Mathematical Biosciences and Engineering

MBE, 19(3): 2896–2912.
DOI: 10.3934/mbe.2022133
Received: 29 September 2021
Revised: 01 December 2021
Accepted: 05 December 2021
Published: 14 January 2022

http://www.aimspress.com/journal/MBE

Research article

The risk assessment on the security of industrial internet infrastructure under intelligent convergence with the case of G.E.'s intellectual transformation

Jiang Zhao[1,2] and Dan Wu[1,3,*]

[1] Business School, Shaoxing University, Shaoxing 312000, China
[2] Zhejiang University of Finance & Economics, Hangzhou 310018, China
[3] Keyi College of Sci-Tech University, Shaoxing 211131, China

* **Correspondence:** Email: dandan_www@163.com.

Abstract: The industrial internet depends on the development of cloud computing, artificial intelligence, and big data analysis. Intelligent fusion is dependent on the architecture and security features of the industrial internet. Firstly, the paper studies the infrastructure mode that needs to be solved urgently in the industrial internet and provides a possible infrastructure mode and related security evaluation system. Secondly, it analyses the digital transformation process with the case of G.E.'s industrial nternet development practice. It clarifies that G.E. is forming a new value closed-loop through digital and strategy mixed channels. Thirdly, industrial internet security research is described within multiple viewpoints based on industrial internet applications, the security service and security assurance defense system's architecture, and the non-user entrance probability model. Finally, the paper illustrates the changes in knowledge workflow and social collaboration caused by the industrial internet under intelligent manufacture.

Keywords: industrial internet; fundamental infrastructure; intelligent integration; security risk assessment; knowledge workflow

1. Introduction

With the rapid development of the global industrial economy, artificial intelligence, the Internet

of Things, cloud computing, and other new information technologies are gradually integrated with modern industrial technology. Otherwise, data intelligence is closely related to the Internet and causes the upgrading and transformation of an industrial system, namely the industrial internet. In 2012, General Electric (G.E.) released the report "Industrial Internet: breaking the boundary between thinking and machine." It called the industrial internet "the third wave" of innovation and change. It first proposed production equipment and its integration and advocated using the Internet and big industrial data to improve its quality and services. From the perspective of production technology, based on an open and global network, which shows a positive effect on the industrial internet. Its essence is to connect equipment, personnel, and data analysis, integrate relevant information processes, and realize intelligent manufacturing by driving production equipment management through closed-loop data. From the perspective of industrial technology development, the industrial internet is the specific result of integrating and developing the global industrial system, advanced computing, and big data analysis. It promotes the intelligent transformation of the global industrial structure system and causes the rapid development of intellectual production and industrial network systems. At present, the industrial internet has been widely used in petrochemical, household appliances, energy, machinery, and other manufacturing-based industries.

According to China's industrial internet data in 2017, the total scale of China's industrial internet market has reached 470.91 billion yuan, with an average annual compound growth rate of more than 13%. By 2025, its industrial-scale will exceed 10 trillion yuan [1,2]. Because of the current situation and prospect of industrial internet development, the Ministry of Information Technology issued the "industrial internet platform construction and promotion guide", which laid the policy foundation and overall implementation plan for the strategic development of industrial internet. Around the future development direction of the industrial internet, the United States took the lead in proposing the concept of "advanced manufacturing". Likewise, Germany also proposed the concept of "industry 4.0". In this condition, Industry 4.0 focuses on improving mass productivity and performance by providing intelligence between devices and applications using machine learning (ML). A recent study by Maddikunnta provided survey-based new concepts and definitions of Industry 5.0 from the perspective of different industry practitioners and researchers. They highlight several research challenges and open issues that should be further developed to realize Industry 5.0 [3]. Subsequently, China also proposed the development plan of "made in China 2025".

Although the specific development strategies of different countries are different, the core is to promote the manufacturing industry's transformation and upgrading. Combined with the new generation of information technology and the significant industrial internet architecture, it enables the intelligent upgrading of equipment and the green environmental protection upgrading of process materials. Its essence is to form an effective ecological network system through the interconnection of data and industrial networks to realize the integration of intelligent manufacturing and industrialization and continuously promote industrial internet development to protect Internet architecture security. However, past decades have witnessed increased industrial systems and equipment newly connecting to the industrial internet. On the one hand, the traditional closed industrial network has been challenging to meet the needs of intelligent connections. Therefore, the industrial links need to adjust the original Internet architecture; on the other hand, the industrial internet system realizes various industrial components through the network interconnection information sharing among industrial systems. Simultaneously, the effective collaboration also exposes the production data, process, and other elements in the network, leading to targeted attacks

by hackers, affecting product production. Therefore, it is urgent to pay attention to the industrial internet's overall system architecture from the system level to improve its robustness and security. Therefore, this paper needs to solve the following problems:

1) How to build a useful industrial internet infrastructure model?

2) How to use the industrial internet architecture to solve security issues and privacy issues.

This assay shows a detailed industrial internet infrastructure model. In fact, it is divided into four layers: industry layer, business layer, application layer, and capability layer. The industry layer is focused on the macro perspective of the overall digital transformation of the industry. The business, application, and capability layers focus on the micro perspective of the digital transformation of enterprises. With this infrastructure model, the enterprises can adjust their business structure and have the ability to improve their competitiveness following the general direction of industrial digital transformation. Our contribution is to prove that the core of the industrial internet is to form data-driven wisdom based on comprehensive interconnection. Network, data, and security are the common foundation and support of industry and the internet.

2. Infrastructure model of industrial internet

2.1.Concept and connotation of industrial internet

Industrial internet is a kind of industrial intelligent information infrastructure formed by integrating and connecting big data, analytical tools, physical wireless networks, industrial equipment, or applying meta-level network functions to distributed systems. It has rich connotation:

1) From the component elements: the industrial internet closely connects information, people, and equipment, realizes the parallel development of the process through data exchange, synchronously reflects the equipment status, controls the equipment action in real-time, accurately optimizes the operation efficiency, and realizes the business objectives and social values. Compared with the ordinary Internet of Things, the users can apply industrial internet in many standard fields, including wearable devices, connected cars, vehicles, smart homes, smart retail, health monitoring, smart city, etc. These applications can bring significant social life changes by building a complex and perfect system.

2) From the perspective of technology development: the development of the industrial internet depends on big data technology, software integration technology, automation technology, intelligent production technology, etc. through platform integration, a distance free communication mode is constructed, which makes the production process safer and more efficient, produces new applications and services, and produces new business models and new economic types.

