ISSN: 2664-9640

Research on Data Security Strategy of Industrial Internet Intelligent Equipment

Lili Shi[1], Zhengqiu Weng[1] and Qing Wu[2,*]

[1] School of Zhejiang, Wenzhou Polytechnic, Wenzhou, China;

[2]School of Zhejiang, Zhejiang Industry & Trade Vocational College, Wenzhou, 325000, China.

*Corresponding Author

Abstract

Industrial Internet security is related to the national economy, people's livelihood and national development,Smart devices are used as terminals for the collection, transmission and storage of massive data in the Industrial Internet.With the increase of the amount of data, the data security of industrial Internet smart devices is related to the industrial development of the entire country.This paper starts from the current situation of data security of industrial Internet smart devices, analyzes the existing problems, and proposes technologies and development strategies for data security of industrial Internet smart devices.

Keywords

Industrial Internet,Data Security, Smart Device.

1. Introduction

At present, a new round of information technology revolution is taking place around the world, and a new generation of information technology represented by big data, artificial intelligence, Internet +, 5G technology, cloud technology and Internet of Things is booming, which greatly promotes industrial development.The new generation of information technology and the Internet platform is deeply integrated with the industry, giving full play to the optimization and integration role of the Internet in the allocation of production factors. [1]The comprehensive connection of people, machines, objects, systems, etc., realizes the deep integration of Internet technology and equipment with industry, deepens the innovative application results of the Internet in all aspects of industrial production, changes the traditional industrial model, greatly improves production efficiency, and effectively. It has promoted the quality, efficiency, cost reduction, green and safe development of the industrial economy.[2]

However, in recent years, there have been frequent attacks on key information infrastructure systems such as electricity, transportation, oil, heating, and pharmaceuticals. For example, the Iranian nuclear facility was attacked by the Stuxnet virus, the Ukrainian power plant was attacked by hackers and caused widespread power outages, and "Eternal Blue" "The ransomware virus has caused many car companies around the world to stop production, etc. The security of the industrial Internet has threatened the security of the national economy, people's livelihood and national development.Due to the lack of safety construction of the industrial system itself, many industrial control equipment lacks safety design.Production data faces security threats such as loss, leakage, and tampering. Traditional information security technologies such as confidentiality, integrity, and availability cannot be directly applied. The security assurance of industrial Internet platforms faces new challenges.

ISSN: 2664-9640

This paper will make an in-depth analysis of the current situation and existing problems of data security of industrial Internet smart devices, and then put forward technical ideas and development strategies for industrial Internet smart data security issues.

2. Status Quo of Data Security of Industrial Internet Smart Devices

2.1. Industrial Internet data security policy continues to improve

With the continuous integration of new-generation information technologies such as cloud computing, 5G technology, artificial intelligence, and the Internet of Things, and the manufacturing industry, the cyber security risks in the industrial field are gradually increasing, and industrial Internet security has become a topic of high concern for countries and enterprises.In recent years, China has successively issued a series of policies and guidelines to continuously refine and improve the industrial Internet security policy system from the macro, meso and micro levels.In July 2019, ten departments including the Ministry of Industry and Information Technology jointly issued the "Guiding Opinions on Strengthening Industrial Internet Security Work", which systematically laid out the industrial Internet security work and pointed out the direction for the healthy development of the industry.It is foreseeable that more industrial policies will be introduced in the future to continue to maintain support for industrial Internet security and guide its comprehensive development.

2.2. Industrial Internet data security standards continue to advance

The industrial Internet security standard system is mainly composed of basic common standards, security protection standards, security service standards, and vertical industry standards.Industrial Internet standardization is crucial to the construction of an industrial Internet security system.Industrial Internet In recent years, in view of the cross-industry, cross-professional, and cross-domain characteristics of industrial Internet standards, my country has accelerated the development of relevant standards.[3]Industrial Internet has recently released the "General Requirements for Industrial Internet Security Protection" and "Industrial Internet Platform Security Protection Requirements" and other standards and specifications, and issued the "Guidelines for the Construction of Industrial Internet Comprehensive Standardization System", etc.Industrial Internet has initially formed an industrial Internet security standard system covering equipment security, control security, network security, data security, application security, platform security, and security management.

