ISSN: 1813-4890

Research on Data Security of Industrial Internet

Yuwen Shi
Wenzhou Polytechnic, Wenzhou 325035, China
147074267@QQ.com

Abstract

With the development of information security technology, data information security has become a key factor in the development of industrial Internet. Ensuring data information security is also related to the efficient operation of industrial Internet system. This paper introduces the data characteristics of industrial Internet and the difficulties of data security protection, studies and analyzes various data security technologies, and finally puts forward some suggestions to strengthen the data security of industrial Internet.

Keywords

Industrial Internet; Data Security; Security Technology.

1. Introduction

The new industrial revolution characterized by digitalization, networking and intellectualization is booming. The industrial Internet as a new form of production and application mode of deep integration of the new generation of information and communication technology and advanced manufacturing industry is the key support for the new industrial revolution and the important cornerstone of deepening the "Internet plus first generation manufacturing", which will produce an all-round and deep going Industrial Development in the future. The revolutionary impact has become a new round of major historical opportunity in the world after the consumer Internet.

By the end of 2020, the scale of China's industrial Internet industry has reached 3 trillion yuan, the industrial ecology of multi-party cooperation has been further expanded, the number of members of the industrial Internet industry alliance has reached 1700, and the industrial cooperation in related technologies, standards, R & D and applications has been continuously strengthened, which has increasingly played a supporting role in the digital transformation of manufacturing industry and the high-quality development of real economy.

With the development of industrial Internet, data is growing rapidly and has a huge volume. Industrial Internet data has become a key attack target. The global data security threat is serious, and the data security situation of industrial Internet is severe. For example, in March 2019, the Norwegian aluminum group suffered a large-scale cyber attack, resulting in the failure of its IT system to work normally, resulting in the interruption of production and the temporary closure of several factories. Finally, the company's share price fell by about 2% and the global aluminum price rose by 1.2%. In April 2020, the military equipment and other confidential documents of SpaceX, Tesla, Boeing and other companies were blackmailed and encrypted; In the same month, EDP, a Portuguese multinational energy company, was blackmailed and its 10TB sensitive data files flowed out. In May 2020, the main line of Venezuela's national grid was attacked, and power outages occurred in 11 state capitals except Caracas, the capital. According to the report on industrial Internet security situation in the first half of 2020 released by China information and Communication Research Institute, 13.56 million malicious network attacks were found in the first half of the year, involving 2039 enterprises.

ISSN: 1813-4890

Industrial Internet data is the "blood" running through the industrial Internet. It has become a key element to improve the productivity, competitiveness and innovation of manufacturing industry. It is an important engine to drive the innovation and development of industrial Internet. With the development of industrial Internet, data grows rapidly and has a huge volume. Data security has become the main line of industrial Internet security. Once the data is leaked, tampered and abused, it may affect the production and operation security, the national economy and people's livelihood and even national security. Therefore, ensuring the data and information security of industrial Internet is one of the key factors related to the smooth and rapid development of industrial Internet system.

2. Characteristics of Industrial Internet Data

The data generated in the industrial Internet runs through all links of industrial design, process, production, management and service, including field equipment data, application system data, knowledge base data, user personal data, enterprise data, etc. Data in the industrial Internet is quite different from that in the Internet. In the industrial Internet, the data acquisition link is completed by intelligent devices such as robots and intelligent sensors. The interconnection between factories and inside and outside enterprises, information systems and production systems enables the connection and transmission of industrial data, and the storage, technology and processing of data are carried out in the cloud inside and outside factories / enterprises. In a word, industrial Internet data mainly has the following characteristics:

2.1. Diversity

Diversity is the biggest feature of industrial Internet data. Compared with traditional network data, its data types are richer and more diverse, including: structured data stored in relational database in relational table format, such as production control information and operation management data; Structured data stored in time series database in time series format, such as working condition status and cloud infrastructure operation information; Semi structured or unstructured data stored in document, picture and video formats, such as production monitoring data, R & D design data, external interactive data, etc.

2.2. Real Time

Industrial Internet data mainly comes from production, manufacturing and product operation and maintenance. Production lines, equipment and instruments require high-speed operation, and have high real-time requirements in terms of data acquisition frequency, data processing, data analysis, anomaly detection and response.

2.3. Reliability

Industrial Internet data attaches great importance to data quality. The authenticity, integrity and reliability of data should be ensured in the links of data collection, transmission and use, so as to ensure the safety and stability of industrial production and operation.

2.4. Closed Loop

Industrial Internet data includes not only the data of the horizontal process of the whole product life cycle (product R & D, production, release, use, operation and maintenance, update and scrapping), but also the data of the vertical process of intelligent manufacturing (production management layer, process monitoring layer, industrial control layer and field equipment layer) and all data in the processing process. So as to support the dynamic continuous adjustment and Optimization in closed-loop scenarios such as state perception, analysis, feedback and control.

