Proceedings of the 6th International Conference on Computing and Data Science
DOI: 10.54254/2755-2721/87/20241443

Design of a cybersecurity defense system based on big data and artificial intelligence

Minbin Yang

Lingshan Vocational and Technical School, Qinzhou City, Guangxi Province, China

124105694@qq.com

Abstract. With the development of big data and artificial intelligence technologies, hacker attack techniques and capabilities have continuously improved, and the methods of network attacks have diversified. Without cybersecurity, there is no national security. Therefore, cybersecurity has become a focal point of attention. To comprehensively enhance the network security defense capabilities of computer operating systems, aligning with the rapid development trends of big data and artificial intelligence technologies, this study focuses on constructing an efficient, stable, and practical cybersecurity defense system. This system deeply integrates advanced technologies of big data analysis and artificial intelligence, thoroughly analyzing the current status of network information security in computer operating systems and closely aligning with the practical needs of design and production. The aim is to provide highly valuable reference solutions for the field of cybersecurity defense.

Keywords: Big Data, Artificial Intelligence Technology, Computer Networks, Security Defense, System Design

1. Introduction

With technological advancements, network information security issues have become a focal point of public concern. Currently, technologies related to network information security, such as early warning technology, security strategy technology, and continuous network monitoring technology, are relatively lagging. This has resulted in traditional computer network defense techniques and systems being unable to effectively resist such intrusion attacks, with a high rate of missed detections. Considering the service environment of big data and artificial intelligence enterprises, there is an urgent need for updated and improved network information security defense systems. The rise of artificial intelligence technology has provided the most feasible and quickest solutions to computational problems across various industries, especially with the development of core artificial intelligence technologies such as machine learning and deep neural networks [1]. Overall, based on this background, this study is dedicated to designing and constructing a computer network security defense system leveraging the characteristics and advantages of big data and artificial intelligence technologies to assist in solving network information security issues. The content of this paper aims to provide a reference for the design of related cybersecurity defense systems, striving to build a complete and practical defense system to comprehensively enhance the level of computer network information security.

DOI: 10.54254/2755-2721/87/20241443

2. Current Status of Computer Network Security in the Big Data Era

2.1. Increasing Sophistication of Hacker Attack Techniques and Capabilities

Entering the new era, China's intelligent mobile cloud technology has also continued to develop, with emerging technologies such as artificial intelligence beginning to permeate various aspects of our lives. This has led to more people independently accessing and learning about these fields and technologies, gradually mastering more network technologies. Among these groups, there are still individuals with weak legal awareness, some even violating laws for profit. They start using illegal software to attack websites with potential security vulnerabilities, exploiting these system loopholes to obtain personal privacy information of internet users, thereby posing a threat to network security.

2.2. Diversification of Network Attack Methods

In today's world, the mobile internet is developing and being applied at an unprecedented speed, and computer network technology is becoming increasingly complex. The number of intelligent mobile terminals on network platforms is also continuously expanding. These technologies are not only applied to common devices and equipment such as smartphones, tablets, and laptops but also to many large and complex electronic digital products. While this has made people's lives more convenient and work easier, it has also laid a solid foundation for network security threats, increasing the difficulty of cybersecurity defense.

3. Requirements for the Design of a Cybersecurity Defense System Based on Big Data and Artificial Intelligence

In the current design of network information security defense systems for computer operating systems, it is crucial to approach from a practical perspective, considering ways to effectively enhance the security defense level. During the design phase, comprehensive planning is essential, understanding the system architecture and actual layout [2]. Specifically, the following measures need to be taken to address these requirements:

Timely Response and Accurate Judgment: When computer network technology faces external illegal intrusions, the constructed security defense system must quickly respond, transmitting information to the intrusion point. This enables clear identification of the type and purpose of the intrusion. However, achieving comprehensive effectiveness in reducing recognition accuracy and false alarm rates is challenging.

Real-time Automatic Response and Digitalization, Intelligence: The system must respond promptly to different security events after the program runs and handle events through automatic shutdown analysis. Digitalization and intelligence significantly improve the efficiency of security handling and make system operation more automated.

Intrusion Tracking and Non-response to Threats: The system should automatically shut down the tracking of large-scale intrusion behaviors in the computer operating system and respond to factors that may threaten the system's safety during the operation of the computer host programs.