2.3. Industrial interconnection Near-industrial Internet equipment security The industrial structure has been continuously improved and the scale has continued to expand

Industrial Internet border protection, terminal protection, monitoring and auditing and other three typical security products have increased types, rich functions, and optimized performance.The research and development of new industrial Internet security products based on big data, artificial intelligence and commercial passwords has accelerated, and the security product system has been continuously improved.The scale of the industrial Internet security industry continues to grow. According to data from the Ministry of Industry and Information Technology, the stock scale of my country's industrial Internet security industry has increased from 1.34 billion yuan in 2017 to 2.72 billion yuan in 2019, with a compound annual growth rate of 42.3%.

2.4. Industrial Internet equipment security technical capabilities continue to improve

The industry, academia, research and application circles carry out theoretical research and research on the basic general technology of industrial Internet data security, data security

ISSN: 2664-9640

management technology, data security protection technology, and the security of the whole life cycle of data covering the generation, transmission, storage, processing, use and destruction of data. technical breakthroughs, With the rapid development of data security technologies such as blockchain, multi-party secure computing, federated learning and data sandbox, access authentication, access control, authority management, network isolation, data encryption, data desensitization, data backup and recovery, etc. The main technical means of the representative are becoming more and more mature, and "data is available and invisible" and "data does not move by program" are accelerating from concept to reality.

3. Data Security of Industrial Internet Smart Devices is Problematic

By visiting and investigating the representative industries in Wenzhou, such as electrical, footwear, clothing, automobile and motorcycle parts, pumps and valves and other enterprises in the industrial Internet enterprises, to understand the use of intelligent equipment in industrial Internet enterprises, the existence of loopholes, the protection measures taken, etc. The situation is summarized in the following three aspects.

3.1. Industrial Internet Smart Device Security Issues

The terminals in the Industrial Internet include products, systems, and equipment used in the industrial field. The security of traditional production equipment focuses on physical and functional security.With the integration of a large number of industrial Internet devices into the platform, the security loopholes in the design of traditional devices will be directly exposed to network attacks. [4]Once attacked, the Trojan virus will spread between devices at an exponential rate.In addition, most countries' industrial equipment relies on foreign advanced manufacturers, and there is no independent and controllable core technology, there is a risk of being controlled by foreign countries, and the terminal security of equipment is in a severe situation.

3.2. Industrial Internet Smart Device Access Problems

A large number of industrial IoT devices are connected to the Internet and communicate with cloud servers through certain protocols. The more common protocols are MQTT, AMQP, XMPP, etc.If the communication process is not encrypted, it is easy for attackers to intercept information, tamper with data, or conduct man-in-the-middle attacks and issue forged control instructions, resulting in serious consequences such as equipment damage and system paralysis.

3.3. Industrial Internet Smart Device Data Transmission Problem

Industrial Internet data security mainly includes the security of various data such as important production management data inside the factory, production operation data, and data outside the factory.[4]The business in the industrial field is complex, the volume of industrial data is large, and the data flows and shares both inside and outside the factory, making data protection more difficult.In addition, the extension of services such as secondary development services and personalized customization also brings the risk of leakage of user privacy data.

4. Industrial Internet Equipment Data Security Technology Ideas

4.1. Using artificial intelligence technology for state detection and alarm

Use artificial intelligence technology to carry out equipment safety management such as status detection and alarm, fault diagnosis, remote operation and maintenance, and predictive maintenance;Carry out employee safety management such as identification, safety wear, behavior identification, etc.;Carry out equipment safety management such as abnormal early

ISSN: 2664-9640

warning and accident prediction; carry out environmental safety management such as hazard identification and environmental monitoring.