3) From the value dimension of the industrial internet, the industrial internet takes the underlying intelligent equipment as the system architecture foundation, realizes the integration of information elements and production factors through the system integration and intellectual perception, and promotes the realization of manufacturing enterprise value. Noteworthy that the industrial internet is an integrated processing and analysis platform for industrial cloud and big data. The industrial internet is a new model for the intelligent industry. It includes intelligent production control, intelligent operation decision optimization, the authentic connection between consumer demand and production and manufacturing, ultimately realizing intellectual production, network coordination, personalized customization, and service-oriented extension of products.

2.2. Research progress of industrial internet

From the perspective of control and analysis, the development of the industrial internet needs to speed up the acquisition, research, and visualization of external data [4] and realize the industrial system's architecture and intelligent production of products through data connection. The industrial internet industry alliance proposed that the basic architecture of the industrial internet mainly includes edge layer, platform layer, and platform application layer around the industrial internet system. Each level can be composed of relevant framework systems, including development service framework, deployment and operation service framework, model-driven unified service framework, business framework, connection computing structure framework, etc. Given the related network energy consumption problem, Wang Kun [5] proposed an energy-saving architecture consisting of an aware entity domain, a smooth service hosting network, a cloud server, and user applications. Similarly, Liu Deng [6] designs the basic framework of an intelligent factory system based on edge computing and discusses critical technical issues such as data fusion, configuration, security, etc. It gives the design scheme of corresponding subsystems. Besides, Lin SW proposed a reference architecture for the industrial internet and submitted future challenges, including security and privacy issues, interoperability, reliability, adaptability, data sharing, and it & or integration [7]. Gilchrist proposed that the key to optimizing industrial internet architecture is intelligent control of the data fusion layer [8]. Unlike the pure technical model framework, M. Iivari [9] proposed a business model framework for understanding value dynamics. The framework is an industrial internet framework obtained from the perspective of the life cycle and ecosystem configuration.

There are many potential risks in the application of the industrial internet. Among them, A. Sadeghi et al. clarified the dangers brought by industrial internet security data and privacy-sensitive data and proposed that externally directed attacks against industrial control systems may cause physical damage to the whole system [10]. Given this security risk, Z. Li et al. Built a secure energy trading system based on energy blockchain using joint blockchain technology, which significantly improved the system's security [11]. Due to blockchain technology's security characteristics, to build a more secure industrial control platform system, A. Bahga and V. K. Madiseti [12] proposed using platform blockchain technology to create a pilot platform, strengthening the scattered network connection points and improving the network security coefficient. With the wide application of industrial internet technology, the existing industrial internet needs a new architecture. Therefore, J. Q. Li [13] proposed using 5C architecture to describe the industrial internet system in the improvement of its security technology and overall performance.

From the development practice of industrial internet, industrial internet has been widely used in many different industries. For example, M. S. Hossain and Muhammad have studied the importance of Internet of things technology combined with medical devices and sensors in the next generation of the medical and health industry and proposed a health detection framework for professional health information acquisition by storing data in the cloud through mobile devices and sensors [14]. H. Wang proposed to apply the industrial internet computing system to the navigation field to improve the ship operation efficiency [15]. Besides, technology is widely used in the intelligent nonferrous metal industry [16]. The enterprises have applied the industrial internet for intelligent manufacturing. In a recent study, Liu Hongwei analyzed the key evaluation technologies such as widely connected low-power accurate measurement, network performance optimization, and large-scale node network reliability to propose an optimized intelligent manufacturing technology scheme [17]. Notably, the

industrial internet is a practical application of the Internet of things in the industrial environment, fully explaining the digital industry's deep integration and the entire industry [18]. Therefore, using industrial internet-related technologies, the virtual and natural worlds will seamlessly connect and interact and improve the intelligent degree of production [19]. This technology enables enterprises to quickly respond to the industrial production cycle and achieve new industrial growth by increasing production capacity, creating new hybrid business models, and promoting product transformation with intelligent technology [20,21]. Recently, Mothukuri et al. provided a comprehensive study concerning federated learning's security and privacy aspects. They prove that the most specific security threats currently are communication bottlenecks, poisoning, and backdoor attacks, while inference-based attacks are the most critical to the privacy of federated learning [22]. Likewise, Wang et al. propose a novel pairing-free certificateless scheme that utilizes the state-of-the-art blockchain technique and intelligent contract to construct a novel, reliable and efficient CLS scheme. Their security analysis holds more reliable security assurance with less computation and communication costs than other related schemes [23].

In short, the existing industrial internet system construction, security and privacy issues, and intelligent optimization have achieved good results. However, the industrial internet architecture systems of different industries and different enterprises often show distinct characteristics. It has not analyzed the typical features of different industrial internet architecture types and how to conduct targeted security measures to improve system security.

2.2.Infrastructure and application of industrial internet

The industrial internet has been widely used in many fields, including smart retail, smart healthcare, smart city, intelligent manufacturing, intelligent oil and gas exploitation, etc. Otherwise, it has a profound impact on these fields. It has brought about changes in the quality of life, operational efficiency, application, and service, resulting in new business models and new economic types. From the perspective of industrial internet infrastructure, the industrial internet of different enterprise types generally includes four basic levels: edge layer, IAAs layer (infrastructure as a service), PAAS layer (platform as service), and SaaS layer (software as service). The edge layer is mainly used for equipment access, edge data processing, and protocol analysis. IAAs layer is primarily used for cloud infrastructure architecture, including server and network storage, virtualization, etc. PAAS layer mainly involves the construction of industrial microservice component library, industrial data modeling and analysis, industrial big data system, resource deployment, and general PAAS platform management. The SaaS layer mainly includes the business operation process of production, management, service design, and the application innovation process of equipment status analysis and supply chain analysis. Thus, these four levels regulate the direct contact between nodes and work nodes in distinct organizational structures through effective cluster control. From the perspective of the information network, the industrial internet platform is the "operating system" of the new industrial system and the resource gathering carrier for enterprises to carry out socialized system production.

The industrial internet has realized the synchronous evolution of information space and physical space through cluster control nodes. Moreover, the effective scheduling of different work nodes is carried out through the intermediate cluster control node. Likewise, the industrial process's self-perception, self-analysis, liberalization, and self-processing can be identified. The industrial internet platform

involves a series of practical problems, such as access to various industrial equipment, massive data modeling and processing, industrial application innovation, and integration. It puts forward new technology requirements on platform database management, including industrial modeling and analysis technology, application development and microservice technology, and security technology.

For this reason, there are several critical technical challenges in the industrial internet: confidentiality and privacy; Interactivity; security; reliability and shock resistance; compatibility of the Internet of Things; and data sharing ability. Finally, suppliers' coordination and unification, intelligent factories/intelligent manufacturing, customer groups, and logistics are formed. The specific architecture is shown in Figure 1.