4. Design and Implementation of a Cybersecurity Defense System Based on Big Data and Artificial Intelligence

4.1. System Intrusion Detection and Alarm Module

The primary task in designing and producing information security defenses and systems for computer operating systems is to leverage the development of big data and artificial intelligence technologies. The intrusion detection system alarm module has robust functionalities, quickly identifying relevant information and database data after the computer operating system is attacked. Integrating the development of artificial intelligence technology with high-performance detection sensors works synchronously to further enhance the speed of the custom module's red alert. Figure 1 illustrates the specific design of the intrusion detection system alarm module.

DOI: 10.54254/2755-2721/87/20241443

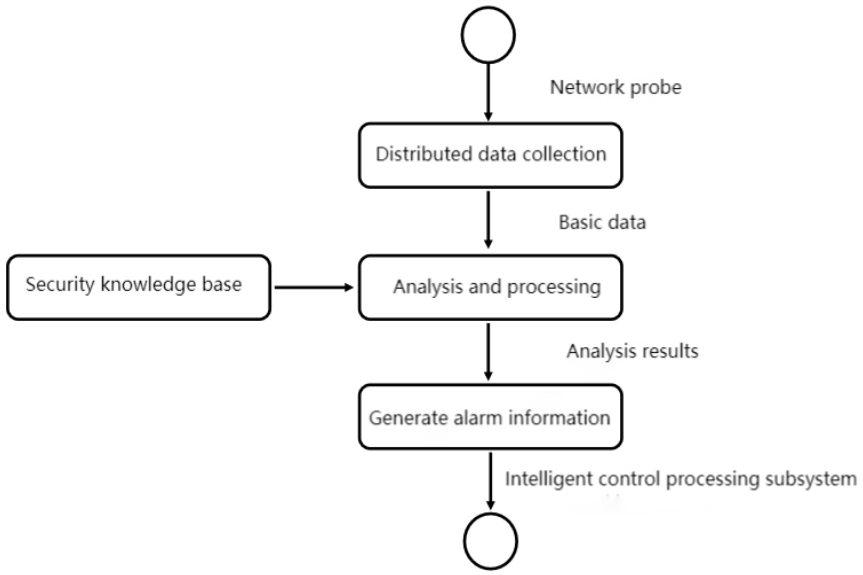

Figure 1. Design and Implementation of the System Intrusion Detection and Alarm Module

While ensuring that alarm detection and calls are conducted as scheduled, the system must also support the efficient and stable operation of eavesdroppers in different network segments. In the detailed data analysis process of detection data, the following high-performance technologies are utilized, such as analyzing user behavior and studying precise protocol content. Additionally, external resources can be collected as much as possible for better software detection. By applying specific event analysis technologies, the time for transmitting information to the intelligent control system's custom module for processing is minimized, achieving unique event analysis security defense. This further enhances the accuracy, stability, and reliability of software detection data.