ISSN: 1813-4890

2.5. Cascading

The data of different industrial production links are highly correlated. If the data of a single link is leaked or tampered, it may cause cascading effects.

2.6. High Value

Industrial Internet data puts more emphasis on user value driving and the availability of data itself, so as to improve innovation ability and production and operation efficiency and realize the transformation of new intelligent manufacturing mode.

3. Difficulties in Data Security Protection of Industrial Internet

Industrial Internet data is related to the production and operation of enterprises. Once leaked or tampered with, it may affect the production and operation safety, national economy and people's livelihood and even national security. However, due to technical loopholes, lack of management and imperfect policies and regulations, the security risk of industrial Internet data permeates the whole life cycle of data. On the other hand, various types of industrial enterprises and massive and polymorphic industrial Internet data have brought difficulties and challenges to data security protection. Industrial Internet data has become a major problem in the development of industrial Internet security.

3.1. It is Difficult to Identify and Analyze in the Acquisition Stage

Industrial Internet data is distributed in massive equipment and systems. Not only the data island phenomenon is serious, the data interface specifications of various manufacturers are not unified, but also most manufacturers use their own private protocols, and the industrial protocols are diverse and mostly closed, resulting in difficult data identification and analysis.

3.2. It is Difficult to Trace the Source of Monitoring in the Transmission Stage

The industrial Internet scenario involves the application of cloud computing, big data, artificial intelligence and other technologies, and the flow of industrial Internet data outside the factory is more complex and diverse. It is difficult to effectively capture and trace sensitive data and security threats in large traffic, virtualization and other environments.

3.3. Storage Stage Classification is Difficult

It is very easy to form data aggregation in the storage stage. According to the category and level of data, various means such as dividing regions, setting access rights, encrypted storage and so on need to be adopted. However, industrial Internet data has various forms and complex formats, which makes data classification, hierarchical management and protection difficult.

3.4. It is Difficult to Use Trusted Sharing

The analysis and utilization of industrial Internet data is an important way to develop industrial Internet data as a factor of production. However, it is difficult to determine the rights and responsibilities of data and to enable safety and credibility, which hinder the orderly and safe sharing of data.

4. Key Technologies of Industrial Internet Data Security

To ensure the safety of industrial Internet data and information, we need to comprehensively consider the safety problems of the whole life cycle such as the generation, transmission, storage, processing, use and destruction of industrial data, and adopt corresponding security protection technical means to prevent data leakage and tampering. The main technical means include access authentication, access control, authority management, network isolation, data encryption, data desensitization For data backup and recovery, different data security

ISSN: 1813-4890

protection technologies are adopted according to the different security threats faced at different stages of the data life cycle.

4.1. Data Acquisition Phase

In the data acquisition stage, it is necessary to ensure the safety, reliability and accuracy of data. It mainly includes data intelligent classification and labeling technology, data source trusted verification technology and content security detection technology, data intelligent classification and labeling technology. Data intelligent classification and labeling technology mainly labels structured, unstructured and semi-structured data from the perspectives of content attribute, security attribute and signature attribute. Through labeling, it lays the foundation and initial basis for subsequent data classification and storage, data retrieval, data protection, data traceability and data analysis. Data source trusted verification technology is to solve the effectiveness of data collection from the source, ensure the safety, credibility and reliability of data sources, and eliminate fake objects and fake data. Its main technical means include trusted authentication technology and biological authentication technology. Content security detection technology is to detect the security of the collected data set to ensure that there is no virus or other non security data. It mainly includes rule-based monitoring technology, machine learning based security detection technology and finite state machine security detection technology.

4.2. Data Transmission Phase

There are security risks such as data eavesdropping, stealing and interception in the process of data transmission. To ensure the confidentiality and integrity of data, it is necessary to identify and authenticate the transmission subject and nodes, mainly including encryption technology, secure multi-party computing (MPC) technology, cross domain secure exchange, traffic identification technology, etc. Encryption technology is to transform identifiable plaintext into ciphertext through specific encryption algorithm. At present, the commonly used technical means include attribute based encryption technology, homomorphic encryption technology, proxy re encryption technology and searchable encryption technology. Secure multiparty computing (MPC) technology was proposed by Yao Qizhi in 1982 and academician Yao Qizhi in 1986. It can ensure the privacy of input and the correctness of calculation at the same time. Without a trusted third party, it can ensure that the input information of all members participating in the calculation is not exposed through mathematical theory, and can obtain accurate calculation results at the same time. Cross domain secure exchange is guaranteed by a series of security technologies such as information encryption, trusted computing, identity authentication, signature and summary, content identification and so on.

