complex algorithms to process sensor data for safe driving. Intelligent transportation systems analyze traffic data to optimize route planning and reduce congestion. In the field of education, AI personalized learning platforms customize teaching content according to students' learning progress and style to improve learning efficiency.

AI tools automatically grade assignments, freeing up teacher resources and allowing them to focus more on teaching interactions. The financial industry uses AI for risk management, fraud detection, and automated transactions to improve decision-making efficiency and security. AI analyzes transaction patterns to identify fraud in real-time and protect consumer assets. In the manufacturing industry, AI promotes intelligent manufacturing and improves production efficiency. Robots work precisely on production lines, and AI analytics help optimize production processes and reduce waste. AI applications in the service industry improve the user experience. Intelligent robots provide 24/7 service, understand customer needs through natural language processing technology, and improve service efficiency. AI in agriculture to monitor crop health and optimize resource use; Analyze data and predict pollution trends in environmental protection; Assist in designing more reasonable urban layouts in urban planning. To sum up, the cross-field application of AI not only improves efficiency but also provides a new way to solve complex problems and is an important driving force for the development of modern society.

2.3. Application Advantages of artificial intelligence technology in the Field of network security

Cyber security is important in safeguarding national security, social stability, and economic development. The application of AI technology in this field has shown its unique advantages. AI can automatically identify and respond to security threats through expert systems, artificial neural networks, and other technologies, improving defense efficiency and accuracy. For example, AI can effectively identify abnormal traffic and potential security risks through learning and pattern recognition and block attacks promptly. In addition, AI's ability to self-learn and adapt allows security systems to be constantly updated to cope with ever-changing cyber threats. In handling large amounts of complex data and nonlinear problems, AI's ability is far beyond traditional methods, providing strong technical support for network security.[4]

3. Application of Artificial Intelligence Technology in Computer Network Security

3.1. Firewall

Firewall technology is the most extensively applied technology in network security management. It can protect the computer network by identifying all activities that may damage the completeness and confidentiality of information. A firewall can guarantee information security. Setting a firewall can isolate hostile attacks from hackers to the computers in the internal and external network [5].

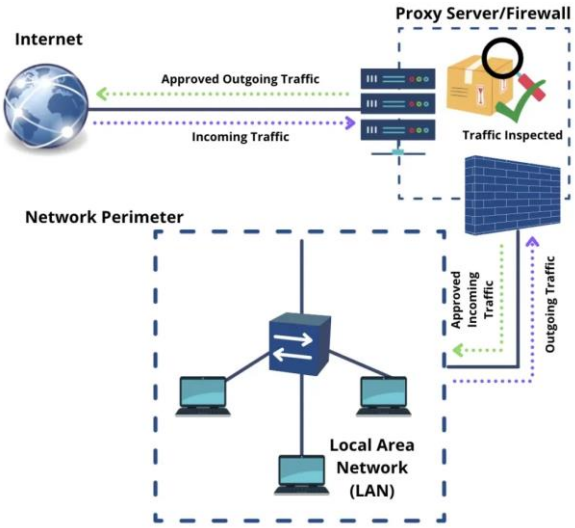

Figure 1. Firewall diagram

3.2. Anti-virus Technology

Online anti-virus technology based on artificial intelligence can quickly discover network virus invasions and alert users to respond promptly to warning messages.

3.3. Establishment of Rule Generation Type Expert System

Expert technology is one of the most extensively applied artificial intelligence technologies in network security management. An *expert system* is an invasion detection system designed based on experts' professional knowledge. Application of expert systems can reduce the workload of invasion detection.

3.4. Application of Artificial Neural Network System

Artificial neural networks are good at identifying invasion modes that carry noise or are hidden. The system is designed based on the long-term simulation of the human brain; hence, it has favorable learning ability and strong adaptive capacity and can efficiently identify invasion behaviors.

3.5. Application of Artificial Immunological Technique

Artificial immunological technique, one of the artificial intelligence technologies, can simulate a series of defenseman- infestations produced after human immunity. In computer network management, it can improve the learning ability of natural defense mechanisms, prevent information from invasion by network viruses, and effectively protect the integrity and confidentiality of information.