From the perspective of industrial internet applications, the industrial internet platform has become the hub of the real economy's whole factor connection, the center of resources, and the core control area of intelligent manufacturing. Industrial internet construction aims to carry out smart integration and data sharing, solve the interaction requirements of the general architecture framework by making different levels, and facilitate enterprises to develop various operational service systems. The first layer is to create a data layer based on data acquisition and transmission, including data analysis and collaboration, cloud security protection, etc., including cloud security, cloud storage, and big data. The cloud security system can strengthen the network and data protection and improve the system's safety factor. Through cloud storage, this data layer can improve the overall data storage capacity and backup capacity of the industrial internet; through the big data system, this data layer can make the data processing and analysis more robust and realize intelligent manufacturing. Noteworthy that the data layer is the fundamental layer. The second layer is the modeling layer of data processing and management with data analysis and processing as the core, including the data processing system, the intelligent management system, and the customized service system. The data processing system mainly completes intelligent data processing, analysis, and collaborative manufacturing. Otherwise, the intelligent management system especially carries out intelligent data management, process management, customer relationship management for industrial internet, and other data.

In contrast, the customized service system mainly carries out minor batch customization, highly customized, and on-demand production design. In this layer, the intelligent management system directly links to the other two systems. The industrial internet always delivers all related processing data to the third layer. Additionally, the third layer controls the intelligent control system Use layer, including the production control system and customer feedback system. The production control system is mainly used for production control, process optimization, and the complete process control of intelligent production. In contrast, the customer feedback system realizes the intelligent demand matching between customers and the market and on-demand production (Figure 1).

From the perspective of intelligent industrial development, the industrial internet will build three optimizations closed loops based on network, data, and security. The first is the closed-loop for machine and equipment operation optimization. Its core is to realize the dynamic optimization and adjustment of machines and equipment and build intelligent machines and flexible production lines based on the real-time perception and edge calculation of machine operation data and production environment data. The second is the closed-loop for production and operation optimization. Its core is the integrated processing and big data modeling analysis of information system data, manufacturing execution system data, and control system data to realize the dynamic optimization and adjustment of production and operation management and form the intelligent production model under various scenarios. The third is the closed-loop for enterprise collaboration, user interaction,

and product service optimization. Its core is to realize the innovation of enterprise resource organization and business activities based on the comprehensive integration and analysis of supply chain data, user demand data, product service data, and form new models such as networked collaboration, personalized customization, and service extension. Through the flow of information between different levels, the overall synergy of the industrial internet is affected. Data protection becomes more difficult due to the complexity of data types and flow paths, especially with new formats such as service-oriented extension and personalized customization. Further requirements are put forward for the industrial internet's security capability. Therefore, the security risk assessment system constructs as follows: three scale methods are used to compare the importance of industrial internet security indicators.

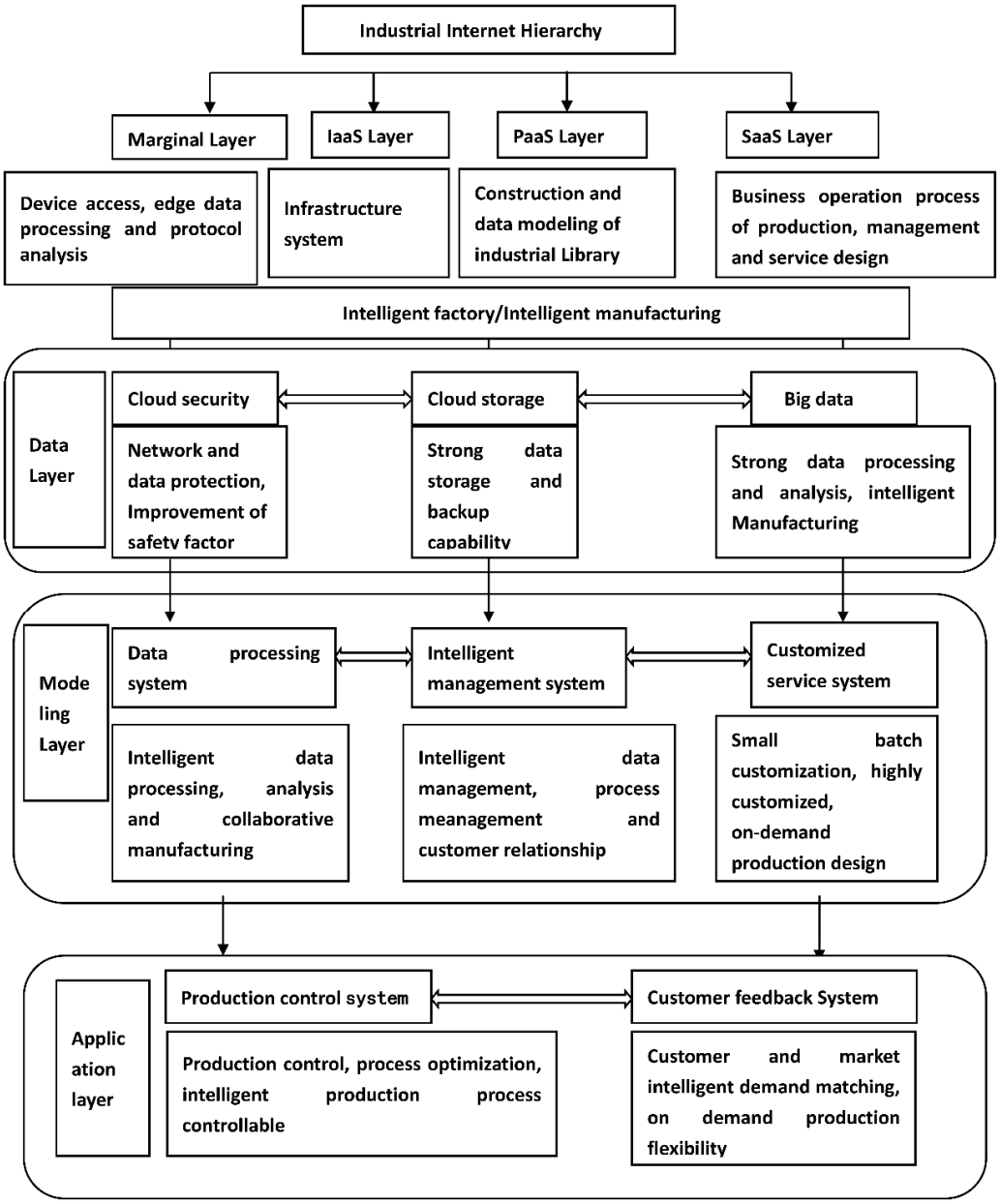

Figure 1. Framework diagram of hierarchical and hierarchical system infrastructure of intelligent industrial internet.

