Journal of Electronic Research and Application, 2024, Volume 8, Issue 6
http://ojs.bbwpublisher.com/index.php/JERA
ISSN Online: 2208-3510
ISSN Print: 2208-3502

Exploration of Industrial Internet Security Technology and Application from the Perspective of Generative Artificial Intelligence

Dinggao Li, Shengda Liao*, Zhuo Zheng

Guangxi Houpu Digital Technology Co., LTD., Nanning 530000, China

Corresponding author: Shengda Liao, 18077165425@163.com

Abstract: In recent years, artificial intelligence technology has developed rapidly around the world is widely used in various fields, and plays an important role. The integration of industrial Internet security with new technologies such as big models and generative artificial intelligence has become a hot research issue. In this regard, this paper briefly analyzes the industrial Internet security technology and application from the perspective of generative artificial intelligence, hoping to provide some valuable reference and reference for readers.

Keywords: Generative artificial intelligence; Industrial Internet security technology; Application

Online publication: November 29, 2024

1. Introduction

At present, in the world, various countries have gradually carried out a comprehensive safety assessment and supervision of key industries, such as the energy industry, transportation industry, communication industry, etc., and gradually increase the resource investment in the field of safety.

However, with the continuous development and innovation of artificial intelligence technology, cloud computing, and big data technology, in the process of industrial production, more control equipment and production systems are gradually connected to the Internet, and with the advantages of the Internet, the purpose of remote operation control and digital and automated production is realized. At the same time, a large number of important industrial production data are also continuously accumulated in these systems. Although the current network security problem has received extensive attention and concern, and can be through the firewall, virtual private network and other technologies to strengthen the protection of communication links and network boundaries, and improve the level of industrial Internet security. However, the network security risks in different industrial environments are different. Therefore, it is far from enough to protect

communication links and network boundaries, which cannot effectively resist new network attacks such as ransomware and zero-day vulnerabilities, thus causing damage to the security environment of industrial production. In this regard, how to use advanced technologies such as generative artificial intelligence and large models to upgrade industrial Internet security has become a hot research topic in the new era.

2. Application status of industrial Internet security technologies

2.1. Industrial Internet security urgently needs to integrate new technologies

Industrial Internet security is a new technology field, and there are obvious differences from traditional computer systems. The industrial Internet connects hardware and software with different uses, such as industrial automation control equipment, industrial production control systems, information production systems and Internet equipment. In this complex network system, each component plays an important role, and may also become the launching point of network attacks [1].

Traditional network security focuses on the network architecture, and its protection focuses on the network boundary and the device itself. However, compared with industrial Internet security, the scope of industrial Internet security is much larger. In the new era, with the continuous development and evolution of network attack forms and means, the architecture of industrial cyber security needs to be reconstructed. In this process, industrial data will become the center of its transformation. The Industrial Internet gathers a massive amount of security-related data, such as industrial production, security logs, enterprise information and other data. Nowadays, the main research direction is how to use these data and combine new technologies to optimize and upgrade the current security architecture [2]. With the continuous development of new technologies such as artificial intelligence, big data and models, they can effectively complete the transition work of data collection and analysis in the field of industrial Internet. At the same time, for different types and different dimensions of data, new technologies can also dig out the internal relationship according to a large number of judgments and decisions to effectively prevent attacks that are difficult to deal with by traditional security technology means. However, because the field of industrial Internet security has not been deeply integrated with new technologies, the industrial network security architecture is still facing many problems [3].

2.2. Generative artificial intelligence can effectively reduce the technical threshold

Generative artificial intelligence is an innovative computer technology. By comprehensively analyzing uncertain data and natural language, and then using the power of relevant data models, it can finally generate similar or better decisions than humans and can generate corresponding pictures, text, instructions and other content [4].

With the continuous development and wide application of deep learning, natural language processing and support vector machine technology, artificial intelligence technology is developing at a rapid pace. From a broad perspective, the research on network security technology is also through a comprehensive analysis of uncertain attack data or target information, and based on previous processing experience or decision-making to obtain effective security protection means, which is similar to the internal logic of artificial intelligence technology [5]

Previously, many network security professionals have proposed that artificial intelligence and network security can be organically integrated, and the advantages of artificial intelligence technology can be used

to improve the accuracy and timeliness of security technology. For example, the advantages of artificial intelligence technology can be used to quickly dig out security vulnerabilities and detect malicious code. However, these technologies do not adopt large models and do not form a complete and clear "analysis and decision" chain, resulting in a low level of intelligence [6].

