Mobile Networks and Applications (2023) 28:1043–1058
https://doi.org/10.1007/s11036-023-02143-5

Security and Privacy in 5G-IIoT Smart Factories: Novel Approaches, Trends, and Challenges

Chun-Cheng Lin[1,2,3] · Ching-Tsorng Tsai[4] · Yu-Liang Liu[5] · Tsai-Ting Chang[1] · Yung-Sheng Chang[1]

Accepted: 23 August 2021 / Published online: 5 July 2023

Abstract
To implement various artificial intelligence and automation applications in smart factories, edge computing and industrial Internet of Things (IIoT) devices must be widely deployed, so as to increase the demand of coping with huge-scale and high-diversity data. Through deployment of fifth-generation (5G) networks (providing wide broadband, low latency, and massive machine type communications), industrial wireless networks, cloud, and fixed/mobile end devices in smart factories are interoperated in a harmony. However, with the huge-scale deployment of 5G networks and the IIoT in smart factories, threats and attacks against various vulnerabilities increase enormously, and cause considerable security and privacy challenges. Consequently, this article investigates crucial security and privacy issues for 5G-IIoT smart factories in three entities (i.e., physical layer, data layer and application layer), and further surveys recent approaches based on deep learning, reinforcement learning, and blockchain. In addition, this article provides future perspectives and challenges along this line of research.

Keywords 5G · Security · Privacy · Smart factory · Deep learning · Smart manufacturing · Industrial Internet of things · Blockchain · Edge computing · Cloud computing

1 Introduction

Recently, 5G networks have acted as catalysts to accelerate the progress in Industry 4.0. As the main application services of 5G networks targeting at enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (URLLC) [1], the wireless service requirements in smart factories (including low-latency wireless communications, reliable real-time data collection, and strong data security) are projected to be fulfilled with the facilitation of 5G networks, as illustrated in Fig. 1.

Although 5G networks bring great benefits to smart factories, a lot of obstacles still need to be overcome, and two of the most critical issues lie in security and privacy. Security and privacy have been regarded as the most challenging issues in smart manufacturing since data from/to factories is extremely confidential and has a high commercial value. In addition, cyber-attacks in factories may also cause physical damages and even threaten human lives (e.g., the TRITON malware attacked the safety instrumented system, and the Mirai malware launched distributed denial-of-service, DDoS, attacks against IIoT devices).

✉ Yu-Liang Liu
ylliu@ocu.edu.tw

Chun-Cheng Lin
cclin321@nycu.edu.tw

Ching-Tsorng Tsai
cttsai@thu.edu.tw

Tsai-Ting Chang
offoffo2424@gmail.com

Yung-Sheng Chang
a509170123@gmail.com

1 Department of Industrial Engineering and Management, National Yang Ming Chiao Tung University, Hsinchu 300, Taiwan

2 Department of Business Administration, Asia University, Taichung 413, Taiwan

3 Department of Medical Research, China Medical University Hospital, China Medical University, Taichung 404, Taiwan

4 Department of Computer Science, Tunghai University, Taichung 407, Taiwan

5 Department of Multimedia and Game Design, Overseas Chinese University, Taichung 407, Taiwan

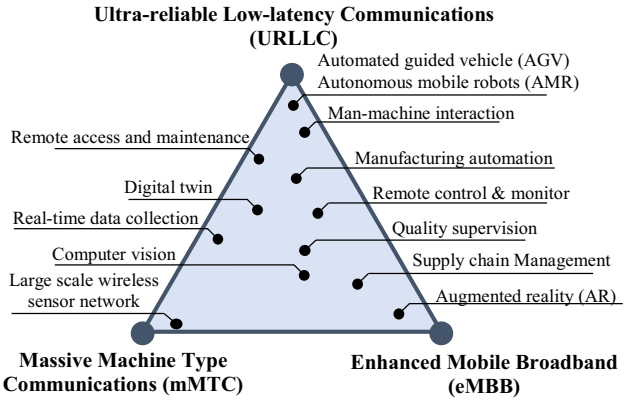

Fig. 1 The applications based on three 5G technologies in smart factories

Complexity of the IIoT network and the large number of devices in factories increase security threats and vulnerabilities. Hence, a lot of attention needs to be paid to cybersecurity. Sisinni et al. [2] discussed the difference between IoT and IIoT, provided an IIoT architecture, and reviewed the state-of-the-art research efforts as well as potential research directions to solve IIoT challenges. Gebremichael et al. [3] introduced the current standards for IIoT, and provided an overview of the solutions to cybersecurity issues. Vitturi et al. [4] discussed the standards, new technologies, and application fields for industrial communication systems. Tange et al. [5] analyzed security and privacy issues and solutions of the 5G and IoT.

Most previous works discussed the security issues of 5G and IIoT separately. Most of them focused on the security issues of network layer and data layer, and seldom talked about the security issues of physical layer. In addition, to the best of our understanding, no previous survey articles considered the security approaches of smart factories based on 5G and IIoT. However, 5G and IIoT are the key technologies to build a smart factory. As a result, this article focuses on the state-of-the-art solutions to security and privacy issues in 5G-IIoT smart factories including physical layer, network layer, and data layer, and discusses their challenges as well as future research perspectives.

The rest of this article is structured as follows. Section 2 introduces related works on the concerned topic. The architecture of the 5G smart factory is presented, and key technologies of the architecture are discussed in Section 3. The security and privacy issues of each layer in 5G-IIoT smart factory are discussed in Section 4. The recent approaches for the above security and privacy issues are presented in Section 5. The future research perspectives on 5G-IIoT smart factory are given in Section 6, followed by conclusions in Section 7.

2 Related works

This section first reviews the related works on IoT and IIoT security, and then reviews and compares the recent works on 5G, IoT, IIoT, and smart factories.

2.1 IoT snd IIoT security

The IoT is more vulnerable to suffer cyber threat than conventional networks, and the infection of threat is more serious than before. The main reasons are as follows: Complex IoT environments leads to a wider attack surface [6]. Large-scale connected devices and considerable users increase the amount of cybersecurity vulnerabilities and attack targets [7]. The leak of uniformity in standards of connectivity protocols, platform, and hardware may cause cybersecurity vulnerabilities [3]. The connection of virtual and physical environments allows cyberthreats to translate into physical consequences, thereby generating a greater impact [8].

Smart factory is one of the IoT application scenarios. The main difference between IIoT and IoT is that the IIoT connects the operation technology and information technology to build a cyber-physical system (CPS) [9]. The IIoT focuses on machine-to-machine communications, in which the reliability and latency of networks are more important. The IIoT network needs to meet specific communication protocols, and the devices must be applicable to particular industrial environment. Therefore, the requirements of security in the IIoT are different.

From the literature, most discussion on the IoT security includes authentication [10], authorization [11], access control [12], cyberattack [13], privacy [14], and CIA Triad, confidentiality [15], integrity [16], and availability [17]. According to the survey of Tange et al. [5], most security issues in the IoT and IIoT are overlapping, but the safety and security requirements for the IIoT are generally stricter than those found in a typical IoT scenario. However, there are still other issues needed to be noticed in the IIoT, e.g., network resilience. Network resilience refers to the capability of remaining operations when suffering attack. Although the security issues between the IoT and the IIoT are similar, the security issues and priorities concerned by the IIoT and the IoT are different.

2.2 5G, IoT, and smart factory

The 5G increases transmission speed and capacity, supports simultaneous connections of more devices, and provides reliable and low latency transmission. Hence, 5G is the accelerator for widespread applications of the IoT [18, 19]. The combination of 5G and IoT is applicable to many fields

[20], e.g., smart city [21], smart agriculture [22], smart health [23], and smart factory [24]. Smart factories have a lot of application scenarios of 5G. For instance, 5G with drones supports the function of monitoring and collecting the environmental data [25], and 5G with AGVs and AMRs is applied to automatic material handling systems (AMHSs) [26]. In addition, customized private 5G networks are a new option for companies to develop their vertical applications [27].

The security and privacy issues of 5G networks are challenging. Especially, adopting novel technologies may cause new security issues. Khan et al. [28] proposed a 5G evolved security model which includes confidentiality, integrity, availability, visibility, and centralized policy. They also discussed new cyberthreats after adopting 5G key technologies, e.g., software-defined network (SDN), network functions virtualization (NFV), and network slices. Ahmad et al. [29] proposed the approaches based on above technologies to solve cybersecurity issues.

Recent works on various integrated approaches of IoT, IIoT, 5G, cybersecurity, and smart factory are compared in Table 1. Surveys on security and privacy of IoT, IIoT and 5G have been hot topics, and recent interests have focused on blockchain [13], fog computing [5], and machine learning (ML) [14]. With the widespread applications of 5G and IoT, more and more surveys on security and privacy have considered the issues of security and privacy for 5G and IoT [20, 30]. However, to the best of our understanding, there was no survey on network communication systems in smart factories based on 5G and IIoT. Therefore, this article focuses on the issues of security and privacy in 5G-IIoT smart factories, and summarized their recent approaches.