All the factors in criterion level A, level indicators P considered are being scored, and we can obtain the analytical matrix as follows.

$$K = \left(k_{ij}\right)_{\mathrm{m\times n}} = \begin{bmatrix} k_{11} & k_{12} & \cdots & k_{1m} \\ k_{21} & k_{22} & \cdots & k_{2m} \\ \cdots & \cdots & & \cdots \\ k_{m1} & k_{m2} & \cdots & k_{mn} \end{bmatrix} \tag{1}$$

Here, k_{ij} is considered as the ratio between i and j. After the comparison, we can obtain the score on the importance according to the three-scale method. The specific meaning is shown in the following expression.

$$k_{ij} = \begin{cases} 0\,, element\ i\ is\ less\ important\ than\ element\ j \\ 1, \quad element\ i\ is\ equal\ important\ to\ element\ j \\ 2, element\ i\ is\ more\ important\ than\ element\ j \end{cases}$$

According to the comparison matrix K and the following

$$k_{ij} = \begin{cases} r_i - r_j\ ;\ r_i > r_j \\ 1, \quad r_i = r_j \\ (r_j - r_i)^{-1}, r_i < r_j \end{cases} \tag{2}$$

Here, $r_i = \sum_{i=1}^{m} k_{il}, r_j = \sum_{j=1}^{m} k_{jl}$. The judgment matrix is obtained in the following Eq (3).

$$A = \left(a_{ij}\right)_{\mathrm{m\times m}} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{bmatrix} \tag{3}$$

Solve the eigenvector and characteristic root that satisfying $AW = \lambda_{max}W$. The factor λ_{max} is the largest eigenvalue of A, and W is considered as the corresponding eigenvalue of λ_{max}. The sub-vector w_i is deemed as the single weight of elements after calculation.

Then, we can perform the consistency test of judgment matrix A with the equation:

$$\mathrm{C.I.} = \frac{\lambda_{max} - n}{\mathrm{n-1}} \tag{4}$$

According to the random index table with distinct order. We can obtain the consistency ratio with the following equation.

$$\mathrm{C.R.} = \frac{\mathrm{C.I.}}{\mathrm{R.I.}} \tag{5}$$

When $\mathrm{C.R.} < 0.1$, the consistency of matrix A is acceptable, whereas $\mathrm{C.R.} \geq 0.1$, the consistency of matrix A needs rectification.

Finally, the total order of hierarchy is performed, which means the sum of multiplication between each element in the judgment matrix and the weight in each corresponding layer (excluding the target layer).

According to the above model, the risk assessment index system of the industrial internet is constructed. Each index's corresponding weight at different levels is established, which finally provides the basis for the industrial internet's security risk prediction.

3. Industrial internet security system and security mechanism

3.1.Content of industrial internet security architecture

According to the Ministry of information technology statistics, the total number of industrial internet platforms with industry influence in China has exceeded 50 by the end of 2018. The number of industrial internet industry alliance members has surpassed 1,000 and the average number of equipment connected to key platforms has reached 590,000. On the one hand, a large number of interconnected devices improve network complexity and application efficiency. On the other hand, with the increasing access devices of the network platform, the traditional security architecture based on the boundary is difficult to adapt to the rapid development of intelligent industrial internet. This result requires a new understanding of security architecture technology:

1) From the industrial application perspective, industrial internet security focus should focus on mobility of intelligent manufacture production's reliability and security duction.

2) From the standpoint of security service architecture, the Internet security system should be replanned. Additionally, the appropriate protective equipment and facilities of "zero trust security architecture" should be deployed. The firm should establish a dynamic and credible access control authorization mechanism. to ensure that the industrial internet can have continuous serviceability and prevent substantial data leakage.

3) From the security construction system's perspective, industrial internet security should focus on architecture security, network security, connection data security, application control security, etc. Its core is to reduce the corresponding attack risk by building a multi-level information security defense system to ensure system security in each technical framework area.

3.2.Industrial internet security risk content

The essence of industrial internet security includes system architecture security, network security, and IT/OT system security. Architecture security means protecting the entire architecture system, including the intelligent facilities, chip sensing system, and operating system. Besides that, these architecture protections are directly related to the multi-level structure of the industrial internet. Otherwise, network security refers to protecting network signal connections associated with the industrial internet to prevent abnormal access. The security of the IT/OT system mainly includes IT/OT integrated security defense. Different O.T. (operation technology) environments are relatively closed. General communication protocols are primarily private, and the difficulty coefficient of secure communication is high. In particular, there are many security loopholes in the external connection equipment of industrial internet, including specific industrial control equipment, wireless access equipment, and essential network equipment. Once used by attackers, it will seriously affect the reliable operation of equipment and network quality. This work is similar to a previous study on securing cloud computing environments used in the Internet of Things (IoT) [24].

The current network security risks are mainly divided into illegal access risks; operation and maintenance control risk, misoperation command risk, risk of remote transmission, malicious code risk, network intrusion attack risk, etc. Besides, due to the in-depth integration of O.T. and its industrial internet environment, the boundary between them is relatively fuzzy. Due to the increased interconnected equipment in the production and operation environment, it is easier to expose more

attack points. It may suffer from different types of space physical attacks. For example, the Maroochy water pump service system in Australia was attacked in 2000, making the whole dam system face the condition that the water pump could not work typically, and the alarm system collapsed. This situation is further aggravated by the communication loss between the intermediate computer and various pumping stations.

Similarly, the long-range cyber attacks on German steel companies in 2014 and the resulting damage to the Ukrainian energy network were also due to the network connection data's damage. Connection data security mainly refers to the production management data, external operation data, and user-related data of an intelligent production system. These intelligent data will decline products' production efficiency and market competitiveness under external attack. We need to prevent the risk of enterprise data leakage and strengthen the security guarantee. Accordingly, we set up perfect enterprise data sharing and open application rules as soon as possible and improve data security protection according to law. Application control security mainly refers to the intelligent production control system's security, including related control platforms, control protocol, and control software. Once the outside attacks the application control system, industrial production will suffer huge losses.

