Edge Computing in Industrial Internet of Things: Architecture, Advances and Challenges

Tie Qiu, *Senior Member, IEEE*, Jiancheng Chi, Xiaobo Zhou, *Senior Member, IEEE*, Zhaolong Ning, *Senior Member, IEEE*, Mohammed Atiquzzaman, *Senior Member, IEEE*, and Dapeng Oliver Wu, *Fellow, IEEE*

***Abstract*—The Industrial Internet of Things (IIoT) is a crucial research field spawned by the Internet of Things (IoT). IIoT links all types of industrial equipment through the network; establishes data acquisition, exchange, and analysis systems; and optimizes processes and services, so as to reduce cost and enhance productivity. The introduction of edge computing in IIoT can significantly reduce the decision-making latency, save bandwidth resources, and to some extent, protect privacy. This paper outlines the research progress concerning edge computing in IIoT. First, the concepts of IIoT and edge computing are discussed, and subsequently, the research progress of edge computing is discussed and summarized in detail. Next, the future architecture from the perspective of edge computing in IIoT is proposed, and its technical progress in routing, task scheduling, data storage and analytics, security, and standardization is analyzed. Furthermore, we discuss the opportunities and challenges of edge computing in IIoT in terms of 5G-based edge communication, load balancing and data offloading, edge intelligence, as well as data sharing security. Finally, we introduce some typical application scenarios of edge computing in IIoT, such as prognostics and health management (PHM), smart grids, manufacturing coordination, intelligent connected vehicles (ICV), and smart logistics.**

***Index Terms*—Industrial Internet of Things (IIoT), edge computing, reference architecture, advances and challenges, application scenarios.**

I. Introduction

The INTERNET of Things (IoT) is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols, making all things communicate with each other, and realizing information sharing and collaborative decision-making [1]. In IoT, all kinds of things with independent address or identity are interconnected through heterogeneous transmission networks to realize dynamic information interaction. The application of IoT to the industrial field has spawned a new research area called the Industrial Internet of Things (IIoT). IIoT is a new service-oriented industrial ecosystem using the network interconnection of industrial resources, data interoperability, and system interoperability to enable flexible resource allocation, on-demand execution of processes, rational optimization of processes, and rapid adaptation of environments [2]. IIoT abstracts industrial processes into data types, turns devices into data terminals, collects underlying basic data in all directions, and combines the powerful data storage and computing functions of cloud computing to perform deeper data analysis and mining to improve efficiency and optimize operations. Its deployment will introduce profound changes to the production, operation, and management modes of industry, laying a solid foundation for the rational allocation of supply chain resources and improvements in production and service efficiency.

Manuscript received September 30, 2019; revised February 5, 2020 and May 24, 2020; accepted June 30, 2020. Date of publication July 14, 2020; date of current version November 20, 2020. This work was supported in part by the National Key Research and Development Program of China under Grant 2019YFB1703601; and in part by National Natural Science Foundation of China under Grant 61672131, Grant 61971084, and Grant 61702365. *(Corresponding author: Xiaobo Zhou; Zhaolong Ning.)*

Tie Qiu, Jiancheng Chi, and Xiaobo Zhou are with the School of Computer Science and Technology, College of Intelligence and Computing, Tianjin University, Tianjin 300350, China, and also with the Tianjin Key Laboratory of Advanced Networking, Tianjin 300350, China (e-mail: qiutie@ieee.org; chijiancheng@tju.edu.cn; xiaobo.zhou@tju.edu.cn).

Zhaolong Ning is with the School of Software, Dalian University of Technology, Dalian 116620, China (e-mail: zhaolongning@dlut.edu.cn).

Mohammed Atiquzzaman is with the School of Computer Science, University of Oklahoma, Norman, OK 73019 USA (e-mail: atiq@ou.edu).

Dapeng Oliver Wu is with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611 USA (e-mail: dpwu@ieee.org).