Table 1 Comparison of recent works on integrated approaches of IoT, IIoT, 5G, cybersecurity, and smart factory

Approach	IoT	IIoT	5G	Cybersecurity	Smart factory
[5]		✓		✓	
[6]	✓				
[7]	✓			✓	
[8]	✓			✓	
[9]		✓			✓
[10]		✓		✓	
[13]	✓			✓	
[14]	✓			✓	
[18]			✓		
[20]	✓		✓		
[26]			✓		✓
[28]			✓	✓	
[29]			✓	✓	
[30]	✓		✓	✓	

3 Architecture of the 5G-IIoT smart factory

From the literature, considerable interests have been put on the architecture of the 5G-IIoT smart factories, which are generally composed of physical layer, network layer, and application layer [9], as illustrated in Fig. 2.

3.1 Physical layer

The physical layer includes all fundamental physical resources in 5G-IIoT smart factories, e.g., manufacturing equipment, communication devices, and computing devices. In smart factories, since all the physical resources need to keep up with novel technologies, the physical layer includes the following devices:

1) Modular production unit: To quickly respond to the rapidly changeable market demand, the production system in smart factories tends to be modular and reconfigurable. Modular production line can be efficiently and easily reconfigured into a variety of production arrangements and production processes. Each modular production unit not only meets the manufacturing requirements of products, but also improves the factory efficiency in a self-reconfigured way. Through modular design, factories can quickly assemble different parts, establish and adjust arrangements, replace parts or the whole module, and easily maintain the unit.
2) Devices for machine-to-machine (M2M) communications: With the increasing amount of wireless communication devices, the production line can be equipped with equipment with high mobility and flexibility (e.g., AMRs and AGVs). All machines, equipment, and related sensors are equipped with 5G wireless communication devices, so that each equipment has the ability to connect to the network and send back real-time information. With development of 5G and low-power wide-area network technologies [31, 32], the M2M communications play an important role. Communication devices in a factory with a large-scale IIoT should include the following features: low setup cost, small size, low energy consumption, long buttery lifetime, and wireless connectivity that can adapt to dynamic and harsh environments. In general, ordinary components of M2M systems in factories includes RFID and Wi-Fi.
3) Edge computing devices: Edge computing is a distributed computing paradigm which brings computation of applications, data, and services closer to the location where the data is stored and processed immediately, to improve response time, save bandwidth, and shorten latency. Edge computing devices also improve security

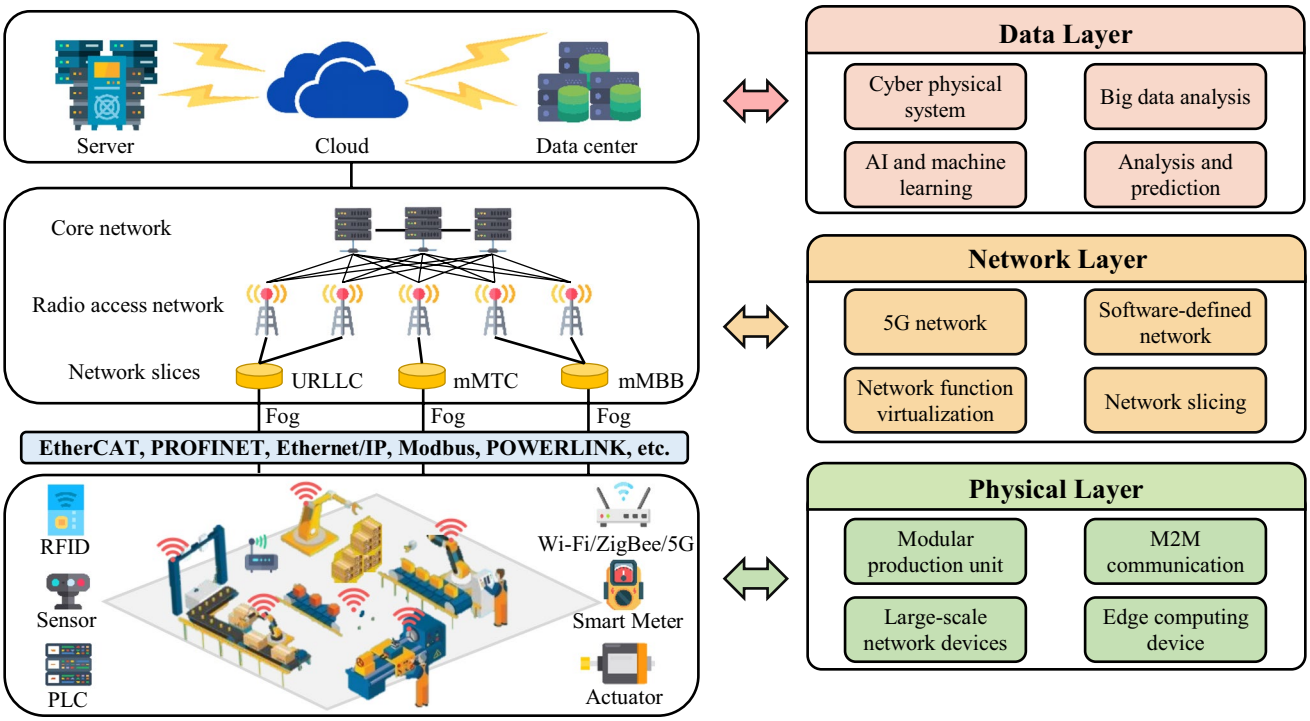

Fig. 2 Architecture of the 5G-IIoT smart factory

and privacy of data because it is not necessary to transmit the whole data to the cloud.

3.2 Network layer

To integrate 5G with the IIoT, networks need to support novel protocols (e.g., [33]) and novel data types with higher flexibility and scalability. For this purpose, SDN and NFV are two enabling technologies for 5G networks. In addition, to meet various applications in factories, the 5G network can create multiple slices according to practical demands of different services (i.e., eMBB, mMTC, and URLLC).

1) SDN and NFV: SDN enables networks to be controlled intelligently and centrally using application software. By separating the control layer from the data layer, SDN enables that the network control becomes directly programmable, and the underlying infrastructure is virtual with applications and network services. NFV is a technology to virtualize network services, e.g., firewalls and routers that conventionally run on specific hardware. Through NFV, these services become software-definable with network functions. By abstracting these services from dedicated hardware, the services can run network functions on standard hardware. That is, less physical hardware is needed, and allows resource consolidation that reduces physical space, power, and overall cost.

2) Network slicing: The physical network is sliced into multiple virtual networks based on requirements of 5G applications in factories. For example, the eMBB network meets the need of large-scale data and high-definition image transmissions, e.g., precision manufacturing requires higher-definition image transmissions to identify defects. The mMTC network supports deployment of large-scale network, which can monitor thousands of equipment and inspect various and complex materials. The URLLC network is suitable for industrial control systems which cannot tolerate time errors, e.g., industrial automatic control and remote-controlled equipment. Note that each network slice is independent and isolated, and hence an attacked network will be separated from the others when a cyberattack occurs.

3.3 Data layer

In a 5G-IIoT smart factory, the amount of data collected from the IIoT can be enormous with large dimensions. With facilitation of cloud technologies, data from the physical layer and network layer can be logically stored in a centralized manner (although the physical deployment of cloud servers may be distributive) [34]. In this case, data can be further processed using ML, deep learning (DL), and AI technologies to establish predictive models and further make decisions.

1) Cyber physical system (CPS): In the CPS, computational and physical resources are strictly interconnected by advanced communication technologies to achieve seamless integration between physical and cyber worlds. Connection between physical equipment and cyber data in factories can be achieved by 5G networks. Through characteristics of high bandwidth and low latency, 5G networks can be used to transfer all the data from the bottom cognitive layer (i.e., machines) to computing devices. These data can be utilized to analyze and make decisions in real time, so that equipment and systems in the smart factory accomplish real-time cognition and dynamic control.
2) Big data analysis and AI: AI acts as a brain in the smart factory, and 5G networks transmit the big data from the whole factory to the brain that analyzes and makes decisions. The applications of AI appear everywhere in the smart factory. On security, AI and 5G can enhance the monitoring system with real-time image recognition. In the manufacturing process, through 5G networks, all the real-time data is transmitted to computing devices, in which conditions of machines are analyzes by AI to decide whether to conduct preventative maintenance. On material handling, after introducing 5G, manual material handling tasks can be replaced by AGVs and AMRs. Furthermore, integrated with computer vision, sensors, and optimization algorithms, the optimal route scheduling and the assignment of handling vehicles can be well arranged [35].

4 Security issues in 5G-IIoT smart factories

The 5G system relies increasingly on software and cloud technologies than previous wireless communication networks. Hence, security issues have received increasing attention. This section discusses secuirty and privacy issues in 5G-IIoT smart factories. Classification of these issues is given Fig. 3, and thes issues in the factory are illustrated in Fig. 4.