3.3.Industrial internet security protection mechanism

Industrial internet security and external equipment connection, network technology architecture, intelligent manufacturing, platform operation, and other links are the main threat from the transmission of information attacks. Information attacks mainly include mass attacks and targeted attacks. The mass attack primarily targets an uncertain link in the industrial internet data layer. In contrast, a directional attack targets any specific weak link in the three-tier architecture of the industrial internet. Therefore, it is not only for enterprises to solve this problem but also for system integrators, government departments, and other external forces to jointly improve system security and defense capability. The core is to build a complete active defense system, strengthen the monitoring and evaluation of the system, comprehensively enhance the safety awareness of managers, build a unified safety operation and maintenance management platform, and build a perfect "Trinity" comprehensive protection technology system before, during and after the event (Figure 2).

Take the industrial internet system as a whole and use various defense technologies to improve the system's transmission security comprehensively.

1) The first defense system of the industrial internet is the pre-defense system of external attack. Through the firewall, I.D. authentication, digital encryption technology, public key technology, and other technologies to establish an effective, trusted mechanism to strengthen the security of data sources, and through the real-time monitoring system to monitor abnormal data, timely perceive the security situation and determine the security risk level, and do an excellent job in defense.

2) The second defense system of the industrial internet is to build a defense system in an external attack. On the one hand, intrusion detection (IDS) technology, honeypot technology, and other technologies are used to identify attacks from outside in time and monitor external network attack nodes. On the other hand, we use a cloud platform and machine learning technology to build an effective information exchange system and establish a real-time vulnerability defense and security risk processing system for specific functional modules.

3) The construction of the third defense system is the defense system of forensics after an external attack. According to the daily network transmission of relevant data, the system log logs' timely

audit records each system's access and operation to identify the industrial control system's security. Besides, the system behavior technology can be used to timely feedback and understand some abnormal behaviors of the whole system after the operation, to timely repair the system vulnerabilities to improve the safety factor.

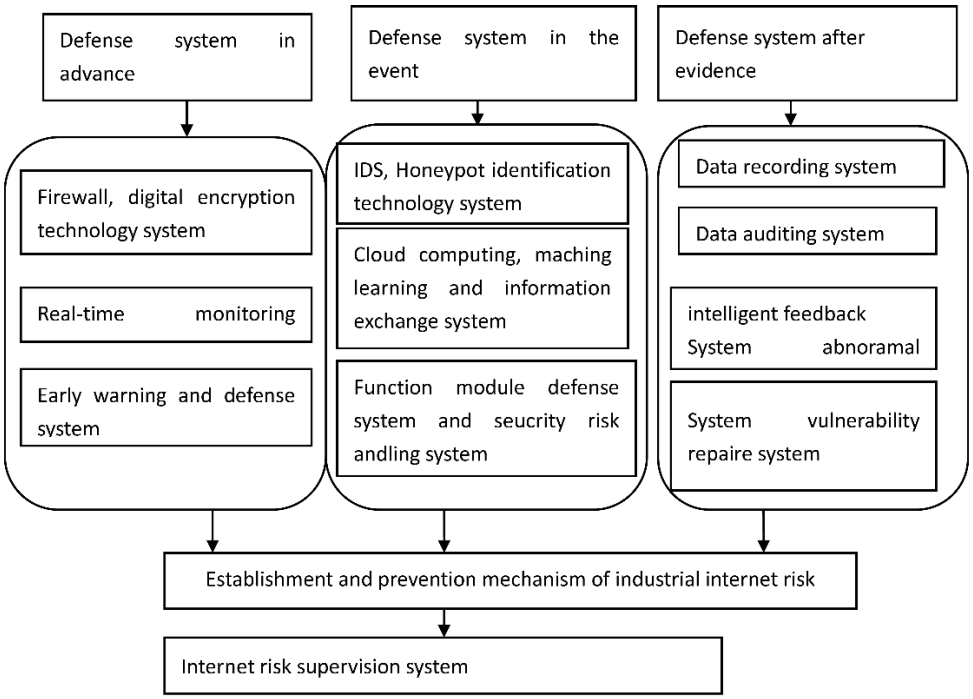

Figure 2. Industrial internet security architecture.

Suppose μ is the probability of external users and the variable q_1 considers being the probability of external illegal users filtered out by the pre-defense system. Moreover, the variable q_2 considers being the probability of external illicit users filtered out by the incident defense system. Finally, the variable q_3 defines as the probability that the post defense system filters out the external illegal users. Then there are two types of external users entering the system after filtering: the possibility is the probability of legitimate external users (1 - ξ) entering the system in proportion

$$p_{\text{legal}} = \mu(1-\xi)(1-q_1q_2q_3); \tag{6}$$

The probability of an illegal external user entering the system is as follows:

$$p_{\text{illegal}} = \mu\xi(1-q_1)(1-q_2)\,(1-q_3) \tag{7}$$

Consider $\mu = 0.7, \xi = 0.2, q_2 = 0.05, q_3 = 0.05$, we can obtain the following simulation with the changes of q_1 and p (Figure 3). The red curve shows the changes in the probability of an illegal external user entering the system. Whereas the blue curve shows the changes in the probability of a legal external user entering the system. From the model, it is evident that the probability of legitimate external users is gradually increasing. However, the probability of an illegal external user entering the system is decreasing rapidly. That means the defense system is quite critical for the industrial internet.

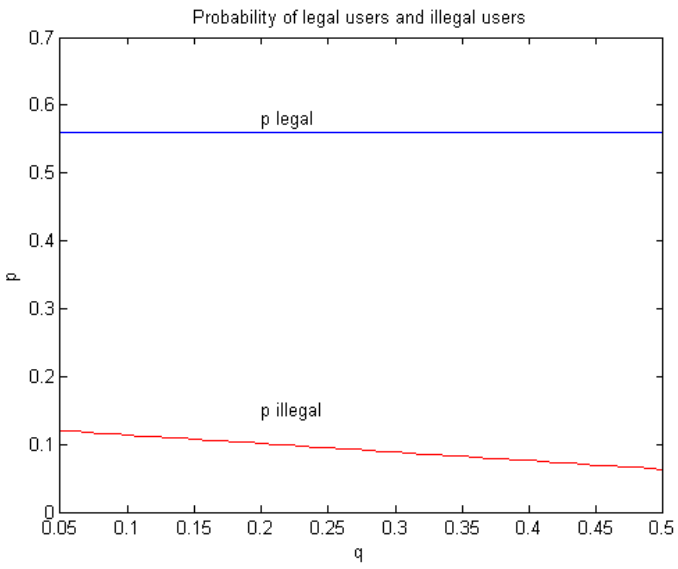

Figure 3. Probability of legal users and illegal users entering the defense system.