4.2. Encrypting Industrial Internet Devices Using Cryptography

Use identification and password technology to encrypt and authenticate industrial Internet equipment, and establish a data encryption channel after confirming the identity.At the same time, the lightweight implementation of password is studied to reduce the time consumption of device authentication.[5]For the architecture of the Industrial Internet, through a unified and trusted key security management intermediate service layer, seamless integration with application systems or third-party authentication services is achieved.

4.3. Decentralized storage strategy through blockchain technology

Blockchain technology can use decentralized storage strategy to store device security information in network nodes, and at the same time divide and conquer process management information in an open cloud manner. Combining industrial software and cloud platform, relying on cloud platform to achieve end-to-end direct connection, network node interconnection, and mutual data backup, to avoid malicious tampering of industrial data, thereby effectively controlling product quality. Utilize blockchain encryption technology, consensus algorithm, trusted identity authentication technology, and P2P technology to effectively ensure industrial equipment terminal security, data security and network security.[6]

4.4. Industrial equipment data protection using privacy protection technology

Use privacy protection technology to strengthen the protection of industrial equipment data, realize desensitization and obfuscation of industrial equipment data, prevent malicious attacks and cyber crimes caused by privacy leakage, and ensure the data security of the industrial Internet. In the technical scheme, secure multi-party computing SMC and distributed anonymized data encryption technology can be used to hide sensitive data in the data mining process;Adopt technology that restricts release to selectively release original data, not release or release sensitive data with lower precision, to ensure that the disclosure risk of sensitive data and privacy is within a tolerable range; The differential privacy method is used to quantify and evaluate the level of privacy protection.[7]

4.5. Use industrial equipment sensors to collect a large number of industrial control equipment data

Use industrial equipment sensors to collect a large number of industrial control equipment data. Use the big data platform to build a threat awareness center and intelligent analysis system for industrial equipment. Collect various internal data and logs, collect various external threat intelligence, correlate them, and use big data and artificial intelligence technology to analyze, discover, judge, and mine potential security problems and risks from multiple dimensions to realize industrial System security of the device.[8-9]

5. Industrial Internet Equipment Data Security Development Policy

5.1. Improve regulations and policies in key areas of industrial Internet equipment data security

The state should step up and further improve the legislation related to the data security of industrial Internet equipment, further regulate the development of the industrial Internet security industry, and strengthen the security supervision of enterprises.Although ten ministries and commissions including the Ministry of Industry and Information Technology have jointly issued the "Guiding Opinions on Strengthening Industrial Internet Security", the

ISSN: 2664-9640

data security policies for industrial Internet equipment in key areas are not clear enough. Guiding directions in the construction of safety.

5.2. Broaden the formulation of data security standards and specifications for industrial Internet equipment

The Industrial Internet involves many industries and fields. It is not only necessary to build an overall industrial Internet device data security standard system framework, but also to clearly apply industry security-related standards and specifications in the vertical application of industrial Internet device data. Developed countries such as the United States and Germany have laid out security standards for key industries ahead of time. my country should take full advantage of it, organize and coordinate industry regulatory authorities, research institutions, manufacturing companies, security vendors, etc. to cooperate to study and formulate management and technology related to data security of industrial Internet equipment. , evaluation and other standards and norms, to guide the industry to carry out the construction of the industrial Internet security system. Actively lead or participate in international standardization activities for industrial Internet security and the formulation of working rules, promote standards with independent intellectual property rights to become international standards, and gradually increase my country's influence in the international standardization organization for industrial Internet security.

5.3. Promote the research and development and application of technologies related to data security of industrial Internet equipment

Encourage technological research and innovation by setting up special scientific research funds and establishing key safety laboratories, and fully mobilize the enthusiasm of universities, research institutes, and safety enterprises.Accelerate the promotion of innovation and breakthroughs in key industrial Internet security technologies such as platform security, data security, and identification resolution system security, and make full use of new technologies such as artificial intelligence, blockchain, and big data to enhance the security assurance capabilities of the industrial Internet. Build a national-level industrial Internet equipment data security technical guarantee system, improve my country's industrial Internet data security monitoring capabilities, and speed up the construction of industrial Internet vulnerability libraries, malicious code libraries and other basic security resource libraries; Promote the construction of emergency technology, build an industrial Internet equipment data threat information sharing and emergency emergency cooperation command platform, and effectively support the industrial Internet equipment data security emergency coordination and command work.