However, with the release and wide application of big models, artificial intelligence technology has ushered in new opportunities for development. The big model is a kind of artificial intelligence model with complex structure and large-scale parameters. Compared with the small data model in the initial stage, it has a more complex computational structure and larger scale parameters, can deal with more complex uncertain data, and generates decisions that are more in line with or better than human thinking [7]. At present, big models have been widely used in various sectors of society, and gradually play an important role. For example, it has been widely used in intelligent speech recognition, medical research, cultural and creative design and other fields. In the field of industrial network security, the large model is still in the initial stage of research, and there is no generative artificial intelligence application and technology designed for this field [8].

3. Classification of generative artificial intelligence application technologies for industrial Internet security

According to the functional focus, the existing industrial Internet security generative artificial intelligence applications and technologies can be divided into the following three categories.

3.1. Security expert robots

The application of large models cannot be separated from the support of natural language processing technology. For example, the current well-known artificial intelligence Chatbot ChatGPT has attracted wide attention worldwide, and its success is closely related to the application of natural language processing technology. ChatGPT can "understand" the natural language input by the user through natural language processing technology, and automatically generate complete, fluent and logical responses [9]. In the field of network security, many enterprises are also inspired by this, and they have increased their investment of resources and begun to study the large model of security. While putting forward a technical scheme, that is, the network security books, related network security technology, security events and other security data as the basis of the security model, to build a special intelligent robot for the field of network security [10].

In the past, when dealing with network security incidents, enterprises often rely on pre-formulated network security emergency plans to quickly respond to and deal with various network security threats [11]. However, with the continuous development of new network attack means and methods, the traditional emergency plan has been unable to meet the needs of current enterprise development. The use of security expert robots based on generative artificial intelligence technology can significantly improve response efficiency, improve the ability to deal with network security threats, and better provide protection for enterprise network security. In addition, the interface between security expert robots and network security equipment, such as firewalls, vulnerability scanning, malware detection, etc., can improve the scope of defense, so as to truly realize automatic network security protection [12]. Although security expert robots have important practical significance in improving the security level of industrial Internet, no application branch has been developed specifically for this technology in industrial Internet security, and due to the lack of integration of industrial security knowledge in the existing

security big model, its real potential has not been effectively developed [13].

3.2. Automated penetration testing robots

Penetration testing is an effective detection method in network security monitoring. Through the use of port scanning, vulnerability scanning and full upgrade technology, the staff plays the role of "attacker," with their rich professional knowledge and skills, to carry out a comprehensive penetration test of the target system. The main purpose of this is to identify possible risks and security vulnerabilities in the target system and generate a comprehensive and detailed system detection report. In this way, the target system is guided to carry out security reinforcement work. Penetration testing has a complete set of processes and steps, including multiple links, such as threat modeling analysis, path optimization, report generation, etc. The decision of each link and process will have a certain impact on the subsequent work, and these decisions are generally made by the staff based on their rich work experience and collected information [14]. Therefore, the results of penetration testing are greatly affected by artificial factors, and the professional quality and comprehensive ability of the staff are highly required. They need to strictly abide by relevant laws, regulations and working guidelines in the testing process to ensure that no damage to the target system is caused during the testing activities. The use of automated penetration testing robots can effectively complete the test work. By using artificial intelligence technology to collect and analyze the data of the target system, the system test report can be automatically generated. However, the number of current commercial automated penetration testing robots is relatively small, and for penetration testing in industrial environments, they tend to focus on configuration software, industrial control protocols, and industrial control equipment vulnerabilities. Therefore, there are certain differences between the path of penetration testing and the third-party tools used [15].

3.3. Integration optimization of security products

Malicious code detection, network vulnerability mining, malicious behavior detection and other work can be completed by using generative artificial intelligence. Large models based on natural language processing technology are also very suitable for this kind of work. It can comprehensively analyze data such as device logs and alarm information, extract data that is helpful for staff to find problems in time, and realize automatic classification and summary of data, which can better help staff to find potential risks in time and improve the efficiency of device log audits. Reduce enterprise costs, so as to improve the level of industrial Internet security. At present, there have been a large number of cases that fully prove the role of big models in improving the efficiency and quality of industrial security threat monitoring.