4.1 Security in the physical layer

Novel 5G technologies in the physical layer include full-duplex (FD) communication, massive multiple-input-multiple-output (mMIMO) [36], ultra-dense network (UDN), and millimeter wave (mmWave). Different from conventional security approaches that focused on the core network and the logical (i.e., not physical) layer, the 5G security issues tend to expand from the central network to the network edge, and from the logical layer to the physical layer. Major security issues in the physical layer of a smart factory are as follows:

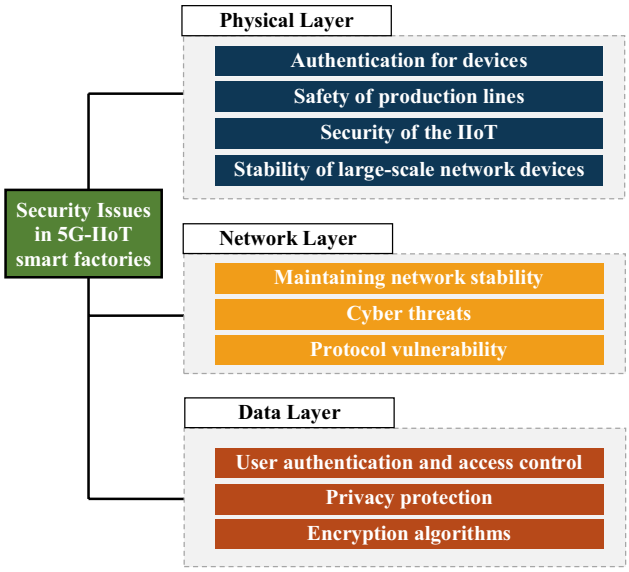

Fig. 3 Classification of security issues faced by the 5G-IIoT smart factory

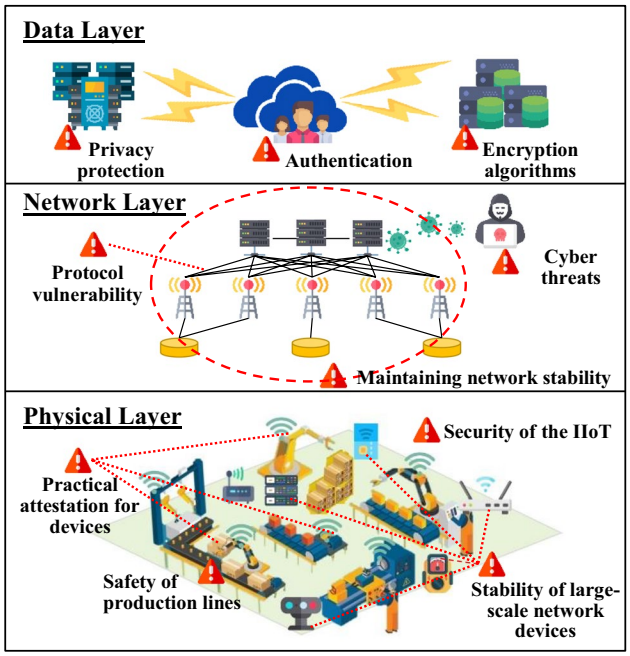

Fig. 4 Security and privacy issues in 5G-IIoT smart factories

1) Authentication for devices: Since considerable IIoT devices are deployed in the factory, any device may be security vulnerability. For mass deployment of IIoT devices, affordable IIoT devices with simple functions are adopted, and hence conventional security approaches are not applicable to these devices. Generally, secure hardware is the best way for device attestation, but is too complicated and expensive to be installed on each

IIoT device. Therefore, it would be more feasible to use software-based device authentication methods. However, these approaches often require to compliance with lots of assumptions, which may not easily be achieved in practice.

2) Safety of production lines: Maintaining safety of production lines would be one of the most fundamental issues in factories. Related challenges include machine fault detection, product quality monitoring, production line health monitoring, remote factory diagnosis, and real-time production system control. As production lines tend to be virtualized and decentralized, it is also crucial to investigate how to collect, analyze, monitor, manage, and control real-time data of equipment, processes, workpieces, finished products, and environment in factories. In addition, it is crucial to avoid complete shutdown of the production system. A robust production system requires keeping operations of production lines and repairing faulty equipment when an attack or sudden failure occurs. Furthermore, it must also be considered how to better use features of 5G in smart factories.
3) Security of the IIoT: Through deployment of fog and edge computing devices, the data storage and computing functions move from cloud to edge, and it makes security of the IIoT more important. However, most sensors in industrial wireless sensor networks (IWSN) and actuators lack computing resources, and hence they are often in an unsafe condition. Therefore, it is crucial to find end-to-end security solutions, such as detection of malicious attacks against sensors, control system, and edge devices.
4) Stability of large-scale network devices: Mobile edge computing (MEC) devices have only limited battery capacity. Hence, it is crucial to extend the battery life in each device, and improve the energy efficiency. In addition, it is challenging to optimize resource allocation in large-scale networking equipment to meet the offloading probability of quality of service (QoS) [37]. It requires innovative solutions to collect, process, and analyze a large amount of data in 5G networks.

4.2 Security in the network layer

In 5G-IIoT factories, threats against security, reliability, and privacy in the network layer are much diversified. In the past, security issues could be addressed through physical protection systems. However, 5G systems extensively use the SDN and NFV technologies, so that it is difficult to protect systems against cyberattacks. Major security issues in the network layer are as follows:

1) Maintaining network stability: The network slicing technology separates 5G wireless networks based on the defined three main application areas (i.e., eMBB, mMTC, and uRLLC). Under this technology, it is challenging to maintain a stable and trustworthy network, including maintaining stable network traffic, establishing reliable communication quality, constructing a large-scale wireless sensor network, improving network reliability, and reducing network latency [38]. It is also challenging to establish a network security mechanism to address problems such as network delays and blocking, and to maintain the QoS.
2) Cyber threats: In an edge computing system with IIoT devices, distributed and peer-to-peer network systems must be built based on 5G networks. Under the wireless network architecture, external attacks have become a serious problem to the factory. Various malicious attacks include worms, Trojans, viruses, and runtime attacks. In addition, new cyber threats are often unpredictable.
3) Protocol vulnerability: Some organizations such as the Global Association for Mobile Communications Systems (GSMA) have been committed to improving 5G protocols. However, network vendors that provide private 5G factory networks may not completely follow the best standards. Hence, it has been hard to defend attacks through protocol vulnerabilities, e.g., man-in at the-middle-attacks, DDoS attacks, eavesdropping, and intrusion attacks.

4.3 Security in the data layer

Various real-time data from (virtual) simulation models to (real-world) job shop production conditions is important in making manufacturing decisions, and hence it is very attractive to competitors or hackers. Major security issues in the data layer are as follows:

1) User authentication and access control: Since 5G heterogeneous networks include diversified and complex applications, they require frequent identity verification and collect more sensitive data. With a lot of participants (including end users, service providers, and infrastructure providers), services (including virtual machines and cloud services), and infrastructures (including user devices and edge data centers) in this network, there are increasing security vulnerabilities, causing external threats and internal malicious behavior.
2) Privacy protection: The 5G-IIoT factory includes an edge computing framework, which is managed by the cloud center. Hence, the edge/cloud center faces various threats. Furthermore, attackers may adopt to program vulnerabilities to conduct privilege escalation to perform unauthorized actions. In addition, it is difficult to set up private 5G networks in the factory to prevent data leakage, because it involves a lot of participants, including

cloud operators, mobile network operators, and network equipment providers.

3) Encryption algorithms: In 5G networks, the confidentiality, integrity, and authentication are accomplished through encryption. According to Kerckhoffs' principle, encryption algorithms are public. The public encryption algorithms with password length limitations could be broken with brute-force search. Aside from the data from sensors, the data in smart factories includes the communication data between various users and IIoT devices, some of which are sensitive data. It is challenging to effectively delete the encrypted data, because it is hard to guarantee revocation of sensitive data, and whether there are no ways to get the deleted data back.

5 Recent approaches for security and privacy issues in 5G-IIoT smart factories

We conducted a survey on recent approaches based on the keywords of the article title (i.e., '5G', 'IIoT', 'smart factory', 'security', and 'privacy') and the issues mentioned in Section 4 with the restriction of the publication year during 2018–2021. The online libraries considered in this survey include the IEEE Xplore, Elsevier/ScienceDirect, and Google Scholar. The recent approaches based on DL, ML, reinforcement learning (RL), blockchain, and other novel techniques for security and privacy issues of the physical layer, network layer, and data layer in 5G-IIoT factories are given in Tables 2, 3, and 4, respectively.

5.1 Solutions for security in the physical layer

1) Authentication for devices

Since considerable IIoT devices are deployed in the factory, high-quality authentication for these devices needs to be conducted frequently. The major goals of the solutions are to improve the efficiency and reduce the cost of authentication, and hence it shows a trend of lightweight authentication scheme. Because of the higher computational cost and complexity of the cryptography-based solutions, recent works have shown much interest to investigate the physical layer authentication, especially the physically unclonable function (PUF). PUF is currently one of the best ways to build a private key for identifying each device. The PUF circuit cannot be determined or controlled in advance, and is not an additional encryption authentication algorithm. Hence, it provides a low-cost authentication scheme.