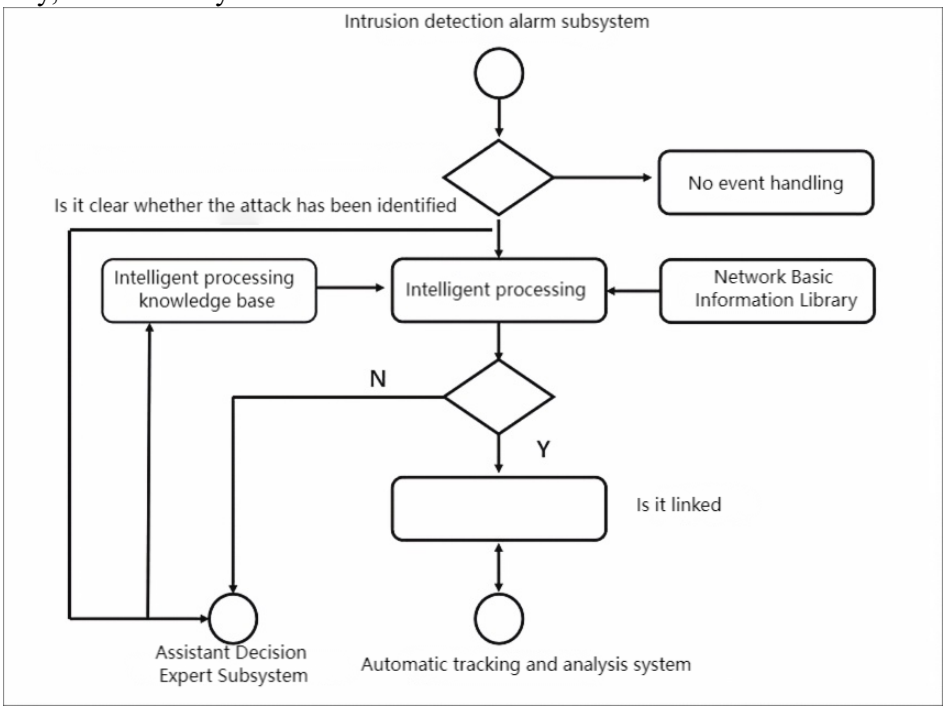

Figure 2. Design and Implementation of the System Intelligent Processing Module

DOI: 10.54254/2755-2721/87/20241443

4.2. System Intelligent Processing Module

The intelligent processing module of the cybersecurity defense system is used to receive security defense-related information collected by the custom alarm module of the intrusion detection system. Its main task is to determine the conditions under which a fixed IP address is under attack and immediately disconnect the network connection associated with that network port to prevent further large-scale intrusions from damaging the computer operating system.

The basic working principle of the intelligent processing module in the cybersecurity defense system for specific situations is shown in Figure 2.

1. Emergency Action: This type of defensive action requires the computer network technology to respond to intrusion situations as quickly as possible to stop the intrusion promptly. The goal of "urgent action" is to take the most direct corrective measures as quickly as possible.

2. Timely Action: When an intrusion occurs, under a timely action control mechanism, the system may not respond to how to handle the intrusion, which could extend for days. The goal of avoiding wasted time must be accomplished through a custom intelligent control system.

3. Local Long-term Action: This type of action is relatively less severe compared to previous situations but aims to be as detailed as possible, allowing security defense personnel to analyze and organize the information.

4. Global Long-term Action: Compared to previous forms, global long-term actions involve the entire computer operating system. In long-term global actions, stricter requirements and specific criteria are introduced for the entire perimeter of the network system. In the system, the response system components and the two custom modules for authorized expert decision support and automatic shutdown tracking analysis maintain a close and normal connection regardless of whether the transmission of relevant banking data is supported.

The specialized custom modules that fully provide decision support are usually connected to the analysis system components and, for various reasons, to the data collection system components for system intrusion detection system alarm calls. This ensures efficient and stable transmission of relevant information and data between system components. Moreover, during theoretical and practical processes, system technology comparisons can support the most critical aspects of system defense, facilitating data sharing and recovery work between them, thus reducing losses caused by the operation of the network system.

4.3. System Auxiliary Decision-Making Expert Module

When designing and producing information security defenses and systems in computer operating systems, the development of big data and artificial intelligence technologies should be combined to design an expert-defined system with complete modules that provide reliable decision support. The primary task of this custom module is to automatically generate suggestions and optimal plans in case of specific intrusions and alarms to assist system security-related managers, forming more optimized results for system security. For decision-makers, it provides excellent support and solutions [3]. When designing and producing the expert-defined module for security and decision support in computer operating systems, reference can be made to the specific content in Figure 3. The knowledge graph's security knowledge is an essential part of the custom professional module, fully providing decision support authority and storing all specific safety knowledge content in the retrieval system. The designed defense and system can quickly take all defense response methods when facing intrusions [4]. Additionally, the custom module that fully provides decision support has a robust automatic shutdown learning function, providing more intelligent decisions for the subsequent security defense of the computer operating system during the continuous learning process.