Digital Object Identifier 10.1109/COMST.2020.3009103

A. IIoT and Related Concepts

IoT and IIoT have their respective focuses on concepts and practical application scenarios although the IIoT is derived from the IoT. The IoT widely accepted by people is mainly consumption-oriented and aims to improve people's life quality. The most typical application scenarios of IoT are smart home, health monitoring and indoor localization, *etc* [3]. The IIoT is production-oriented and aims to improve industrial production efficiency. Typical application scenarios of IIoT include smart logistics, remote maintenance and intelligent factories [4]. The system frameworks of different IoT application scenarios generally need to be built from scratch, and the deployment scale of sensors is relatively small with low precision requirements [2]. However, the system frameworks of IIoT application scenarios are built based on traditional industrial infrastructure, so the deployment scale of sensors is very large with high precision requirements. For the IoT, devices generally have strong mobility, generate medium data volume and have high tolerance for delay; while for the IIoT, most of the devices are fixed in position, generate great amount of perceived data and have low tolerance for delay. Table I gives a qualitative comparison of IoT and IIoT.

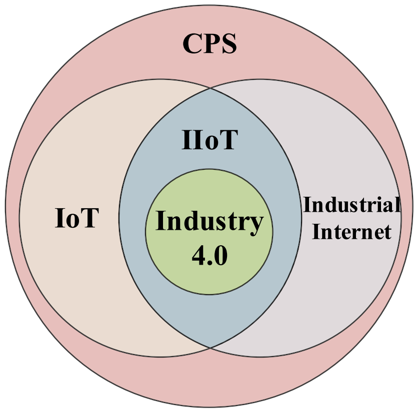

Fig. 1. CPS, IoT, Industrial Internet, IIoT and Industry 4.0 in venn diagram.

The concept of IIoT is closely related to some widely accepted concepts, such as cyber-physical systems (CPS), IoT, the Industrial Internet, and Industry 4.0. CPS, proposed by Helen Gill in 2006, emphasizes the deep integration of various information technologies, such as sensing technology, embedded technology, and software & hardware technology, aiming to achieve the highly synergistic and autonomous informationization capabilities, real-time and flexible feedback, and positive cycle between the physical and information worlds. As a subset of CPS, IoT mainly emphasizes the interactions between objects through the Internet based on unique identifications. The globalization, openness, interoperability, and socialization of the Internet provide the basis for supporting the IoT concept. The Industrial Internet, proposed by the Industrial Internet Consortium (IIC) launched by the top five companies in the US, namely GE, AT&T, IBM, Intel, and Cisco, mainly focuses on the construction, application, and standardization of innovative networks, the enhancement of data circulation, and the digital transformation of the whole industrial field. The sub-concept of IIoT called Industry 4.0 launched in Germany is a globally oriented, artificial intelligence-based information CPS, essentially in the smart manufacturing field. In summary, CPS provides a blueprint for the relationship between the physical world and information world based on the interconnection of things, so CPS represents the broadest of the concepts mentioned above. IoT highlights the interconnections among objects through physical addresses, regardless of whether they are industry or civilian oriented, while the Industrial Internet portrays the potential future trends of industries based on emerging technologies. In this sense, IoT and the Industrial Internet are subsets of CPS [5], [6]. Meanwhile, IoT and the Industrial Internet intersect, and this intersection is called IIoT. Moreover, Industry 4.0 is a subset of IIoT, which concerns manufacturing. The relationships between IIoT, IoT, CPS, Industry 4.0, and the Industrial Internet are shown in Figure 1.

B. Deploying Edge Computing in IIoT

The IIoT system consists of a large number of heterogeneous node devices, interconnected through heterogeneous wired and wireless networks. The heterogeneous networks include sensor networks, wireless Wi-Fi networks, mobile communication 3G/4G/LTE/5G networks and dedicated industrial buses [12]. A large number of distributed heterogeneous industrial devices form an edge network, collecting industrial data in real time and transmitting it to the cloud server for computing and control. With the development of IIoT, the scale of such networks is becoming larger, and traditional cloud data center networks struggle to satisfy the real-time, security, and reliability requirements of IIoT for massive data transmission and processing. For example, in a smart factory, a large number of production devices collect a large of sensory data, sometimes the data volume gets the level of GB per second [13]. If all the data are uploaded to the cloud platform for processing, too much bandwidth resources will be consumed, the operation cost will be high, and the overall delay of data processing will also increase. In the intelligent connected vehicles scenario, the task is sensitive to delay due to the high speed of vehicles. If the information collected by vehicles is handed over to the cloud platform for processing and making decisions, the effective time phase of information may be missed all the time [14]. In some time-sensitive tasks, such as emergency shutdown of equipment in smart factory and emergency braking of smart connected vehicles, data transmission to the cloud platform for processing and then back will causes more serious consequences. Therefore, offloading some data from IIoT cloud data centers to edge networks is an important research solution for the above problems, which is called edge computing. Edge computing is gradually applied in some IIoT scenarios (e.g., remote equipment monitoring [15]–[17], predictive maintenance [18], and quality control [19]).