4. The Framework of the Trojan Horse Detection Model

Trojan horse virus is a virus that controls a computer through specific programs. Generally, the Trojan horse virus is divided into two programs, i.e., control site and controlled site. Trojan horse virus is prevalent currently. Unlike other viruses, it will neither multiply nor infect other files on purpose. It induces users to download through disguise and then provide the channel of the invaded computer for the invader; as a result, the invader can damage or steal users' documents and even control the host remotely. General viruses have strong infection ability because of self-replication. It multiplies through self-replication and spread by taking advantage of the weakness of computers.

Artificial intelligence-based Trojan horse detection model classified programs using Bayesian classifier according to program behaviors and Trojan horse behavior features library. The model was mainly composed of pro-gram behavior extraction, behavior features library, pro-gram behavior analyzer, Trojan horse processor, and user negotiation and judgment.

The main function of program behavior extraction was to monitor and record suspicious behaviors in the system and send the recorded data to the program behavior analyzer. There were suspicious behaviors such as the automatic operation of documents, hiding documents, and closing the security systems when the Trojan Horse operated. Trojan horse behavior features library included information such as Trojan horse behaviors and its action objects of the

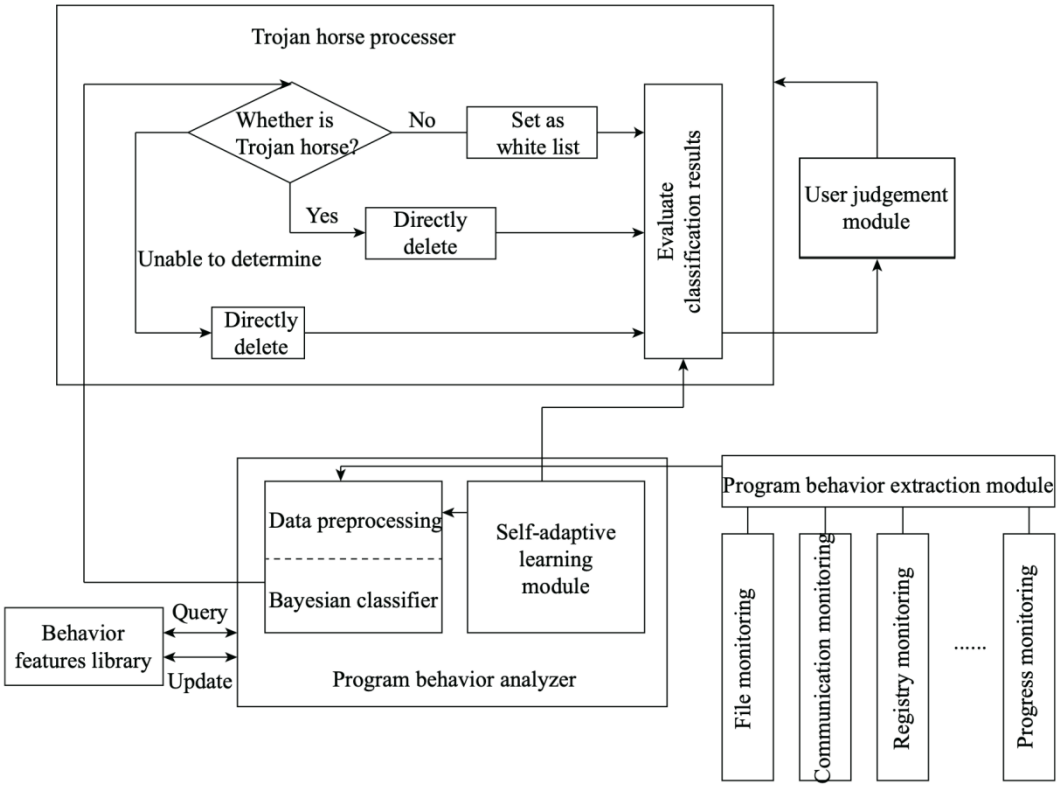

Figure 2. Artificial intelligence-based Trojan horse detection model

5. Module design of artificial intelligence technology in computer network security defense system

5.1. Firewall Module Design

The firewall is widely used as the most common means of defense in the computer network. However, at this stage, many people lack a correct understanding of the network security defense system and do not understand some vulnerabilities and defects, believing that a firewall will eliminate

all network intrusion behaviors. This misunderstanding leads to more and more network security problems appearing.