DOI: 10.54254/2755-2721/87/20241443

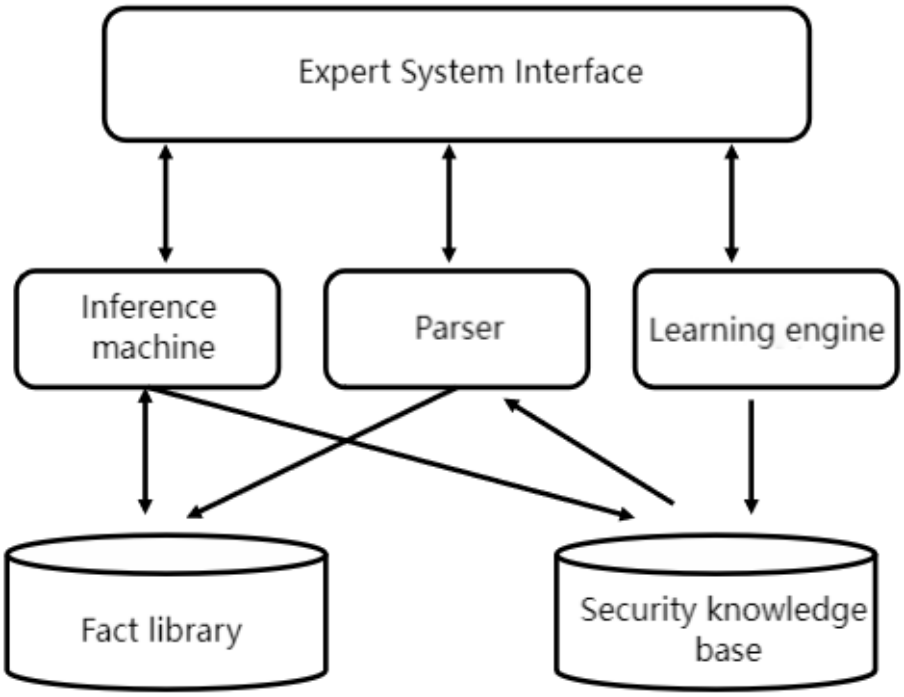

Figure 3. Design and Implementation of the System Auxiliary Decision-Making Expert Module

4.4. System Automatic Tracking Analysis Module

Using automated, in-depth analysis to address crises, the system will automatically shut down and initiate the tracking analysis custom module, taking proactive remedial measures to counteract intrusions when the information source or the entire specific information flow is attacked [5]. This custom module also helps to improve and optimize subsequent cybersecurity defense plans for computer operating systems.

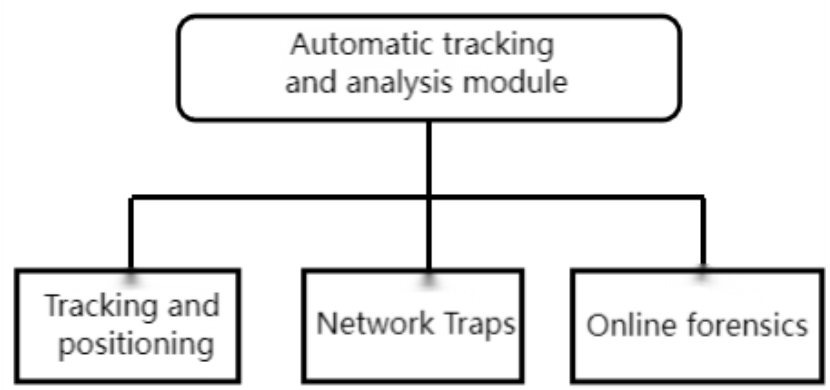

Figure 4. Design and Implementation of the System Automatic Tracking Analysis Module

Based on the basic design and production structure shown in Figure 4, it can be concluded that these sub-custom modules operate independently but within the computer operating system's security protection system. They must be connected to the custom module of the intelligent control system to collaborate effectively.

DOI: 10.54254/2755-2721/87/20241443

5. Conclusion

In summary, to further improve the quality of network information security work in our country's computer operating systems in the new era, we need to invest effort in developing big data and artificial intelligence technologies. The most critical task in constructing network information security defenses and systems is to build custom modules for intrusion detection system alarms. This allows local network-connected computer users to promptly understand and detect intrusion points and specific intrusion details, thus enhancing the security system and improving its efficiency and quality.

Author Biography: Yang Minbin, born in December 1986, female, native of Lingshan, Guangxi; Education: Bachelor's degree; Workplace: Qinzhou Lingshan Vocational and Technical School; Position: Vice Principal; Title: Senior Lecturer; Research direction: Computer technology; Email: 305615514@qq.com.

References

[1] Zhang Xiaoyan. Application of Artificial Intelligence Technology in Cybersecurity Defense [J]. Information System Engineering, 2021(07): 58-60.

[2] Zhang Rong. Research on a Multi-level Cybersecurity Defense Model Based on Artificial Intelligence [J]. Information & Computer (Theory Edition), 2021(13): 180-182.

[3] Liao Yuxiang. Application of Artificial Intelligence Technology in Cybersecurity Defense [J]. Information Technology and Informatization, 2021(06): 182-184.

[4] Wang Yang. Analysis of Information Security Risks and Preventive Measures in the Context of Big Data [J]. Cybersecurity Technology and Applications, 2020(11): 9-11.

[5] Li Fei. Optimization Strategies for Computer Network Security Technology in the Big Data Environment [J]. Computer and Information Technology, 2020, 28(5): 66-68.