TABLE I
A QUALITATIVE COMPARISON OF IOT AND IIOT

Features	IoT	IIoT
Objective	Consumption-oriented and improving life quality [1], [7], [8]	Production-oriented and promoting efficiency [4], [9]–[11]
Application Scenarios	Indoor localization, health monitoring, smart home [1], [3], [7], [8]	Smart logistics, remote monitoring,smart factory [4], [9]–[11]
Platform Foundation	Self-building [1], [7]	Based on industrial facilities [4], [9]
Sensors Scale	Small to medium [1], [7]	Large to very large [9]
Precision Requirement	Low to medium [1], [7], [8]	High to very high [4], [9]
Mobility	Strong [1], [7]	Weak [4], [9]
Data Volume	Medium to high [1], [7], [8]	High to very high [4], [9]–[11]
Latency Tolerance	High [1], [7]	Very low [4], [9]

Edge computing refers to a new computing model that analyzes and processes a portion of data using the computing, storage, and network resources distributed on the paths between data sources and the cloud computing center [20]. Edge computing uses edge devices with sufficient computing power to implement local preprocessing of source data, make some immediate decisions, and upload computing results or preprocessed data to the cloud computing center. The main advantages of edge computing applied to the IIoT are as follows:

- *Improve System Performance:* In addition to collecting and transmitting data to the cloud platform, the most important thing edge computing in IIoT has done is to achieve *ms* level of data processing. It's efficient to reduce the overall delay of the system, reduce the demand for communication bandwidth, and improve the overall performance of the system.
- *Protect Data Security and Privacy:* Cloud platform service providers give customers comprehensive system of centralized data security protection solutions. However, once centralizing stored data get leaked, it will lead to serious consequences. Edge computing in IIoT allows enterprises to deploy the most appropriate security solutions in the local vicinity, reducing the risk of data leakage during transmission and the data volume stored in the cloud platform, so as to minimize security and privacy risks.
- *Reduce Operational Costs:* When data is transferred directly to the cloud platform, data migration, good bandwidth and delay characteristics require a lot of operational costs. Edge computing in IIoT can reduce data uploading volume, thereby reducing data migration volume, bandwidth consumption and latency, so as to reduce operational costs.

C. Motivation and Paper Organization

In order to provide a comprehensive and systematic understanding, this paper focuses on edge computing in IIoT and combs through many research achievements concerning edge computing in IIoT, discussing the architecture, advances, challenges and applications of edge computing in IIoT. This is undertaken to offer some help in clarifying the relationship between IIoT and edge computing and promoting the further development and integration of the two. More importantly, we provide a significant reference for follow-up researchers, designers, and beginners.

The remainder of this paper is structured as follows. Section II summarizes the concepts and surveys related to edge computing. The reference architecture of edge computing in IIoT is proposed in Section III. Section IV reviews the research progress concerning edge computing in IIoT. Then, Section V discusses the challenges and opportunities in the development of edge computing in IIoT. Furthermore, Section VI introduces some applications of edge computing in IIoT. Finally, a conclusion is provided in Section VII.

II. Related Advances and Surveys of Edge Computing

Following an investigating, we find that there is only a few of surveys discussing the current status of edge computing in IIoT because it has not be mature although attracted too many people's attention. Therefore, in this section, we firstly summary existing edge computing surveys involving many research directions (e.g., fog computing, mobile edge computing (MEC), edge networking, edge security), and provide a overview and comparison of the surveys related to edge computing in IIoT. This will demonstrate the developing processes of edge computing, aid in understanding the evolution of edge computing in IIoT and verify the innovation of our work.