4. Development suggestions

4.1. Industrial safety model branch

In the field of industrial Internet, different production environments have different security concerns. Some production environments pay more attention to the security of industrial control devices, while others pay more attention to the security of internal networks. In addition, different industrial production environments use different equipment, network structures, network protocols and so on. However, security expert robots have certain limitations, which can only analyze and make relevant decisions on the network security level, and cannot carry out comprehensive coverage and data analysis. At the same time, they cannot effectively deal with cyber threats from industrial control protocols and industrial control equipment. Therefore, industrial protocol

data, industrial security incidents, and vulnerability information of industrial control equipment should be integrated and integrated into the big model, to develop a branch specifically for industrial security and develop robots specifically for the industrial Internet field, which is an important direction for future development.

4.2. Customization of industrial scenarios

For some complex and large-scale industrial scenarios, its multi-dimensional data can be used to customize large models and train security robots that can deal with various network security threats. When used in relevant industrial scenarios, it can not only quickly identify various network risks, but also take rapid response measures to improve the level of the industrial Internet field. At the same time, different industrial production environments have different network structures, and the cybersecurity risks they face are also different. For this, we can build penetration testing paths and threat models based on experience. Based on real test data, automated penetration robots are trained to improve the security level in the industrial Internet field.

4.3. Promoting technical standardization

The list of new products not only represents the development and innovation of technology but also is often accompanied by some security risks. At present, many security enterprises, research institutions, universities and so on have conducted in-depth research on generative artificial intelligence in the field of industrial Internet, and invested a lot of resources, I believe that the future will be able to see more innovation and application of new technologies. To ensure the standardized development of new applications, intelligent classification requirements should be formulated. In this way, on the one hand, it helps researchers develop corresponding technologies or products according to the requirements of different levels, and on the other hand, it helps users quickly identify the work scope of different levels of artificial intelligence technology applications.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Dong Y, Zhang Q, Li B, et al., 2024, Research on Industrial Internet Security Technology and Application Based on Generative Artificial Intelligence. Information and Communication Technology and Policy, 50(8): 32–37.

[2] Zhang T, Shi Z, 2024, Research on the Innovation of “Future Manufacturing” Driven by “Digital + Algorithm.” Shanghai Management Science, 46(4): 15–19.

[3] Xiao H, Tang Z, Song S, 2024, Research on Security Technology of Industrial Internet Identity Resolution System. Automation Expo, 41(7): 44–47.

[4] Xu D, Liu X, Fu Q, 2024, Security Management Method of Industrial Internet Data Assets Based on Data Fusion Technology. Information & Computer (Theoretical Edition), 36(12): 43–45.

[5] Hu W, 2024, Digital Technology Empowers New Industrialization. Smart China, 2024(6): 26–27.

[6] Feng Y, He K, Wei Y, 2012, Research and Practice of Industrial Internet Security Protection Based on Blockchain. Cyberspace Security, 15(3): 113–117.

[7] Zhao S, Chen W, Liu Z, 2024, Analysis of Network Security Technologies and Challenges in Industrial Internet Environment. Information Systems Engineering, 2024(6): 133–136.

[8] Xia H, 2024, Research on Design of Industrial Internet Security Platform Based on Blockchain Technology. Network Security and Informatization, 2024(6): 144–145.

[9] Xia J, Cai Y, Li L, 2024, Research on Automated Penetration Testing Technology for Industrial Internet Security. Cyberspace Security, 15(2): 73–77.

[10] Editorial Department of this Journal, 2024, List of Industrial Internet Pilot Demonstration Projects in 2023 Announced by the Ministry of Industry and Information Technology. Group Technology and Production Modernization, 41(1): 51–62.

[11] Chen Z, Zhu Y, Guo M, et al., 2024, Research on the Circulation of Industrial Data Security Based on Internet Technology. Journal of Wind Science and Technology, 2024(8): 49–51.

[12] Zhong Y, Wang H, Zhu Y, et al., 2024, Application of Twin Technology in Industrial Internet Safety Emergency Response. Information Recording Materials, 25(2): 148–150.

[13] Zeng Z, 2024, Empowering Safety and Efficiency with Industrial Internet Technology. China Businessman, 2024(1): 28–29.

[14] Ji K, 2024, Research on Industrial Internet Security Technology. Network Security and Informatization, 2024(1): 44–46.

[15] Sun C, Liu Y, 2023, Application of 5G Technology in Security Risk Management and Control of Refinery Enterprises. Petrochemical Technology & Economy, 39(6): 40–43.