Gope et al. [39] proposed a two-factor authentication protocol based on password and PUF for IoT devices, and

Table 2 Recent approaches of the physical layer in 5G-IIoT factories

Issue	Technique	Approach
Authentication for devices	Blockchain for authentication	Password and PUF two-factor authentication scheme [39] Lightweight and physically secure anonymous mutual authentication protocol [40] Active physical layer authentication mechanism [41]
	Blockchain for authentication	Lightweight blockchain-enabled RFID-based authentication protocols [42] Identity-based cryptograph and blockchain [43]
	ML for authentication	ML-based threshold-free physical layer authentication [44] CSI-based physical layer authentication and SVM [45]
Stability of production lines	Condition monitoring, diagnosis, prediction, and health management	ST-CNN [46] Integrated multi-objective optimization with DL [47] Dynamic EDBN fault classification modeling [48] Deep transfer learning [49]
Security for IIoT	Edge computing security	FLANN、E-TLBO [50] Distributed DL system [51] Evidence reasoning network [52]
	Connecting devices security	Random finite set theory and Bayesian filter [53] EPCA-HG-CNN [54] Permutation entropy [55]
Large-scale network devices	Fog computing	Online learning and iterative algorithm [56] Stackelberg game model [57]
	Edge computing	Lyapunov and convex optimization [58] Greedy and threshold strategies based two-phase scheduling [59] RL [60]
	Energy management	Lyapunov optimization and ADMM [61] Distributed Q-learning algorithm [62]

Table 3 Recent approaches of the network layer in 5G-IIoT factories

Issue	Technique	Approach
Maintaining network stability	Resource scheduling	Route-aware data flow dynamic reconstruction algorithm [63] Polynomial time approximation algorithm [64] CGA-CC [65] Q-learning, RL [66]
	Network slicing	online Gaussian mixture model clustering algorithm [67] DRL [68]
	Flow control	Redistribution of hop delay bounds based heuristic algorithm [69] Incremental learning-based network elephants learner and analyzer [70]
Cyber threat	DDos attack detection	Learning-driven semi-supervised learning model [71]
		Blockchain and AI [72]
	network flow anomaly detection	Random subspace-based random tree [73]
		Long short-term memory [74] Deep Learning [75]
	Other attack detection	SHMM-Siamese Network [76] Online- learning-base Kalman filter [77]
Protocol vulnerabilities		DCNN framework [78] Distributed attack detection system of DL [79] Combining AI and blockchain [80] Deep auto-encoded dense neural network [81]

Table 4 Recent approaches of the data layer in 5G-IIoT factories

Issue	Technique	Approach
User authentication and access control	Data access control	Hybrid cloud infrastructure, tag-aided encryption [82] CP-ABE with AAM [83]
	Blockchain for access control	Blockchain system with credit-based consensus mechanism [84] Blockchain system with trust evaluation-based voting mechanism [85]
	User authentication and identification	Facial dynamics-based identification [86] Biometric verification and user's smart card, two-factors authentication [87]
Privacy protection	Privacy protection architecture	Blockchain-based IIoT framework, Bell-La Padula model, and Bbia model [88]
		Distributed and anonymous data collection framework based on multilevel edge computing [89]
	Data sharing privacy	Blockchain and federated learning-based sharing architecture [90] Privilege-based multilevel organizational data-sharing scheme [91] Blockchain-based compressed and private data sharing framework [92]
	Data Integrity	stochastic blockchain-based data checking scheme [16]
Data sharing privacy	The search of encrypted data	File-centric multi-key aggregate keyword searchable encryption system [93] Secure k-nearest neighbor scheme, order-preserving encryption, R tree [94] Paring-free certificate-based searchable encryption [95] Blockchain-aided searchable attribute-based encryption [96]
	The deletion of encrypted data	outsourced policy-based puncturable encryption [97] A key-policy attribute-based encryption scheme [98]

using the concept of reverse fuzzy extractor to solve the nose noise issue in the PUF operation. Gope et al. [40] used PUF and the lightweight cryptographic primitives in lightweight and physically secure anonymous mutual authentication protocol for IWSNs. Towards non-coherent massive single-input multiple-output (SIMO) IIoT communication systems, Gu et al. [41] adopted an active physical layer authentication mechanism. In their mechanism, transmitters send the messages embedded with additional information (normally referred to as tag) to perform authentication. This mechanism minimizes the message and the tag symbol error rate while fulfilling the requirements of power constraint and message accuracy to improve the reliability of authentication system.

Blockchain technology makes the access control of data more widely without damaging the data integrity. Therefore, blockchain has been applied in the field of device authentication frequency. Jangirala et al. [42] proposed lightweight

blockchain-enabled RFID-based authentication protocols for supply chains in the 5G MEC environment. RFID can assist automatic identification and data capture in materials and supply chain management. Through characteristics of blockchain and combination with the 5G MEC technique, a secure distributed information architecture can be built.

Through smart contracts of blockchain, the authentication for the departments of supply chain can perform efficiently. Shen et al. [43] used blockchain to improve the efficiency and reliability of authentication. Their proposed blockchain-based security authentication mechanism used the public secret key anonymously to authenticate devices from cross-domain IIoT. It avoids the security issues of leaking identity and addresses the constraint of cross-domain device authentication in identity-based cryptograph.

Except for blockchain, ML also plays a role in the authentication field. Pan et al. [44] proposed an ML-based threshold-free physical layer authentication for industrial wireless CPSs. By using ML to learn the channel state information (CSI), received messages are classified into legitimate or illegitimate messages according to the CSI. Chen et al. [45] applied ML to physical layer authentication and detection of clone attacks as well as sybil attacks for industrial wireless edge networks. Their method adopted the data from CSI-based physical layer authentication as offline training sample sets and support vector machine (SVM) as the training model to detect attacks.

2) Safety of production lines

The classic fault diagnosis model includes two key points: feature extraction and fault classification. A lot of recent works have investigated condition monitoring, diagnosis, prediction and health management, i.e., distinguishing abnormal and normal conditions and identifying abnormal types.

Han et al. [46] adopted the spatiotemporal pattern network (STPN) for spatiotemporal feature learning, and adopted convolutional neural networks (CNNs) for condition classification. Multivariate time series data of complex mechanical systems for troubleshooting is applied to establish a self-adaptive classifier suitable for various working conditions and different fault severity. Ma et al. [47] proposed an integrated multi-objective optimization DL-based fault diagnosis method, which weights and integrates the convolution residual network (CRN), the deep belief network (DBN), and the deep auto-encoder (DAE), and showed that the fitness of the results is better than other single DL models.

In a smart factory environment, it is difficult to ensure that operators can always find abnormal conditions and fix them correctly and immediately. Hence, Wang et al. [48] developed an extended deep belief network (EDBN) to mitigate this problem, and established a dynamic EDBN fault classification modeling framework. Digital twin is an important way to achieve smart manufacturing. Xu et al. [49] presented a two-phase digital-twin-assisted fault diagnosis method using deep transfer learning, which provides new possibilities for fault diagnosis.

3) Security for The IIoT

The physical layer includes edge computing devices and considerable sensors as well as actuators. The following discussion is separated into edge computing security and connecting devices security.

As for edge computing security, the fundamental issue is concerned about how to detect the intrusion attack. Naik et al. [50] proposed an intrusion detection model for IoT edge computing devices using the functional link artificial neural network (FLANN) as detection model and the elitist teaching-learning based optimization (E-TLBO) metaheuristic to adjust parameters. Tian et al. [51] developed a distributed DL system for web attack detection on edge devices. Their method used uniform resource locator addresses (URLs) in three DL models to improve the system stability, in which anomalous requests and normal ones can be distinguished through automatically learning features. Tian et al. [52] proposed a real-time lateral movement detection scheme based on evidence reasoning networks for the edge computing environment. With vulnerability correlation, their scheme can track suspicious events, and provide strong guarantee for rapid and effective evidence investigation to make sure the accuracy of detection.

On the other hand, as for the security of connecting devices in factories (including sensors, actuators, and industrial control systems), all of these devices could suffer from cyber-attacks, and types of those attacks would be diversified. Yang et al. [53] developed a model to detect multiple attacks in the CPS using the random finite set theory and the Bayesian filter with the sequential Monte Carlo method to reduce computational complexity. Krithivasan et al. [54] detected cyber-attacks in industrial control systems through using the enhanced principal component analysis (EPCA) to reduce the dimensionality and using the hypergraph-based convolution neural network (HG-CNN) to detect anomality, in which the hypergraph can assist in identifying relevant information, removing redundant features, and reducing the training cost and time.

For detecting stealthy attacks in industrial control systems, Hu et al. [55] presented a permutation entropy-based method. They showed that there is significant difference between the residuals generated during a stealthy attack and original random series; and hence, the permutation entropy can characterize the non-randomness contained in the residuals so as to distinguish the attack.

4) Stability of large-scale network devices

As for resource allocation and task scheduling in the fog computing architecture, Wang et al. [56] proposed a fog computing architecture based on non-orthogonal multiple access (NOMA), which uses online learning and iterative algorithm to conduct task scheduling and subcarrier allocation with an objective to minimize the time delay and energy consumption. Jie et al. [57] used the Stackelberg model to build a two-phase game model that contains cloud centers, fog service providers, and data users, in which the competitive goal is to achieve the Nash equilibrium and Stackelberg equilibrium as the final allocation result of fog computing resource.

As for resource allocation in the edge computing architecture, Wu et al. [58] transformed the data collection and delay problem in the MEC-based IIoT into a stochastic optimization problem for queuing stability, in which Lyapunov functions and convex optimization are leveraged to allocate data transmission and system utility balancing throughput as well as fairness. Li et al. [59] proposed a four-level computing system architecture for smart manufacturing and AI applications, and they designed two-phase edge computing resource allocation based on greedy and threshold strategies with latency constraints. The first phase is to choose the edge computing server for tasks, and the second phase is to conduct cooperative scheduling of multiple edge computing servers. Deng et al. [60] considered the service-level agreement (SLA) as the trustworthiness indicator for the IoT system and used RL to generate a dynamic resource allocation scheme for edge computing of CPU and memory resource.