TABLE II
Comparison of Fog Computing and Edge Computing

Features	Fog Computing	Edge Computing
Network Access	Mostly LAN [25]	LAN/WLAN [23]
Mobility Support	Low [25], [26]	High [23]
Latency	Low [25]–[27]	Low or very low, depending on layers [24]
Scalability of Servers	Distributed and low [25]–[27]	Distributed and high [24]
Computing Power Location	Infrastructure between cloud and terminals [25]–[27]	All computing resources except cloud [23], [24], [28]–[30]
Distribution	Distributed [25]–[27]	Widely distributed [23], [24], [28]
Reliability	High [26], [27]	Low [29], [30]
Deployment cost	Very low [26]	Low [30]
Maintenance	Experts of enterprise [25]	Expert, engineers and employees of enterprise [30]
Standardization	Yes [27]	No [29], [30]

A. Fog Computing

Fog computing is a similar concept to edge computing, which was introduced by Cisco in 2012 [21]. Vaquero and Rodero-Merino defined fog computing as a new computing model that migrates tasks from the cloud computing center to light servers near to devices by introducing a fog layer, which consists of some servers deployed between the cloud platform and edge devices [22]. The core idea of fog computing and edge computing is to make data processing closer to the data source, shorten the latency of some decisions, and reduce the network transmission load. However, fog computing focuses on the infrastructure between edge devices and cloud platform, while edge computing focuses not only on the infrastructure that fog computing cared, but also on the edge devices with enormous quantities. Therefore, we believe that fog computing is a subset of edge computing. A comparison between fog computing and edge computing is presented in Table II, based on [23], [24].

Some surveys have summarized the research on fog computing. For instance, Naha *et al.* [26] summarized the concepts, definitions, research trends, and architectures of fog computing; discussed the differences and limitations of existing research directions in resource allocation and scheduling; and proposed some personal opinions on these limitations. Mouradian *et al.* [27] conducted a comprehensive survey of fog computing; reviewed the current technological situation, including fog system architecture, algorithms, research challenges, and research directions; and prospected the key role that fog may play in emerging technologies such as the Tactile Internet. Mukherjee *et al.* [25] described the overview and foundation of the fog computing architecture; summarized the main research on service and resource allocation methods and networks; and highlighted ongoing research work, open challenges, and research trends in the field of fog computing.

B. MEC

MEC was proposed by the European Telecommunications Standards Institute (ETSI). The basic idea of MEC is to migrate some requests and tasks from mobile core network to the mobile access network, achieving the efficient usage of computing and storage resources. This concept deeply integrates the traditional telecom cellular network with the Internet service, aiming to reduce the end-to-end delay of mobile service delivery and explore the inherent capabilities of the wireless network, thereby enhancing the user experience, introducing new changes in the operation modes of the telecom operator, and establishing a new industrial chain and network ecosystem. In 2017, the ETSI extended the concept of MEC from telecom cellular networks to other access networks, such as Wi-Fi and fixed access, which is called multi-access edge computing. Therefore, MEC has become the abbreviation of multi-access edge computing since 2017 and has been widely accepted by researchers.

Many surveys are available of research on MEC. Taleb *et al.* [28] introduced an overview of research on MEC and the key technologies for implementing MEC, analyzed the MEC reference architecture and main deployment scenarios, and expounded the current standardization work and challenges of open research. Porambage *et al.* [29] provided a comprehensive overview of the use of MEC technology to implement IoT applications and their synergies, discussed the technical aspects of enabling MEC in IoT, and provided some insights into various integration technologies. Moura and Hutchison [31] investigated the main challenges of MEC services for wireless resources based on classic and evolutionary games, discussed some specific factors affecting the performance of game theory and how to balance the above factors to achieve a performance-cost balance in realistic edge network scenarios, and prospected future trends and research directions in the application of game theory in future MEC services. Giust *et al.* [32] provided an in-depth interpretation of the MEC technologies specified and researched by the ETSI Industry Specification Group, by demonstrating automotive use cases related to MEC.

C. Edge Networking

The developmental trend of edge computing networks involves multi-technology convergence, and the integration with advanced network technologies such as software defined networks (SDN), network function virtualization (NFV), and the fifth generation (5G) cellular network technology has become mainstream.