According to the model, after the three-tier defense system, the entry probability of illegal users is significantly reduced, while legitimate users' entry probability increases considerably. Also, the safety supervision system needs an effective operation. The firm should establish a sound safety system and risk management system. It needs to frequently speed up the research and development of safety core technology, improve and promote a multi-level safety risk supervision system. Our work shows some differences from a recent study. Their work presents a novel security framework for the message queue transport telemetry (MQTT) protocol based on publish/subscribe message order to enhance secure and privacy-friendly Internet of Things services. Their work relates to the light cryptographic schemes [25].

4. Case analysis of industrial internet–G.E. company

From the production practice, the development of the industrial internet has its internal reasons. Among them, a traditional manufacturing system's product design and product service are relatively out of touch with users' needs. Otherwise, the conventional manufacturing system has an insufficient perception of the production process. It isn't easy to reflect the deep dynamic characteristics of the physical process in the production process. On the other hand, it is difficult to accurately describe the manufacturing system due to its lack of accuracy. Industrial automation is a relatively conservative field from the development process, and the higher reliability of an infinite network often exceeds the complexity of unlimited connection. Wireless network sensors, time-sensitive networks, industrial software-defined networks, and related identification resolution systems have also become essential research fields. G.E.'s industrial internet development has gone through two stages: the first stage, through localization and expansion, G.E. has built several software departments, which has promoted the development of I.T. technology in enterprises. Then, its technology and platform layer applications are linked.

In the second stage, G.E. needs to redesign the business process based on the foundation and redesign the business network for the industrial internet. In the future, the development of G.E.'s

industrial internet will go through the third stage, redefining the business scope based on the industrial internet to help Ge become a solution-oriented organization to connect with employees, customers, and shareholders effectively. The development of the industrial internet represented by G.E. is going through the third stage. It carries out the overall enterprise digital architecture with cloud computing. Otherwise, G.E. shows digitization technology characteristics with big data analysis. Later, it forms a new value closed loop through the hybrid drive of digital and process. Therefore, G.E. company takes the lead in proposing the application data ring elements of industrial internet to drive the data flow process (Figure 4):

1) equipped industrial machines;
2) data extraction and storage of special devices;
3) industrial internet system construction;
4) machine algorithm and data analysis;
5) big data analysis;
6) data visualization of remote centers;
7) data sharing between target groups and machines;
8) objects It connects with the artificial network and the intelligent flow of data.

This process has laid a practical foundation for the development of the industrial internet.

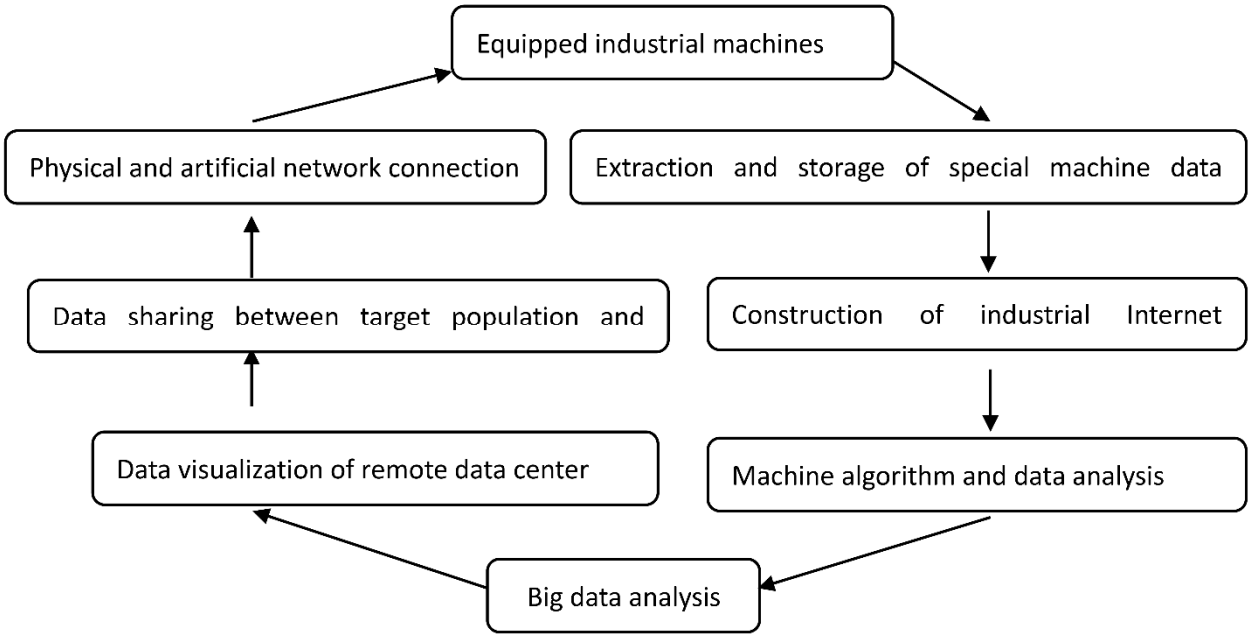

Figure 4. Data ring element driven process model of G.E. industrial internet.

Besides, G.E. has built four cloud computing centers to monitor and analyze all G.E. products every day. Through prefix, an open platform, we aimed to create an ecological strategy of the data-driven platform and pay attention to the coordination among all levels to prevent various internal and external risks. Finally, G.E. can effectively realize intelligent equipment. Through brilliant data analysis, it directly connects the equipment data with the network, and the operation results are timely analyzed and uploaded to the cloud. Then, the cloud server and user app software are combined to realize the intelligent flow of data. The enterprise's intelligent manufacturing mainly

includes two aspects: one is lean, and the other is intelligent manufacturing. The modeling and application layers framework cooperates with domestic manufacturers and universities to strengthen production, teaching, and research projects, including applying robot and artificial intelligence technology to intelligent production.

On the other hand, it constructs a digital transformation to form an effective supply chain ecosystem through the combination of upstream and downstream to achieve data sharing and information transparency mechanisms. For example, G.E. has a wind power department. By installing sensors on each wind turbine blade, the wind speed, wind speed, temperature, etc., of the wind turbine are nearly 100.

The wind power increases up to 4% by data acquisition, analysis, and wind turbine blade adjustment by wind turbine. In general, through lean, intelligent manufacturing and digital transformation, the cost and benefit of G.E. are optimized, the manufacturing process is shorter and faster, and the speed iteration is strengthened, which plays a role in promoting the industry.