The application of artificial intelligence technology and big data technology in the design of computer network security defense systems can further improve the defense capability of the system and establish a dual protection mechanism by modifying the firewall. In fact, when implementing this work, it is necessary to establish two firewalls; the first is the commonly used firewall, mainly to set the user's access rights. The second firewall function it restricts the network access of internal users, gives full play to the role of the subsystem, and improves the defense performance through the dual protection mechanism.

5.2. Intrusion Detection Module Design

The computer network security defense system is in the actual operation of the process, mainly in the intrusion after the relevant information is transmitted to the management, with a timely warning. In order to improve the alarm speed and detection accuracy, we need to make full use of artificial intelligence technology, carry out protocol analysis, behavior analysis, matching pattern analysis, etc., and install high-performance sensors. In order to improve the accuracy of intrusion detection alarms, it is necessary to implement efficient network segment monitoring, match gigabit network adapters, analyze the message content in all aspects, carry out feature detection, and use intelligent event analysis and processing technology to conduct in-depth analysis of the original event, and obtain detailed information in a short time. When detecting system intrusion, the intrusion detection alarm module plays a corresponding role in different links. The ultimate goal is to quickly detect and analyze network intrusion events in the first time, reduce the false alarm rate and false alarm rate as much as possible, and improve the detection accuracy. When constructing and designing the computer network security defense system, the intrusion detection and alarm module should make full use of computer hardware and software technology to monitor the network virus intrusion in real-time and make full use of a firewall to supervise the network virus intrusion at the application level. Upgrading the terminal system allows you to analyze network traffic information based on the firewall, improving the security detection effect. Add vulnerability scanning linkage devices, the first warning of vulnerabilities and security problems, and participate in vulnerability repair with other functional modules, effectively improving the level of computer network security defense. In the implementation of hardware virtualization, it is also necessary to improve the efficiency of system data collection, transmission, and storage and improve the defense performance through artificial intelligence networks so that the response speed of network intrusion behavior is improved.

5.3. Application of artificial intelligence technology and big data technology

First, artificial intelligence technology. Compared with traditional operating technologies, artificial intelligence technology has greatly improved the efficiency and quality of computer network security defense systems. In the current era, the network attack channels and network access methods have become more diversified, and the traditional defense mode has been unable to meet the current development requirements. It is necessary to make full use of artificial intelligence technology, in-depth mining, and analysis of all kinds of security issues.

In practice, we can quickly eliminate Trojan horses and viruses in computer networks through the self-learning characteristics of artificial intelligence technology, establish a perfect security defense system, and effectively prevent various network attacks. In addition, the use of artificial intelligence technology can also identify and track the source of trojans and viruses, which can solve the network intrusion problem from the source and provide a reference for subsequent network attacks. Second, big data technology. The computer network security defense system built and designed by advanced technology means can collect and analyze the number of information of each node that has been invaded through the virtualization function of the network layer and master the characterization of network intrusion behavior through the study of multiple sample parameters. Use these data to improve the network defense security system further.

5.4. Design of safety isolation technology

First, meet modern network security requirements. The network environment is easy to be attacked by hackers, so it is necessary to isolate the network environment before the attack. Security isolation technology can avoid affecting the internal network information exchange because it uses physical space isolation, and the access is carried out through independent network lines and devices. However, this method costs higher maintenance costs and construction costs, requiring more lines and equipment.

Second, isolate the data propagation process. When data is being transmitted, you can isolate files to improve network security. In practice, you can copy files through the system to isolate them. However, this mode has a greater impact on the efficiency of use and even requires manual assistance, which takes a long time, but it still has a very strong defense capability.

Finally, safe channel isolation technology. In the established data protocol exchange system, the secure channel can be used to realize the transmission and isolation of data. This needs to be realized based on the exchange protocol and communication hardware, which can effectively protect the data transmission between the internal and external networks and isolate the problem file.