SDN liberates the forwarding device from the routing management task and performs this separately on the logically centralized control plane, which simplifies the process of network control and configuration, adds many functions to the network by introducing virtualized components, and achieves reflecting control. The idea of separating the plane from the data-forwarding plane promotes the development of virtualized networks. NFV separates the software and hardware of a traditional network, virtualizes network functions, and realizes the sharing of network hardware resources, which facilitates the rapid deployment of network functions and flexible allocation of service capacities on demand. 5G is a combination of emerging commercially available communication technologies, such as micro-base-station, massive MIMO, and beamforming technologies [33]. In the 5G era, we will have faster transmission rates, lower latencies, larger capacity base stations, and a better quality of service (QoS).

Lingen *et al.* [34] argued that NFV and 5G convergence is a trend, and fog computing will be part of this convergence. Furthermore, they introduced an open and converged architecture based on MANO, which provides unified management of IoT services from the cloud to edge continuum. Baktir *et al.* [23] believed that SDN can serve as an enabler to reduce the complexity of edge computing and realize its true potential. They discussed the functionality of SDN, combined this with the technical flaws of edge computing implementations, proposed a clear SDN-EDGE computing interaction collaboration model, proved that SDN-related mechanisms can run effectively in the edge-computing infrastructure, and described the future directions of SDN development to ensure the effective integration of edge computing and SDN. Cziva and Pezaros [35] developed a container-based NFV platform, to tackle the problem that traditional NFV is difficult to deploy at the edge of a network, and demonstrated the effectiveness of the platform in saving core network utilization and reducing latency through three use cases, confirming the opportunity for virtualization at the edge of the network. Huang *et al.* [36] proposed a 5G-supported software-defined vehicle network (5G-SDVN) for the future development of intelligent networked vehicles, and used mobile edge computing to enhance the network control of 5G-SDVN, establishing a programmable, flexible, and controllable 5G-SDVN network structure. They used a case study of automotive cloud computing to demonstrate the advantages of 5G-SDVN to simplify network management and improve resource utilization and discussed open problems in 5G-SDVN.

D. Edge Security

Edge computing allows some data to be processed and filtered at the data source, reducing the total amount of data transmission, and also avoiding the possibility of data theft and privacy leakage by avoiding the forwarding and transmission of data. Therefore, edge computing has the natural feature of reducing data leakage and protecting data privacy. Despite this, edge computing still faces some serious security and privacy issues, such as edge nodes, edge servers, or edge networks being attacked and the leakage of private data owing to the access rights of the edge computing system or the unreasonable design of the encrypted transmission protocol.

Because a series of researchers have conducted long-term explorations of the security problems in edge computing, achieving some progress, relevant review papers are reasonably common. Zhang *et al.* [37] outlined the basic definition and architecture of edge computing; analyzed the data security and privacy requirements, challenges, and mechanisms in detail; summarized techniques based on cryptography for solving the data security and privacy issues; investigated the edge correlation paradigm of the most advanced data security and privacy solutions; and proposed several open research directions for data security in the field of edge computing. Ni *et al.* [38] introduced the overall architecture and several promising edge-assisted IoT applications; studied the security, privacy, and efficiency challenges of mobile edge computing in data processing; discussed opportunities to improve the computational efficiency of data security in IoT with the help of edge computing in secure data aggregation, secure data deduplication, and secure computational offloading; and presented several interesting research directions for edge-enhanced data analysis. Guan *et al.* [39] discussed the design of data security and privacy in fog computing, pointed the reasons why the data protection scheme fitting in cloud computing doesn't suitable in fog computing, and proposed some data security and privacy design challenges introduced by fog computing.

E. Edge Computing in IIoT

Edge computing in IIoT is in the ascendant stage at present, and there are a lot of relevant researches. However, according to investigating, only a few surveys are talking about edge computing in IIoT due to its development stage.

Some surveys related to edge computing in IIoT just considered a small part of research scopes. For instance, Georgakopoulos *et al.* [42] introduced Internet of Things and edge cloud computing roadmap for manufacturing; Seitz *et al.* [43] presented two case studies which show the applicability of the fog paradigm for IIoT applications. Sitton-Candanedo *et al.* [30] introduced the main existing edge computing reference architectures aimed at Industry 4.0 proposed by different consortiums and made a comparison among these reference architectures. Steiner and Poledna [44] proposed fog computing as an architectural way to implement IIoT, and discussed technologies that support fog computing. To some extent, some topics related to edge computing in IIoT are pointed out by these surveys. However, they are too short to make a complete and systematic introduction. Therefore, these surveys are not listed in the summary table of edge computing in IIoT.