5. Research conclusions and prospect

The proportion of the global digital economy in GDP increases rapidly, and the digital economy is expanding from consumption to manufacturing. The new industrial internet format based on intelligent manufacturing has become a new thrust for industrial development and product innovation [26,27]. In the future, the digital transformation of the industrial internet will further accelerate the fourth industrial revolution, and 5G communication network facilities will become critical supporting assets for developing the industrial internet[28]. High-speed mobile internet will realize the all-around interconnection of people, machines, and materials, promote efficient allocation of relevant manufacturing resources, and promote artificial intelligence, mobile internet, big data, and the real economy. To promote industrial quality reform. Through the industrial internet to realize the intelligent factory, speed up the real-time monitoring of the market, make an accurate judgment on the market orders, and finally realize the interconnection and optimization of production, manufacturing, management, and enterprises. This study shows that: first, different types of enterprises need to build a multi-level industrial internet infrastructure including edge layer, IAAs layer, PAAS layer, and SaaS layer and do not need to use cloud computing, big data, and other technologies to integrate and interconnect the industrial data of relevant production data and processes, to improve the effectiveness of intelligent manufacturing. Second, enterprises need to build a complete pre-, in-process, and post-event defense security system in the data, modeling, and application layers to effectively improve industrial internet security for potential targeted attacks.

Therefore, the future industrial internet will be improved and developed in many aspects: first, enhance perception depth. For example, the hydrogen plant in the “intelligent process manufacturing” program in the United States can model, analyze, and adjust the temperature field in real-time through multi-channel camera sensing. Second, enhance the scope of interconnection. For example, the German “digital factory” project integrates product design, planning, trial production, and mass production to form a digital factory and fully form process interconnection. Third, enhance the predictability of analysis. For example, the “knowledge dependence project” in Europe dynamically adjusts the production target according to the prediction analysis model. The next decade needs an expectation to develop into distributed manufacturing, collaborative manufacturing processes, and collaborative manufacturing capabilities in the future. The industrial production and

knowledge production processes require integration to form the knowledge workflow's automatic operation (Figure 5).

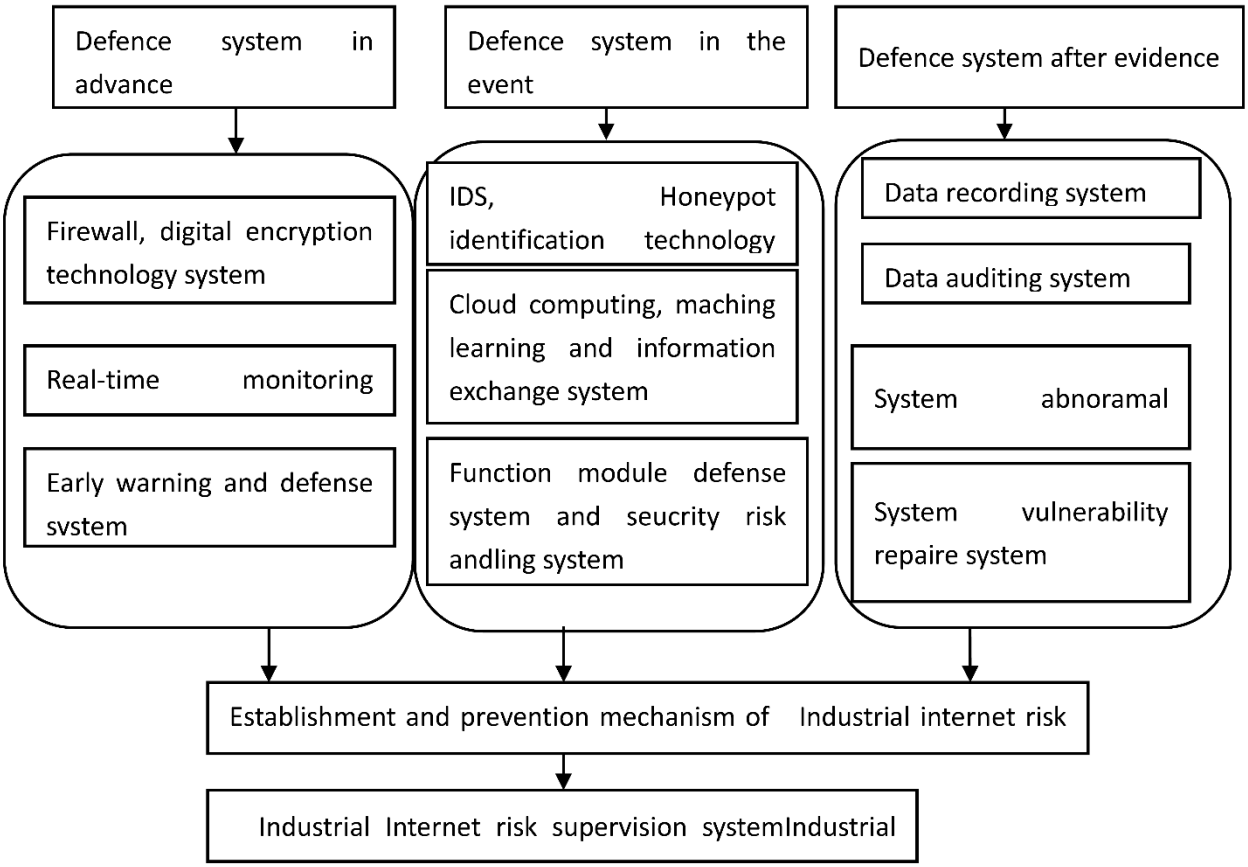

Figure 5. Flow diagram of intelligent knowledge workflow.

We can use digital integration to the resource allocation in the precision medicine and manufacturing industry. In the workflow, the task allocation model should be improved, including the unified service, access interface basic service layer (service container, cluster, configuration item, cache), the core algorithm processing, extra services, and others. The unified service access interface includes organization role adaptation, flow control adaptation, and integrated service interface. The firms can complete service expansion through intelligent sensor port, including pre-filtering model, dynamic preprocessing, assembly processing, action/event response, and conditional branch calculation. Likewise, the firms can also complete the service configuration by intelligent control adaptation of intelligent service port and competent services integration. That is to improve and optimize the customer value process by optimizing the platform's design, production, and management model, forming a perfect industrial internet Ecosystem, and realizing the profound reform of platform development subject, development content, and operation mechanism. In this process, we will continue to promote the transformation of the business model. The firm can construct the industrial ecological system with the new industrial technology. The firms should accelerate product innovation. They need to improve the typical digital design of the products. In the long run, it is helpful for social collaboration by the industrial internet.

Acknowledgments

Projects supported by Zhejiang Provincial Social Science Foundation (No. 21NDJC096YB), and Zhejiang Provincial Soft Science Project (No. 2021C25036) are greatly acknowledged.