Cross network and cross domain exchange security of massive data. Traffic identification is to determine the service and data type of each data flow by analyzing or analyzing the collected network data. Its main technical methods include traffic identification method based on network port mapping, traffic identification method based on payload analysis, traffic identification method based on traffic behavior characteristics and traffic identification method based on machine learning.

4.3. Data Storage Phase

In the data storage stage, it mainly solves the secure storage of multi-user and large quantities of heterogeneous data in the cloud environment, which can be realized through distributed storage password, storage isolation, data backup, access control and other technologies. Distributed password storage technology mainly applies password service resource pool technology, key access control technology, password service cluster key dynamic configuration management technology and password service engine pool technology to improve the ability of efficient and concurrent password service and realize the function of key management. Storage isolation technology stores data in isolation according to the security level. Options

ISSN: 1813-4890

include logical isolation and physical isolation, or both; Data backup technology is to ensure data integrity through technical means such as data synchronization, data replication, data mirroring, redundant backup and disaster recovery for special data, such as metadata, highly intensive data or data accessed at high frequency.

4.4. Data Processing Stage

In the data processing stage, on the one hand, technical means such as privacy protection, access control and identity authentication can be adopted to ensure that the data processing platform or system will not be tampered with, collect or disclose relevant important data of enterprises or individuals without authorization. On the other hand, the protection and fallback mechanism of data import and export process is established to ensure timely and effective restoration and recovery of data in case of problems in the process of import and export. In addition, before data processing, test and analyze the knowledge mechanism, digital models, algorithms and tools needed to prevent data forgery, malicious tampering, illegal information hiding and overload operation, so as to ensure the accuracy and security of industrial Internet data processing results. In the process of data processing, access control, identity authentication and other technical means are used, and fuzzy processing and other methods are used to desensitize industrial Internet data without affecting data processing and analysis.

4.5. Data Sharing Phase

It mainly includes blockchain technology, monitoring and audit technology, shared review technology, data desensitization technology, etc. Blockchain technology makes use of the decentralized characteristics to enable multiple distributed computing nodes to participate in and record together, and verify the effectiveness of each other, so as to ensure that the data is not tampered with and traceable; The consensus mechanism of distributed nodes is similar to multiple secret contact points with common beliefs. When a single node is attacked, it can avoid affecting the overall operation of the blockchain system and effectively reduce the risk of centralized data management. Monitoring audit technology is to comprehensively evaluate abnormal events, violations and business changes in data security sharing, and conduct post security inspection. It mainly carries out correlation analysis, digital forensics, event tracing, anomaly monitoring, data connection, etc. according to the security event log, and ensures the safety of data sharing through all-weather real-time monitoring. Sharing review technology is mainly aimed at the data security protection strategies implemented in different states such as paid sharing, free sharing, time-sharing, partition sharing, directional sharing and active distribution of data after the release of data sharing, including the review of compliance, security and sensitive information, so as to meet the data security challenges under different data sharing modes in the future. Data desensitization, also known as data De privacy or data deformation, is a technical mechanism to transform and modify sensitive data under given rules and policies. While exchanging sensitive information, data desensitization also needs to retain the original characteristic conditions or the necessary information required for data processing after desensitization. Only authorized managers or users can access the real value of data through applications and tools under specific circumstances.

4.6. Data Archiving and Destruction Stage

In the stage of data archiving and destruction, it is necessary to archive the important industrial Internet data with very low access frequency, so as to prevent the data from being tampered with and deleted. At the same time, it is necessary to completely destroy the sensitive data to avoid illegal residual information or information leakage caused by restoring the deleted data. It mainly includes metadata deletion technology, cache data deletion technology, recycle bin data deletion technology and disk residual information deletion and writing technology to ensure that the data is completely destroyed without leaving traces and can not be recovered.

ISSN: 1813-4890

5. Suggestions on Strengthening Data Security Protection of Industrial Internet

5.1. Strengthen Data Security Management

It is suggested to formulate and release relevant policies, systems and standards for industrial Internet data security classification and grading, security protection, security exchange and sharing, security evaluation and so on. We will promote the publicity, implementation and pilot application of policies and standards in key industries and regions, and promote the implementation of corporate responsibility. Clarify the requirements for data retention and data disclosure notification, and regularly carry out industrial Internet data security supervision and inspection. Actively organize and carry out benchmarking inspection and third-party evaluation, evaluate the current situation of enterprise data security management, promote enterprises to locate their own problems in combination with business development needs, formulate targeted rectification plans, constantly improve corresponding data security management plans, methods, standards, measures and processes, and gradually establish and improve the industrial Internet data security management system.