Some surveys related to edge computing in IIoT covered necessary topics relatively, but the depth of discussion is still insufficient. For example, Aazam *et al.* [40] introduced the architecture of IIoT and industry 4.0, discussed how fog provided computing support in an IIoT environment, as well as some use cases and emerging research challenges. However, it didn't discuss the relevant advanced technologies, and the discussion of challenges and application scenarios is also too simple. Basir *et al.* [41] discussed the history of industrial revolution and key technologies as the basis of industrial transformation, focused on fog computing and discussed key challenges and the applications of fog computing in different domains. However, the paper is more closely related to IIoT rather than edge computing, and it just focused on communication and network when introducing advanced technologies and challenges, so it's not comprehensive enough. A summary and comparison of relatively surveys of edge computing are shown in Table III.

III. REFERENCE ARCHITECTURE OF EDGE COMPUTING IN IIoT

A reference architecture is a comprehensive model of high-level abstraction for a certain type of technology, which is used to guide the design of a software system suitable for different application scenarios. At present, integrating edge computing into IIoT will be an inevitable trend in the future. In this section, a reference architecture of edge computing in IIoT is proposed based on the existing reference architectures.

A. Existing Reference Architectures

Architectures are usually proposed based on the technical, business, and service requirements of a particular scenario, to determine the number and functionality of layers. Edge computing does not form a unified standard reference architecture, as it is currently a burgeoning technology. However, as a subset of edge computing, fog computing has many proposed reference architectures based on the standardization works by OpenFog, and the reference architecture viewpoints for fog computing are tending to become unified. Therefore, fog computing architecture can be used as a starting point to explore the future architecture of edge computing in iioT. Most researchers believe that the reference architecture for fog computing can be divided into three layers, which can be named the equipment layer, fog layer, and cloud layer; IoT layer, fog computing layer, and cloud computing layer [27]; or things/end-devices layer, fog layer, and cloud layer [25]. Although the names of the three layers vary, the functions of each layer are relatively similar. In general, the first layer is composed of terminal equipment with a sensing ability, which is responsible for collecting the required data. The second layer consists of various devices that transmit information to the cloud channel, and is responsible for processing part of the data. The third layer, composed of cloud-computing resources, is responsible for mass data processing and decision-making.

A basic understanding of the IIoT architecture is also required in order to integrate edge computing into IIoT. For IIoT, a typical reference architecture has three layers: the physical layer, communication layer, and application layer [9]. Alternatively, a service layer can be added between the communication and application layers of a three-tier architecture to form a four-tier architecture [45]. For some specific IIoT industries, reference architectures typically require customization and further complexity, such as the standardized architecture for Industry 4.0 [46].

Although the fog computing and IIoT reference architectures are relatively mature and unified, there is little research focusing on the reference architecture of edge computing in IIoT because edge computing in IIoT is an emerging research field. Some papers have been trying to discuss the reference architecture of edge computing in IIoT. For instance,