Conflict of interest

The authors declare that they have no competing interests.

References

1. W. Z. Khan, M. H. Rehman, H. M. Zangoti, M. K. Afzal, N. Armi, K. Salah, Industrial internet of things: Recent advances, enabling technologies and open challenges, *Comput. Electr. Eng.*, **81** (2020), 106522. https://doi.org/10.1016/j.compeleceng.2019.106522.
2. D. Yin, Exploration on industrial internet to promoting the integration development of factory network and internet, *China Manage. Inf.*, **22** (2019), 74–75.
3. P. K. R. Maddikunta, Q. V. Pham, B. Prabadevi, N. Deepa, K. Dev, T. R. Gadekallu, et al., Industry 5.0: A survey on enabling technologies and potential applications, *J. Ind. Inf. Integr.,* (2021), 100257. https://doi.org/10.1016/j.jii.2021.100257.
4. J. Posada, C. Toro, I. Barandiaran, D. Oyarzun, D. Stricker, R. D. Amicis, et al., Visual computing as a key enabling technology for industrie 4.0 and industrial internet, *IEEE Comput. Graphics Appl.*, **35** (2015), 26–40. https://doi.org/10.1109/MCG.2015.45.
5. K. Wang, Y. Wang, Y. Sun, S. Guo, J. Wu, Green industrial internet of things architecture: An energy-efficient perspective, *IEEE Commun. Mag.*, **54** (2016), 48–54. https://doi.org/10.1109/MCOM.2016.1600399CM.
6. D. Liu, W. Zhou, A smart factory system based on edge computing, *J. Hubei Univ. Technol.*, **34** (2019), 74–77.
7. S. W. Lin, B. Miller, J. Durand, G. Bleakley, A. Chigani, R. Martin, et al., *The Industrial Internet of Things Volume G1: Reference Rrchitecture, Industrial Internet Consortium*, (2017), 10–46.
8. A. Gilchrist, Designing industrial internet systems, *Industry 4.0. Apress*, Berkeley, (2016), 87–118. https://doi.org/10.1007/978-1-4842-2047-4_5.
9. M. Iivari, P. Ahokangas, M. Komi, M. Tihinen, K. Valtanen, Toward ecosystemic business models in the context of industrial internet, in *the 23rd Nordic Academy of Management Conference (NFF 2015), Business in Society,* Copenhagen, 2015.
10. A, Sadeghi, W. Cristian, M. Waidner, Security and privacy challenges in industrial internet of things, in *Proceedings of the 52nd Annual Design Automation Conference*, (2015), 1–6. https://doi.org/10.1145/2744769.2747942.
11. Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, Y. Zhang, Consortium blockchain for secure energy trading in industrial internet of things, *IEEE Trans. Ind. Inf.*, **14** (2018), 3690–3700. https://doi.org/10.1109/TII.2017.2786307.
12. A. Bahga, V. K. Madisetti, Blockchain platform for industrial internet of things, *J. Software Eng. Appl.*, **9** (2016), 533–546. https://doi.org/10.4236/jsea.2016.910036.

13. J. Q. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, Q. Yan, Industrial internet: A survey on the enabling technologies, applications, and challenges, *IEEE Commun. Surv. Tutorials*, **19** (2017), 1504–1526. https://doi.org/10.1109/COMST.2017.2691349.
14. M. S. Hossain, G. Muhammad, Cloud-assisted industrial internet of Things (iiot)–enabled framework for health monitoring, *Comput. Networks*, **101** (2016), 192–202. https://doi.org/10.1016/j.comnet.2016.01.009.
15. H. Wang, O. L. Osen, G. Li, H. N. Dai, W. Zeng, Big data and Industrial Internet of Things for the maritime industry in northwestern Norway, in *TENCON 2015–2015 IEEE Region 10 Conference*, (2015), 1–5. https://doi.org/10.1109/TENCON.2015.7372918.
16. J. Guo, Research on automatic control system based on intelligent non-ferrous metal industry internet, *World Nonferrous Met.*, **3** (2019), 14–15.
17. H. W. Liu, Research on technology of intelligent factory industrial internet simulation and evaluation system based on electronic products, *Electron. Test*, **8** (2019), 134–136.
18. L. L. Xiao, Jing Yu, Y. J. Xia, J. Huang, Z. M. Zhang, An empirical study on the application of global industrial internet platform, *Technol. IoT AI*, **51** (2019), 1–8.
19. L. Wang, G. Wang, Big data in cyber-physical systems, digital manufacturing and industry 4.0, *Int. J. Eng. Manuf. (IJEM)*, **6** (2016), 1–8. https://doi.org/10.5815/ijem.2016.04.01.
20. S. Gierej, The framework of business model in the context of Industrial Internet of Things, *Procedia Eng.*, **182** (2017), 206–212. https://doi.org/10.1016/j.proeng.2017.03.166.
21. S. M. Laudien, B. Daxböck, The influence of the Industrial Internet of Things on business model design: A qualitative-empirical analysis, *Int. J. Innovation Manage.*, **20** (2016), 1640014. https://doi.org/10.1142/S1363919616400144.
22. V. Mothukuri, R. M. Parizi, S. Pouriyeh, Y. Huang, A. Dehghantanha, G. Srivastava, A survey on security and privacy of federated learning, *Future Gener. Comput. Syst.*, **115** (2021), 619–640. https://doi.org/10.1016/j.future.2020.10.007.
23. W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, C. Su, Blockchain-based reliable and efficient certificateless signature for IIoT devices, *IEEE Trans. Ind. Inf.*, 2021. https://doi.org/10.1109/TII.2021.3084753.
24. C. Thirumalai, S. Mohan, G. Srivastava, An efficient public key secure scheme for cloud and IoT security, *Comput. Commun.*, **150** (2020), 634–643. https://doi.org/10.1016/j.comcom.2019.12.015.
25. L. Malina, G. Srivastava, P. Dzurenda, J. Hajny, R. Fujdiak, A secure publish/subscribe protocol for Internet of Things, in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, (2019), 1–10. https://doi.org/10.1145/3339252.3340503.
26. Q. Li, Q. Tang, L. Chan, H. Wei, Y. Pu, H. Jiang, et al., Smart manufacturing standardization: Architectures, reference models and standards framework, *Comput. Ind.*, **101** (2018), 91–106. https://doi.org/10.1016/j.compind.2018.06.005.
27. Y. Lv, J. Zhang, Intelligent factory technology framework based on big data, *Comput. Integr. Manuf. Syst.*, **22** (2016), 2691–2697. Available from : https://kns.cnki.net/kcms/detail/11.3619.tp.20161021.1035.010.html.