Because the IIoT includes a considerable number of connected devices, the efficiency of power consumption and energy management become an important issue. For the problem of energy management in a multiuser MEC system with energy harvesting devices, Zhang et al. [61] formulated the power consumption minimization problem with the battery queue stability and QoS constraints as a stochastic optimization programming model, and adopted the Lyapunov optimization approach to design an online algorithm for central energy management. They also used an alternating direction method of multipliers (ADMM) based distributed algorithm to compute the power management of each user. Wang et al. [62] developed a distributed Q-learning aided power allocation algorithm for two-layer heterogeneous IIoT networks which includes macro base stations and femto micro base stations. The Q-learning method combines three multi-agent collaboration modes (i.e., independent learning, docitive learning, and cooperative learning) to accelerate convergence speed and improve training performance.

5.2 Solutions for security in the network layer

1) Maintaining network stability

Through the technologies of SDN, NFV, and network slicing, it is flexible to dynamically allocate resources and to connect the network slices based on different QoS and network requirements in the 5G-IIoT smart factories so as to realize different smart manufacturing applications. The following discussion on maintaining network stability is separated into resource scheduling, network slicing, and flow control.

For resource scheduling, Wan et al. [63] proposed a mechanism of cross-network fusion and scheduling, which is analyzed from the perspective of high dynamic characteristics and different delay requirements of data flows, and proposed a route-aware data flow dynamic reconstruction algorithm to improve the efficiency of manufacturing data cross-network fusion, especially for multi-variety and small-batch smart manufacturing systems. Wang et al. [64] adopted the SDN to extract the network control logic from the cyber and physical network of CPS. They redesigned the communication rules and combined the two networks to solve the problem of task scheduling and the network path assignment simultaneously through a polynomial time approximation algorithm.

To solve the controller placement problem (CPP) and the controller scheduling problem (CSP) in SDN, Huang et al. [65] developed a gradient-descent-based scheduling algorithm to optimize the probabilistic distribution of requests among all controllers and to balance the workload and minimum of response time. For the CPP, they adopted the clustering algorithm to split the network into non-overlapping sub-networks, and then applied the genetic algorithm to solve the CPP in each sub-network.

For virtual network function (VNF) resource allocation, Li et al. [66] reformulated the VNF scheduling problem with the consideration of latency requirement for different services as a Markov decision process problem, and used RL to learn the best scheduling policy.

The network can be sliced according to QoS requirements or application scenarios. However, from the literature, there have been no consensus on which method is best suitable for network slicing. Messaoud et al. [67] proposed a resource allocation scheme for network slices, which ensures the requirements of bandwidth, delay, and reliability for different QoS requirement applications in Industry 4.0. First, their scheme uses the online Gaussian mixture model clustering algorithm to assign IoT devices to slices and estimate the average throughout of the slices. Then, it uses mini-batch gradient descent to reserve the radio resource and channel based on the throughout. Finally, it allocates the intra-slices based on

the max-utility algorithm. Xiang et al. [63] developed a method for fog and radio access network slicing. They used deep reinforcement learning (DRL) to tackle content caching and mode selection for cloud servers with the constraint of the fronthaul capacity and the fog access points capability; and uses the Perron-Frobenius theorem and proximal theory to solve a sub-problem on the power allocation considering the inter-slice and intra-slice interference.

Control and scheduling of network flow have been receiving much attention. It has been challenging to meet the QoS requirements when the flow in 5G network slices changes over time. Qu et al. [69] investigated the dynamic flow migration problem for embedded services in SDN/NFV-enabled 5G core networks, and used a heuristic algorithm based on redistribution of hop delay bounds to address the tradeoff between load balancing and reconfiguration overhead and to meet end-to-end delay requirements with time-varying traffic. Estrada-Solano et al. [70] proposed an incremental learning-based method (i.e., network elephant learner and analyzer) to detect flow at the server side of the SDN-based data center. It can timely identify elephant flow and mice flow while generating low control overhead.

2) Cyber threats

The attacks from the network are the major threat to network systems in smart factories. Hence, the first line of defense for protecting network security is to detect malicious attack. DDoS attack is one of the common attack types. For DDoS attack detection, Ravi and Shalinie [71] proposed a security scheme which leverages the SDN paradigm to mitigate the DDoS attack on IoT servers, and uses semi-supervised ML algorithm to detect attacks. Fang et al. [72] developed a smart contract and AI-based security countermeasure, which hides the protected servers in blockchain networks and restricts the scale of DDoS flexibly through transaction fees.

Changes in network flow are usually the direct evidence of suffering from cyberattacks. Therefore, a lot of detection methods based on network traffic analysis have been proposed. Hassan et al. [73] adopted an ensemble-learning model using network traffic of supervisory control and data acquisition (SCADA)-based IIoT platform to detect cyberattack. Their model combines random subspace learning method with random trees to solve the sensitivity of irrelevant features and to reduce the overfitting problem, while it is applicable to deployment on different IoT platforms. Saharkhizan et al. [74] implemented a long short-term memory model using network traffic to detect IoT cyberattack. Maimó et al. [75] proposed a MEC of 5G mobile network solution using DL techniques to analyze network traffic and detect network anomalies, which showed exceptional abnormal symptom detection (ASD) performance experimentally.

For detection of other cyberattacks, Wang et al. [76] proposed a channel virtual representation-based pilot contamination attack detection model for 5G-IoT networks. They distinguished the sensitive message senders by physical characteristics of the 5G mmWave channel, and used the single hidden and multiple measurements Siamese network (SHMM-Siamese Network) as detect model, which can be deployed on communication devices without change and extra computing.

Against false data injection attacks, Chattopadhyay and Mitra [77] developed a detection model using online-learning Kalman filter to filter out malicious sensor observations while retaining other sensor measurements. To minimize the estimation error of data sets from various sensor subsets, the filter gain matrix is updated iteratively over time through simultaneous perturbation stochastic approximation (SPSA).

3) Protocol vulnerabilities

Introducing CPSs to smart factories remarkably increases information transmissions, and further magnifies protocol vulnerabilities. Hussain et al. [78] integrated the deep CNN and real network data to provide early detection of malicious operations of CPSs. Increasing vulnerabilities in various IIoT protocols increase the number of zero-day attacks, and most of these attacks are slight variants of previously known attacks. Hence, instead of using conventional centralized systems, Diro et al. [79] proposed a distributed attack detection system and used DL to discovery the hidden patterns.

Blockchain can establish a secure environment that provides resource sharing in a decentralized way. Dai et al. [80] integrated AI and blockchain with wireless networks to build a flexible, safe, and smart cache environment, and used advanced DRL to maximize cache resource utilization. In addition, Rezvy et al. [81] implemented a deep auto-encoded dense neural network algorithm to defense against external attacks on protocol vulnerabilities, and used it to detect 5G and IoT network intrusions or attacks. It also used the benchmark Aegean Wi-Fi as the evaluation dataset of the algorithm, showing excellent performance. In addition to DL, blockchain technology is also suitable for use in 5G networks on security issues.

5.3 Solutions for security in the data layer security

1) User authentication and access control

It has been common to use cryptography-based schemes to encrypt data and restrict user access. Especially, ciphertext policy attribute-based encryption (CP-ABE) is often adopted to enforce fine-grained access control. Qi et al.

[82] designed a hybrid cloud infrastructure which includes private cloud and public cloud. To maintain efficiency and privacy, the public cloud storages the encrypted IIoT data, and the CP-ABE tasks are assigned to the distributed private clouds. Xiong et al. [83] proposed a secure and efficient multiauthority access control for IoT cloud storage (SEM-ACSIT) scheme. It not only uses CP-ABE, but also introduces an attribute authority management (AAM) module as an authentication agent to reduce the storage cost of public secret key and to make sure the forward and backward secrecy when authenticating.

Blockchain enjoys the characteristics of decentralization, anonymity, immutability, and security. Hence, blockchain-based access control schemes have received a lot of attention. Huang et al. [84] provided a blockchain system with credit-based consensus mechanism towards secure IIoT. Their system adopts directed acyclic graph-structured blockchain, and leverages the asynchronous consensus model to improve the system throughput. Because of the transparency of blockchain, symmetric key flexibility is easily updated by each node without any central server while reducing computing consumption.

Wu and Ansari [85] translated IIoT devices into a number of groups of blockchain architecture. The IIoT devices within one group can share information and deter malicious users from accessing the network by modifying the access control list (ACL). Each block records all results of IIoT sensors accessing requests and all the changes of ACL. They designed a new voting mechanism with trust evaluation to make decision of access request.

Except for the above solutions to access control and authentication, combing personal identification with devices authentication can improve the system security. Castiglione et al. [86] used facial dynamics in identity authentication. Their method exploits the dynamic appearance and the local features characterizing the face of an individual during speech to identify. The above information is captured by the edge IoT device and is transmitted to the cloud data center to train the identification model by a deep feedforward network. Das et al. [87] provided a biometric-based privacy preserving user authentication using biometric verification and user's smart card as two factors to authenticate the user.

2) Privacy protection

The data transmission range of 5G-IIoT in smart factories is from the physical devices in factories to network service providers as well as cloud data centers. To realize smart manufacturing applications, the data needs to be shared from local equipment to cloud servers. However, privacy protection is challenging during transferring data while making sure to meet the CIA Triad.