5.4. Expand the data security industry of industrial Internet equipment

Encourage enterprises to increase investment in industrial Internet security, and form systematic and targeted industrial Internet security products and solutions. Continue to carry out industrial Internet innovation and development projects and pilot demonstration security projects, accelerate the transformation of technological achievements, and fully apply technological innovation achievements into practice. Encourage colleges and universities, professional institutions and security enterprises to establish a joint training mechanism, accelerate the cultivation of industrial Internet security compound talents, rely on industry alliances, continue to carry out offensive and defensive drills, security practical training, etc., to select and cultivate industrial Internet security practical talents.

ISSN: 2664-9640

6. Conclusion

At present, the Industrial Internet has become a key support for major countries to seize development opportunities and speed up their strategic layout. The national level attaches great importance to the development of the Industrial Internet, and has gradually formed a good interactive situation of strategic guidance, planning guidance, policy support and industrial advancement. The data security of industrial Internet equipment has corresponding industrial characteristics. It is necessary to apply relevant data security solutions for different stages of the data life cycle to deal with industrial Internet data security threats, so as to ensure the security of industrial Internet equipment data. With the continuous updating and application of new information technologies such as 5G technology and artificial intelligence in the industrial Internet, the data security technology of industrial Internet equipment will usher in new challenges. Therefore, it is necessary to actively develop the corresponding data security technology, and at the same time apply the new information technology to the future data security technology of industrial interconnected equipment, improve the security protection capability of the system, and make quick and reasonable targeted defenses against emerging security threats. It can ensure the normal and stable operation of the Industrial Internet.

Acknowledgements

Scientific Research Projects of Wenzhou Polytechnics (No.WZY2020043);
Zhejiang Industry & Trade Vocational College Party Building Research Project (No. 2020dj05).

References

[1] Liu Xiaoman,Li Yi, Wu Hao. Industrial internet security architecture and future development[J]. Secrecy Science and Technology, 2019,102(3): 14-21.

[2] Liu Xiaoman,Discussion on the current situation and situation of industrial Internet data security[J].Secrecy Science and Technology,2021(09):10-14.

[3] Yang Zitao,Wang Zun.Talking about the industrial data security protection suggestions of industrial enterprises[J].The Journal of New Industrialization,2021,11(10):141-143.

[4] Jiang Rongrong,Weng Zhengqiu,Chen Tieming.Development of industrial internet platform and its security challenges[J].Telecommunications Science,2020(3):3-10.

[5] Zhu Lifeng. Discussion on industrial Internet data security solution[J]. Application of Electronic Technique，2022,48(2):1-3.

[6] TIAN W, HAO L, WEI J J, et al. MTES: an intelligent trust evalua-tion scheme in sensor-cloud-enabled industrial internet of things[J].IEEE Transactions on Industrial Informatics,2020(16).

[7] ALI M S, VECCHIO M, PINCHEIRA M. Applications of block-chains in the internet of things: a comprehensive survey[J]. IEEECommunications Surveys & Tutorials, 2019(21).

[8] HUANG J Q, KONG L H, CHEN G H, et al. Towards secure indus-trial IoT: blockchain system with credit-based consensus mechan-ism[J]. IEEE Transactions on Industrial Informatics, 2019(15).

[9] DI PIETRO R, SALLERAS X, SIGNORINI M, et al. A block-chain-based trust system for the internet of things[C]//Proceedingsof 23rd ACM on Symposium on Access Control Models and Tech-nologies (SACMAT). Piscataway: IEEE Press, 2018: 77-83.