5.2. Strengthen Data Security Governance and Protection

Accelerate the establishment of industrial Internet data security governance system, take the classification and classification of industrial Internet data security as the starting point, organize the thorough investigation of industrial Internet data, and establish a list of important data protection. While strengthening the awareness of data security, enterprises actively respond to risks, increase capital investment, carry out the construction of data security protection means of industrial Internet, implement differentiated hierarchical management and protection, promote data hierarchical security sharing, establish and improve data security guarantee system, and improve the level of risk prevention and disposal.

5.3. Accelerate Data Security Technology Innovation and Capability Improvement

Focusing on the security protection requirements of the whole life cycle of industrial Internet data, speed up the technical breakthrough of data security monitoring, lightweight encryption, data desensitization and trusted protection, and improve the ability of anti tampering, anti theft and anti leakage. Support national professional institutions to build national industrial Internet security technology support capacity, and strive to improve the capabilities of data security monitoring and protection, security assessment, trusted exchange and sharing, tracking and traceability. Give full play to the guiding role of relevant industrial alliances, integrate industrial resources, innovate service models, and carry out joint technological research.

5.4. Promote the Safe Exchange, Sharing and Orderly Flow of Data

Build a trusted exchange and sharing service platform for industrial Internet data, ensure the safety of data exchange, sharing and transaction in the whole process, and form public service capabilities such as trusted security protection, security exchange and security sharing of industrial Internet data. Relying on the service platform, gather all parties from industry, University, research and application to jointly build a safe and reliable industrial Internet data space, promote the construction of a safe and reliable data market driven by industrial Internet data sharing, create a variety of services and business models such as industrial Internet data safe sharing, safe exchange and safe transaction, and activate the industrial Internet data security industrial ecosystem.

ISSN: 1813-4890

5.5. Strengthen the Construction of Industrial Data Security Talent Team

Actively strengthen cooperation with relevant government departments, various colleges and professional institutions, establish a comprehensive mechanism for the training, reward and introduction of security talents, and build a team with data security protection knowledge and data security protection technology through talent introduction, talent training, talent selection and other means, with the help of regular training and education, skill assessment, exchange and learning and other means A compound talent team that understands the overall situation of national data security protection and has a certain degree of practical operation ability, and provides intellectual and technical support for industrial data security strategic deployment, planning, decision-making consultation and major problems in the mode of "small core and large periphery".

Acknowledgments

This work was supported by the Wenzhou Polytechnic project under grant No. WZY2021002, the project of Wenzhou philosophy and social science planning under grant No.21wsk059,the visiting engineer project of Zhejiang Provincial Education Department under grant No. FG 2020 073.

References

[1] Zhang Xueying, Yang Shuaifeng, et al.Research on industrial Internet data security classification and grading protection framework[J]. Information Technology and Network Security, 2021,40(01):1-9.

[2] China Industrial Control Systems Cyber Emergency Response Team, National Industrial Security Industry Alliance. White paper on Industrial Internet data security[R].2020.

[3] Laszka, Abbas, Vorobeychik, Koutsoukos. Integrating redundancy, diversity, and hardening to improve security of industrial internet of things[J]. Taylor & Francis, 2020, 6(1):344-347.

[4] Zyskind G, Nathan O. Decentralizing privacy: Using blockchain to protect personal data[C]//2015 IEEE Security and Privacy Workshops. IEEE, 2015: 180-184.

[5] Kouzinopoulos C S, Spathoulas G, Giannoutakis K M, et al. Using blockchains to strengthen the security of internet of things[C]//International ISCIS Security Workshop. Springer, Cham,2018: 90-100.

[6] Alphand O, Amoretti M, Claeys T, et al. IoTChain: A blockchain security architecture for the Internet of Things[C]//2018 IEEE Wireless Communications and Networking Conference (WCNC). IEEE, 2018: 1-6.

[7] AITZHAN N Z,SVETINOVIC D. Security and privacy in decentralized energy trading through multi-signatures,blockchain and anonymous messaging streams[J].IEEE Transactions on Dependable and Secure Computing, 2016,PP (99).

[8] Ponomarev S, Atkison T. Industrial control system network intrusion detection by telemetry analysis [J]. IEEE Transactions on Dependable and Secure Computing, 2016,13 (2): 252–260.

[9] Kabir M R, Onik A R, Samad T. A network intrusion detection framework based on Bayesian network using wrapper approach [J]. International Journal of Computer Applications, 2017, 166 (4): 13–17.

[10] Knapp E D, Langill J T. Industrial Network Security: Securing critical infrastructure networks forsmartgrid, SCADA,andotherIndustrialControlSystems[M].Syn-gress,2014.

[11] Xiao ZF. Application analysis of vulnerability mining technology based on industrial Internet environment [J].Changjiang Information & Communications,2021,34(10):127-129.

[12] Liu Ruonan. Industrial big data security risk and technical response[J]. China Industry & Information Technology,2020,(8):20-24.