For the privacy protection overall architecture, Wan et al. [88] proposed a blockchain-based IIoT architecture to enhance security and privacy in smart factories. The storage layer of the architecture plays the role of a data center which keeps the encrypted tamper-resistant data and blockchain records. They designed a private unique block structure with block header and block body. The block header stores the structured data; and the block body stores the access record of each node. Through the above design, each operation will be strictly supervised through blocks, while maintaining the advantages of conventional databases. Usman et al. [89] designed a distributed and anonymous data collection framework based on the multilevel edge computing architecture to improve the QoS and minimize packet drop and end-to-end delay. Mobile sinks must be registered as a level-two edge device before collecting data from level-one edge devices to protect the network, and the privacy of mobile sinks is preserved through group-based signed data collection requests.

For the privacy of data sharing between the IIoT and the cloud, Lu et al. [90] provided a privacy-preserved data sharing architecture based on blockchain and federated learning. The blockchain is only utilized for retrieving data and managing the sharing transactions while the real data is stored in local edge devices. They transformed the data sharing problem into an ML problem using federated learning to build data models and sharing the models instead of raw data directly. Zaghloul et al. [91] proposed a privilege-based multilevel organizational data-sharing scheme for big data sharing in could. Their scheme combined the privilege-based access structure into attribute-based encryption to manage and share the big data. Qi et al. [92] designed a compressed and private data sharing framework by using blockchain to efficiently provide product traceability and to record the product status during production process. They adopted an off-chain procedure to compress product data before being submitted to the system, and the access control mechanism dedicates an access control manager to specify access policies for encryptions and to distribute the key to authorized users.

To keep data integrity, Chen et al. [16] proposed a stochastic blockchain-based data checking scheme to protect data integrity in the IoT. The stochastic blockchain combines the chain structure with the consensus mechanism to restrict the number of cooperative nodes and to distribute the load to edge nodes. The data is broadcasted by randomly selected nodes, thereby confusing the attackers to improve the system security.

3) Encryption algorithms

For the search of encrypted data, Zhou et al. [93] developed a file-centric multi-key aggregate keyword searchable encryption system, which is applicable to share data and

authorize the search of data for IIoT data management. They also presented two security models: the security models for the indistinguishable selective-file chosen keyword attack and the indistinguishable selective-file keyword guessing attack, to protect trapdoor and ciphertext privacy. Xu et al. [94] proposed an efficient and geometric range query scheme to search and access control of encrypted spatial data. Their scheme is based on secure k-nearest neighbor scheme and uses order-preserving encryption to achieve comparative operations among encrypted spatial data. Then, the R-tree is used to classify spatial data according to the criteria of distance relationships among points in space to reduce search space and comparison time.

To handle the cloud ciphertext retrieval, Lu et al. [95] presented a paring-free certificate-based searchable encryption method. Through their method, all desired ciphertexts can be obtained without decrypting the ciphertexts and leaking the search keywords. Their method is built over the prime-order elliptic curve group; and the keyword ciphertexts and trapdoor are embedded with a secret that is only shared between the data owner and the recipient to defend against keyword guessing attacks. Liu et al. [96] proposed a blockchain-aided searchable attribute-based encryption method with the function of revocation and decryption for fine-grained IoT data sharing and searching. The conventional central server is replaced by a coalition blockchain with a set of trusted consensus nodes to manage user keys and system parameters. The users' search requests and partial token are submitted to the blockchain, and consensus nodes generate the complete token with the user's attribute keys so as to realize the searchable attribute-based encryption.

For the deletion of encrypted data in cloud, Hao et al. [16] provided a self-controlled outsourced data deletion scheme based on outsourced policy-based puncturable encryption which can convert the puncture policies-based puncture process into the update process of access policies. Therefore, the data owners can control the decryption capability through key puncturing without distributing key materials to the cloud and IoT devices to realize the reliable data deletion. Xue et al. [98] proposed a key-policy attribute-based encryption scheme for assured deletion, in which the attribute revocation cryptographic primitive and the Merkle hash tree are used to implement a fine-grained access control and a verifiable data deletion method, so that the large amount of data in smart manufacturing is more secure.

6 Future research perspectives

This section provides future research perspectives for DL technologies for security and privacy in 5G-IIoT smart factories (Fig. 5).

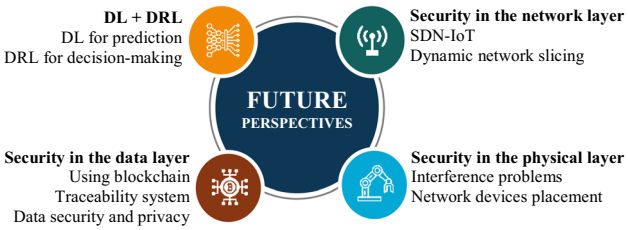

Fig. 5 Future research perspectives of DL technologies for security and privacy in smart factories

6.1 Future trend for security of devices in the physical layer and stability maintenance

Establishing a private 5G network in a factory implies that a large number of small cells need to be erected. The interference of neighboring small cells may increase remarkably, and hence it may cause severe adverse effects on performance of 5G networks. ML and DL can be used for interference alignment, jamming resistance, modulation classification, and physical coding. When the communication spectrum signal is abnormal, ML and DL can also be used to detect the abnormal behavior, so as to maintain the safety and stability of communication devices. In addition, the choice of deploying devices is also a key point to ensure the network stability. Hence, it would be of future interest to apply ML and DL to determine the location of edge and IIoT devices in 5G networks in the factory.

6.2 Future trend for maintaining security in the network layer

AI has been used in maintaining network stability, e.g., network traffic analysis and routing selection. In the IIoT environment using SDN, the convergence of different-scale networks increases the complexity of network resource allocation and control. Therefore, the network stability problems in the SDN-IIoT-based architecture will receive increasing attention. Network slicing is another core technology of 5G. It would be of interest to investigate how to use AI to analyze network resource requirements for dynamic slicing to ensure QoS and network stability. For identifying the types of cyber-attacks, ML has been shown to have good performance. However, because the transmitted data in the IIoT is more heterogeneous, the attack channels are more diversified. Hence, it is much difficult to label all the data from various sources, so that the labelled data is not enough to train a DL model. Therefore, it would be another line of future research to investigate how to integrate ML and transfer learning to address the cyberattack problems in 5G-IIoT factories.

6.3 Future trend for security in the data layer

With the blockchain technology in smart factories, the manufacturing data becomes traceable, and it is easy to control the production process of each product. By analyzing the data through DL and AI, when some problem on the production line occurs, the operators or managers can base the analysis results to find the crux to solve the problem, thereby ensuring the safety and stability of the production line. For data privacy, the blockchain technology can disperse computing and storage requirements in various devices, which not only significantly reduces maintenance costs of data centers, but also effectively prevents the risk of any single node being maliciously manipulated.

6.4 DL and DRL for smart manufacturing applications

DL is mostly used for prediction and classification, and has no specific "action response". DRL uses a Markov decision model to decide the choice of different "actions" based on the state transition model. Therefore, integration of DL and DRL will be adopted in more smart manufacturing applications. For example, DL is used to analyze network traffic, and DRL is used to make decisions on network resource allocation. Another example is that DL is used to detect the type of network attack, and DRL is used to choose the preventive measure for this attack. Aside from security issues, DL and DRL can also be applied in the problems of production lines. DL can predict when a machine will break down and when the machine should be stopped to replace components. DRL can decide a new production scheduling based on states of the production line.

7 Conclusion

This article has provided the architecture of a 5G-IIoT smart factory in three layers, and then discussed the security and privacy issues in the smart factories. Then, recent works for each layer of the 5G-IIoT smart factory were reviewed. Part of the works focused on solutions based on DL which has the powerful self-learning characteristic, and cooperates it with advanced big data analysis techniques to optimize and solve various security issues in 5G-IIoT factories. In addition to DL, this article has also discussed other solutions to 5G-IIoT security issues. Finally, this article provided some future research perspectives for security and privacy issues in 5G-IIoT factories.

Acknowledgements This work has been supported in part by National Science and Technology Council, Taiwan, under Grants NSTC 112-2221-E-A49-116-MY3, NSTC 111-2221-E-A49-081, MOST 109-2221-E-009-068-MY3, MOST 108-2628-E-009-008-MY3, MOST 110-2622-E-A49-004, and MOST 108-2221-E-156-003.