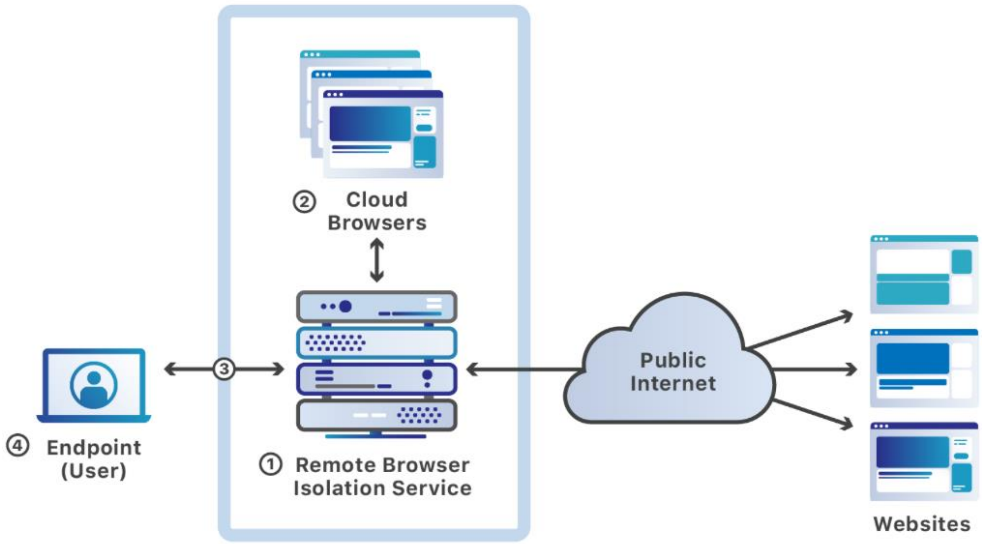

Figure 3. Safety isolation technology

5.5. Transmission encryption system design

Data encryption using network layer protocol is mainly divided into link encryption and end-to-end encryption; for encryption, because the binary data used by the computer needs to be decrypted through transformation, in the encryption, the use of encryption technology to analyze the logical location, and then through the transmission mode of each communication node and data self-construction to play a role in defense and protection. For end-to-end encryption, using software to encrypt data information does not need to encrypt path control information, does not change the state of information data during transmission, and does not affect the security of the overall data. In the context of the development of the new era, in order to achieve high-quality encryption, it is necessary to give full play to the value of big data and artificial intelligence technology, reconstruct the original management mechanism, create a more complex key management mechanism, and ensure the security of data information transmission process.

6. Conclusion

Artificial intelligence technology has shown significant application advantages in cyberspace security, especially in the Internet of Things and system security fields. This study summarizes the

concept, development, and cross-field application of artificial intelligence and focuses on its application advantages in network security. Artificial intelligence technology has been applied in many fields, such as firewalls, junk advertising, and computer security monitoring, and has played an important technical support role. It can be seen that the future development prospects of artificial intelligence technology are very broad; if it is integrated with computer network security technology, it can effectively reduce various dangers and improve computer network security so as to better provide high-quality and convenient services and security for people's production and life.

References

[1] Shatha A , Afraa A ,Daniyal A .Integrating Blockchain with Artificial Intelligence to Secure IoT Networks: Future Trends[J].Sustainability,2022,14(23):16002-16002.

[2] Gregory B ,Yang L ,Rongxing L , et al.Interactions between artificial intelligence and cybersecurity to protect future networks[J].Annals of Telecommunications,2022,77(11-12):727-729.

[3] Fulin L. Application of Artificial Intelligence Technology in Computer Network Security Communication [J]. Journal of Control Science and Engineering,2022

[4] Elias P. Special issue on large-scale neural computing and cybersecurity opportunities using artificial intelligence [J]. Neural Computing and Applications, 2022, 34(18): 15099-15100.

[5] Junxu W, Badarch T. Research on the Application of AI in the Cyberspace Security: A Case Study of Smart Campus Network Security[J]. American Journal of Computer Science and Technology,2022,5(2):