References

1. Lien SY, Hung SC, Deng DJ, Wang YJ (2018) Optimum ultra-reliable and low latency communications in 5G new radio. Mob Networks Appl 23(4):1020–1027
2. Sisinni E, Saifullah A, Han S, Jennehag U, Gidlund M (2018) Industrial internet of things: challenges, opportunities, and directions. IEEE Trans Industr Inf 14(11):4724–4734
3. Gebremichael T, Ledwaba LP, Eldefrawy MH, Hancke GP, Pereira N, Gidlund M, Akerberg J (2020) Security and privacy in the industrial internet of things: current standards and future challenges. IEEE Access 8:152351–152366
4. Vitturi S, Zunino C, Sauter T (2019) Industrial communication systems and their future challenges: next-generation ethernet, IIoT, and 5G. Proc IEEE 107(6):944–961
5. Tange K, De Donno M, Fafoutis X, Dragoni N (2020) A systematic survey of industrial internet of things security: requirements and fog computing opportunities. IEEE Commun Surv Tutorials 22(4):2489–2520
6. Alaba FA, Othman M, Hashem IAT, Alotaibi F (2017) Internet of things security: a survey. J Netw Comput Appl 88:10–28
7. Ogonji MM, Okeyo G, Wafula JM (2020) A survey on privacy and security of internet of things. Comput Sci Rev 38:100312
8. Kouicem DE, Bouabdallah A, Lakhlef H (2018) Internet of things security: a top-down survey. Comput Netw 141:199–221
9. Xu H, Yu W, Griffith D, Golmie N (2018) A survey on industrial internet of things: a cyber-physical systems perspective. IEEE Access 6:78238–78259
10. Al-Naji FH, Zagrouba R (2020) A survey on continuous authentication methods in internet of things environment. Comput Commun 163:109–133
11. Fang H, Qi A, Wang X (2020) Fast authentication and progressive authorization in large-scale IoT: how to leverage AI for security enhancement. IEEE Network 34(3):24–29
12. Zhang Y, Kasahara S, Shen Y, Jiang X, Wan J (2018) Smart contract-based access control for the internet of things. IEEE Internet Things J 6(2):1594–1605
13. Sengupta J, Ruj S, Bit SD (2020) A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. J Netw Comput Appl 149:102481
14. Amiri-Zarandi M, Dara RA, Fraser E (2020) A survey of machine learning-based solutions to protect privacy in the internet of things. Comput Secur 96:101921
15. Eugster P, Kumar S, Savvides S, Stephen JJ (2019) Ensuring confidentiality in the cloud of things. IEEE Pervasive Comput 18(1):10–18
16. Chen YJ, Wang LC, Wang S (2018) Stochastic blockchain for IoT data integrity. IEEE Trans Netw Sci Eng 7(1):373–384
17. Xiong J, Ren J, Chen L, Yao Z, Lin M, Wu D, Niu B (2018) Enhancing privacy and availability for data clustering in intelligent electrical service of IoT. IEEE Internet Things J 6(2):1530–1540
18. Li S, Da Xu L, Zhao S (2018) 5G internet of things: a survey. J Industr Inform Integr 10:1–9
19. Wollschlaeger M, Sauter T, Jasperneite J (2017) The future of industrial communication: automation networks in the era of the internet of things and industry 4.0. IEEE Ind Electron Mag 11(1):17–27
20. Chettri L, Bera R (2019) A comprehensive survey on internet of things (IoT) toward 5G wireless systems. IEEE Internet Things J 7(1):16–32
21. Vo NS, Duong TQ, Guizani M, Kortun A (2018) 5G optimized caching and downlink resource sharing for smart cities. IEEE Access 6:31457–31468
22. Tang Y, Dananjayan S, Hou C, Guo Q, Luo S, He Y (2021) A survey on the 5G network and its impact on agriculture: challenges and opportunities. Comput Electron Agric 180:105895
23. Selem E, Fatehy M, Abd El-Kader SM (2019) E-Health applications over 5G networks: challenges and state of the art. In: Proc. of 2019 6th International Conference on Advanced Control Circuits

and Systems (ACCS) & 2019 5th International Conference on New Paradigms in Electronics & information Technology (PEIT):111–118
24. Rao SK, Prasad R (2018) Impact of 5G technologies on industry 4.0. Wireless Pers Commun 100(1):145–159
25. Bera B, Saha S, Das AK, Kumar N, Lorenz P, Alazab M (2020) Blockchain-envisioned secure data delivery and collection scheme for 5G-based IoT-enabled internet of drones environment. IEEE Trans Veh Technol 69(8):9097–9111
26. Oyekanlu EA, Smith AC, Thomas WP, Mulroy G, Hitesh D, Ramsey M, Sun D (2020) A review of recent advances in automated guided vehicle technologies: integration challenges and research areas for 5G-based smart manufacturing applications. IEEE Access 8:202312–202353
27. Ordonez-Lucena J, Chavarria JF, Contreras LM, Pastor A (2019) The use of 5G non-public networks to support Industry 4.0 scenarios. In: Proc. of 2019 IEEE Conference on Standards for Communications and Networking (CSCN):1–7
28. Khan R, Kumar P, Jayakody DNK, Liyanage M (2019) A survey on security and privacy of 5G technologies: potential solutions, recent advancements, and future directions. IEEE Commun Surv Tutorials 22(1):196–248
29. Ahmad I, Kumar T, Liyanage M, Okwuibe J, Ylianttila M, Gurtov A (2018) Overview of 5G security challenges and solutions. IEEE Commun Stand Mag 2(1):36–43
30. Sicari S, Rizzardi A, Coen-Porisini A (2020) 5G in the internet of things era: an overview on security and privacy challenges. Comput Netw 179:107345
31. Deng DJ, Chen KC, Cheng RS (2014) IEEE 802.11 ax: next generation wireless local area networks. In: Proc. of IEEE 10th International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness:77–82
32. Deng DJ, Gan M, Guo YC, Yu J, Lin YP, Lien SY, Chen KC (2019) IEEE 802.11ba: low-power wake-up radio for green IoT. IEEE Commun Mag 57(7):106–112
33. Deng J, Chang RS (1999) A priority scheme for IEEE 802. 11 DCF access method. IEICE Trans Commun 82(1):96–102
34. Pham TN, Tsai MF, Nguyen DB, Dow CR, Deng DJ (2015) A cloud-based smart-parking system based on internet-of-things technologies. IEEE Access 3:1581–1591
35. Lien SY, Deng DJ, Lin CC, Tsai HL, Chen T, Guo C, Cheng SM (2020) 3GPP NR sidelink transmissions toward 5G V2X. IEEE Access 8:35368–35382
36. Deng DJ, Lin YP, Yang X, Zhu J, Li YB, Luo J, Chen KC (2017) IEEE 802.11ax: highly efficient WLANs for intelligent information infrastructure. IEEE Commun Mag 55(12):52–59
37. Deng DJ, Lien SY, Lee J, Chen KC (2016) On quality-of-service provisioning in IEEE 802.11 ax WLANs. IEEE Access 4:6086–6104
38. Wang K, Qi X, Shu L, Deng DJ, Rodrigues JJPC (2016) Toward trustworthy crowdsourcing in the social internet of things. IEEE Wirel Commun 23(5):30–36
39. Gope P, Sikdar B (2018) Lightweight and privacy-preserving two-factor authentication scheme for IoT devices. IEEE Internet Things J 6(1):580–589
40. Gope P, Das AK, Kumar N, Cheng Y (2019) Lightweight and physically secure anonymous mutual authentication protocol for real-time data access in industrial wireless sensor networks. IEEE Trans Industr Inf 15(9):4957–4968
41. Gu Z, Chen H, Xu P, Li Y, Vucetic B (2020) Physical layer authentication for non-coherent massive SIMO-enabled industrial IoT communications. IEEE Trans Inf Forensics Secur 15:3722–3733
42. Jangirala S, Das AK, Vasilakos AV (2019) Designing secure lightweight blockchain-enabled RFID-based authentication protocol for supply chains in 5G mobile edge computing environment. IEEE Trans Industr Inf 16(11):7081–7093
43. Shen M, Liu H, Zhu L, Xu K, Yu H, Du X, Guizani M (2020) Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE J Sel Areas Commun 38(5):942–954
44. Pan F, Pang Z, Wen H, Luvisotto M, Xiao M, Liao RF, Chen J (2019) Threshold-free physical layer authentication based on machine learning for industrial wireless CPS. IEEE Trans Industr Inf 15(12):6481–6491
45. Chen S, Pang Z, Wen H, Yu K, Zhang T, Lu Y (2020) Automated labeling and learning for physical layer authentication against clone node and sybil attacks in industrial wireless edge networks. IEEE Trans Industr Inf 17(3):2041–2051
46. Han T, Liu C, Wu L, Sarkar S, Jiang D (2019) An adaptive spatiotemporal feature learning approach for fault diagnosis in complex systems. Mech Syst Signal Process 117:170–187
47. Ma S, Chu F (2019) Ensemble deep learning-based fault diagnosis of rotor bearing systems. Comput Ind 105:143–152
48. Wang Y, Pan Z, Yuan X, Yang C, Gui W (2020) A novel deep learning based fault diagnosis approach for chemical process with extended deep belief network. ISA Trans 96:457–467
49. Xu Y, Sun Y, Liu X, Zheng Y (2019) A digital-twin-assisted fault diagnosis using deep transfer learning. IEEE Access 7:19990–19999
50. Naik B, Obaidat MS, Nayak J, Pelusi D, Vijayakumar P, Islam SH (2019) Intelligent secure ecosystem based on Metaheuristic and functional link neural network for edge of things. IEEE Trans Industr Inf 16(3):1947–1956
51. Tian Z, Luo C, Qiu J, Du X, Guizani M (2019) A distributed deep learning system for web attack detection on edge devices. IEEE Trans Industr Inf 16(3):1963–1971
52. Tian Z, Shi W, Wang Y, Zhu C, Du X, Su S, Guizani N (2019) Real-time lateral movement detection based on evidence reasoning network for edge computing environment. IEEE Trans Industr Inf 15(7):4285–4294
53. Yang C, Shi Z, Zhang H, Wu J, Shi X (2019) Multiple attacks detection in cyber-physical systems using random finite set theory. IEEE Trans Cybernetics 50(9):4066–4075
54. Krithivasan K, Pravinraj S, VS SS (2020) Detection of cyberattacks in industrial control systems using enhanced principal component analysis and hypergraph-based convolution neural network (EPCA-HG-CNN). IEEE Trans Ind Appl 56(4):4394–4404
55. Hu Y, Li H, Luan TH, Yang A, Sun L, Wang Z, Wang R (2020) Detecting stealthy attacks on industrial control systems using a permutation entropy-based method. Future Gener Comput Syst 108:1230–1240
56. Wang K, Zhou Y, Liu Z, Shao Z, Luo X, Yang Y (2020) Online task scheduling and resource allocation for intelligent NOMA-based industrial internet of things. IEEE J Sel Areas Commun 38(5):803–815
57. Jie Y, Guo C, Choo KKR, Liu CZ, Li M (2020) Game-theoretic resource allocation for fog-based industrial internet of things environment. IEEE Internet Things J 7(4):3041–3052
58. Wu H, Tian H, Fan S, Ren J (2020) Data age aware scheduling for wireless powered mobile-edge computing in industrial internet of things. IEEE Trans Industr Inf 17(1):398–408
59. Li X, Wan J, Dai HN, Imran M, Xia M, Celesti A (2019) A hybrid computing solution and resource scheduling strategy for edge computing in smart manufacturing. IEEE Trans Industr Inf 5(7):4225–4234
60. Deng S, Xiang Z, Zhao P, Taheri J, Gao H, Yin J, Zomaya AY (2020) Dynamical resource allocation in edge for trustable internet-of-things systems: a reinforcement learning method. IEEE Trans Industr Inf 16(9):6103–6113
61. Zhang G, Chen Y, Shen Z, Wang L (2018) Distributed energy management for multiuser mobile-edge computing systems with energy harvesting devices and QoS constraints. IEEE Internet Things J 6(3):4035–4048

62. Wang J, Jiang C, Zhang K, Hou X, Ren Y, Qian Y (2019) Distributed Q-learning aided heterogeneous network association for energy-efficient IIoT. IEEE Trans Industr Inf 16(4):2756–2764
63. Wan J, Yang J, Wang S, Li D, Li P, Xia M (2019) Cross-network fusion and scheduling for heterogeneous networks in smart factory. IEEE Trans Industr Inf 16(9):6059–6068
64. Wang X, Chai L, Zhou Y, Dan F (2021) Dual-network task scheduling in cyber-physical systems: a co-optimization approach. IEEE Trans Industr Inf 17(5):3143–3152
65. Huang V, Chen G, Zhang P, Li H, Hu C, Pan T, Fu Q (2020) A scalable approach to SDN control plane management: high utilization comes with low latency. IEEE Trans Netw Serv Manage 17(2):682–695
66. Li J, Shi W, Zhang N, Shen X (2021) Delay-aware VNF scheduling: a reinforcement learning approach with variable action set. IEEE Trans Cogn Commun Netw 7(1):304–318
67. Messaoud S, Bradai A, Moulay E (2019) Online GMM clustering and mini-batch gradient descent based optimization for industrial IoT 4.0. IEEE Trans Industr Inf 16(2):1427–1435
68. Xiang H, Yan S, Peng M (2020) A realization of fog-RAN slicing via deep reinforcement learning. IEEE Trans Wireless Commun 19(4):2515–2527
69. Qu K, Zhuang W, Ye Q, Shen X, Li X, Rao J (2020) Dynamic flow migration for embedded services in SDN/NFV-enabled 5G core networks. IEEE Trans Commun 68(4):2394–2408
70. Estrada-Solano F, Caicedo OM, Da Fonseca NL (2019) Nelly: flow detection using incremental learning at the server side of SDN-based data centers. IEEE Trans Industr Inf 16(2):1362–1372
71. Ravi N, Shalinie SM (2020) Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture. IEEE Internet Things J 7(4):3559–3570
72. Fang L, Zhao B, Li Y, Liu Z, Ge C, Meng W (2020) Countermeasure based on smart contracts and AI against DoS/DDoS attack in 5G circumstances. IEEE Network 34(6):54–61
73. Hassan MM, Gumaei A, Huda S, Almogren A (2020) Increasing the trustworthiness in the industrial IoT networks through a reliable cyberattack detection model. IEEE Trans Industr Inf 16(9):6154–6162
74. Saharkhizan M, Azmoodeh A, Dehghantanha A, Choo KKR, Parizi RM (2020) An ensemble of deep recurrent neural networks for detecting IoT cyber attacks using network traffic. IEEE Internet Things J 7(9):8852–8859
75. Maimó LF, Celdrán AH, Pérez MG, Clemente FJG, Pérez GM (2019) Dynamic management of a deep learning-based anomaly detection system for 5G networks. J Ambient Intell Humaniz Comput 10(8):3083–3097
76. Wang N, Li W, Alipour-Fanid A, Jiao L, Dabaghchian M, Zeng K (2020) Pilot contamination attack detection for 5G MmWave grant-free IoT networks. IEEE Trans Inf Forensics Secur 16:658–670
77. Chattopadhyay A, Mitra U (2019) Security against false data-injection attack in cyber-physical systems. IEEE Trans Control Netw Syst 7(2):1015–1027
78. Hussain B, Du Q, Sun B, Han Z (2021) Deep learning-based DDoS-attack detection for cyber-physical system over 5G network. IEEE Trans Industr Inf 17(2):860–870
79. Diro AA, Chilamkurti N (2017) Distributed attack detection scheme using deep learning approach for internet of things. Future Gener Comput Syst 82:761–768
80. Dai Y, Xu D, Maharjan S, Chen Z, He Q, Zhang Y (2019) Blockchain and deep reinforcement learning empowered intelligent 5G beyond. IEEE Network 33(3):10–17
81. Rezvy S, Luo Y, Petridis M, Lasebae A, Zebin T (2019) An efficient deep learning model for intrusion classification and prediction in 5G and IoT networks. In: Proc. of 2019 53rd Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, pp 1–6
82. Qi S, Lu Y, Wei W, Chen X (2020) Efficient data access control with fine-grained data protection in cloud-assisted IIoT. IEEE Internet Things J 8(4):2886–2899
83. Xiong S, Ni Q, Wang L, Wang Q (2020) SEM-ACSIT: secure and efficient multiauthority access control for IoT cloud storage. IEEE Internet Things J 7(4):2914–2927
84. Huang J, Kong L, Chen G, Wu MY, Liu X, Zeng P (2019) Towards secure industrial IoT: blockchain system with credit-based consensus mechanism. IEEE Trans Industr Inf 15(6):3680–3689
85. Wu D, Ansari N (2020) A trust evaluation enhanced blockchain-secured industrial IoT system. IEEE Internet Things J 8(7):5510–5517
86. Castiglione A, Nappi M, Ricciardi S (2020) Trustworthy method for person identification in IIoT environments by means of facial dynamics. IEEE Trans Industr Inf 17(2):766–774
87. Das AK, Wazid M, Kumar N, Vasilakos AV, Rodrigues JJ (2018) Biometrics-based privacy-preserving user authentication scheme for cloud-based industrial internet of things deployment. IEEE Internet Things J 5(6):4900–4913
88. Wan J, Li J, Imran M, Li D (2019) A blockchain-based solution for enhancing security and privacy in smart factory. IEEE Trans Industr Inf 15(6):3652–3660
89. Usman M, Jan MA, Jolfaei A, Xu M, He X, Chen J (2019) A distributed and anonymous data collection framework based on multilevel edge computing architecture. IEEE Trans Industr Inf 16(9):6114–6123
90. Lu Y, Huang X, Dai Y, Maharjan S, Zhang Y (2019) Blockchain and federated learning for privacy-preserved data sharing in industrial IoT. IEEE Trans Industr Inf 16(6):4177–4186
91. Zaghloul E, Zhou K, Ren J (2019) P-mod: secure privilege-based multilevel organizational data-sharing in cloud computing. IEEE Trans Big Data 6(4):804–815
92. Qi S, Lu Y, Zheng Y, Li Y, Chen X (2020) Cpds: enabling compressed and private data sharing for industrial internet of things over blockchain. IEEE Trans Industr Inf 17(4):2376–2387
93. Zhou R, Zhang X, Du X, Wang X, Yang G, Guizani M (2018) File-centric multi-key aggregate keyword searchable encryption for industrial internet of things. IEEE Trans Industr Inf 14(8):3648–3658
94. Xu G, Li H, Dai Y, Yang K, Lin X (2018) Enabling efficient and geometric range query with access control over encrypted spatial data. IEEE Trans Inf Forensics Secur 14(4):870–885
95. Lu Y, Li J, Wang F (2020) Pairing-free certificate-based searchable encryption supporting privacy-preserving keyword search function for IIoTs. IEEE Trans Industr Inf 17(4):2696–2706
96. Liu S, Yu J, Xiao Y, Wan Z, Wang S, Yan B (2020) BC-SABE: blockchain-aided searchable attribute-based encryption for cloud-IoT. IEEE Internet Things J 7(9):7851–7867
97. Hao J, Liu J, Wu W, Tang F, Xian M (2019) Secure and fine-grained self-controlled outsourced data deletion in cloud-based IoT. IEEE Internet Things J 7(2):1140–1153
98. Xue L, Yu Y, Li Y, Au MH, Du X, Yang B (2019) Efficient attribute-based encryption with attribute revocation for assured data deletion. Inf Sci 479:640–650