TABLE III
A SUMMARY OF RELATIVELY SURVEYS OF EDGE COMPUTING

Aspect	Ref.	Main Contribution	Relavance to Edge Computing in IIoT
Fog Computing	[26]	An overview of architectures, taxonomy, existing research works (e.g., resource allocation and scheduling, fault tolerance, simulation tools, and Fog-based microservices), open issues and future research directions for fog computing.	Discussed the relationship of fog computing and IoT and how to use it, but didn't focus on edge computing in IIoT specifically.
	[25]	A comprehensive survey on the state of the art, architectures, algorithms, challenges and research directions, lessons learned and prospects of fog computing.	Discussed how to combine fog computing with IoT, but no explicit focus on edge computing in IIoT.
	[27]	A survey of architecture, state of the art, applications and major research aspects, open challenges and research trends in fog computing.	No explicit focus on edge computing in IIoT.
MEC	[28]	A comprehensive survey on key enabling technologies, reference architecture, deployment scenarios, standardization activities and open research challenges for MEC.	No explicit focus on edge computing in IIoT.
	[29]	A holistic overview on the exploitation of MEC technology for the realization of IoT applications and their synergies.	Discussed the vital role MEC will played in enabling future IIoT applications briefly.
	[31]	A presentation of the literature, use cases, models, lessons learned, , major challenges, future trends and research directions for applying theoretical model games in MEC services.	Discussed the fog computing architecture based on IoT architecture, but no explicit focus on edge computing in IIoT.
	[32]	A discussion of the MEC-relevant automotive use cases and the technologies specified and investigated by the ETSI Industry Specification Group MEC.	Disscussed a typical application scenario of edge computing in IIoT.
Edge Networking	[34]	An elaboration of architecture based on MANO, models and the application of models for the combination of NFV, 5G, and fog computing.	No explicit focus on edge computing in IIoT.
	[23]	A comparative discussion of approaches and technologies, capabilities, possible modes and future directions for the SDN.	Discussed IoT and wireless sensor networks (WSN) that can be learnt to deploy IIoT networks, but no explicit focus on edge computing in IIoT.
	[35]	A discussion of the opportunities of virtualization at the network edge, a container-based NFV platform that runs and orchestrates lightweight container VNFs, and three useful examples of the platform.	Discussed the role IIoT gateways played at edge networking.
	[36]	An investigation of 5G-enabled software defined vehicular networks (5G-SDVNs), the network architecture combining software defined networking with mobile edge computing, case studies of vehicular cloud computing, and some open issues in 5G-SDVN.	Disscussed a typical application scenario of edge computing in IIoT.
Edge Security	[37]	A comprehensive analysis of the data security and privacy threats, protection technologies, countermeasures and pen research directions inherent in edge computing.	Discussed security issues and solutions for edge IoT devices.
	[38]	An overview of architecture, applications, efficiency challenges, opportunities and interesting directions on edge-empowered IoT data analysis.	Discussed some typical security solutions for edge-empowered IoT that can be used in edge computing in IIoT.
	[39]	A discussion of the design issues for data security and privacy in fog computing.	No explicit focus on edge computing in IIoT.
Edge Computing in IIoT	[40]	An overview of the architecture of IIoT and industry 4.0, fog computing approach to providing local computing support, the core elements and building blocks of IIoT, and some of the emerging research challenges associated with IIoT.	Discussed how to deploy fog computing in IIoT.
	[41]	A review of the application areas of IIoT, key technologies under industry transformation, and fog computing's solutions to key challenges.	Discussed the prospects and technical challenges of deploying fog computing in IIoT.

Aazam *et al.* [40] introduced the fog-based IIoT reference architecture briefly, which include device layer, fog layer and cloud layer; Sitton-Candanedo *et al.* [30] discussed the edge computing reference architecture for industry 4.0. However, these architectures only introduced a few layers roughly and did not discuss each layer in depth with the characteristics of IIoT. In addition, with the gradual integration of edge computing into IIoT, some obvious trends should also be considered in order to make the reference architecture of edge computing in IIoT more reasonable and practical, such as the computing power of equipment in the fog layer in traditional fog computing reference architecture sometimes varies by several orders of magnitude, which was always neglected by existing reference architectures.

B. Proposed Reference Architecture of Edge Computing in IIoT

The edge computing in IIoT is focusing on deploying edge computing into different IIoT scenarios to reduce network traffic and decision-making delay. Therefore, the reference architecture of edge computing in IIoT needs to be improved and refined from the existing edge computing reference architectures. Meanwhile, it also needs to consider the characteristics of edge computing and IIoT comprehensively. In view of the above considerations, this paper proposes the reference architecture of edge computing in IIoT as shown in Figure 2. The proposed reference architecture is composed of three layers, namely the Device Layer, the Edge Layer and the Cloud Application Layer, which are derived from the existing edge computing reference architectures. Different from the existing edge computing reference architectures discussed in previous papers, the proposed reference architecture in this paper comprehensively considers the characteristics of IIoT and edge computing, focusing on what functions each layer should have and how layers communicate with each other in detail.

1) Device Layer: The Device Layer includes all kinds of sensors, handheld terminals, instruments and meters, smart machines, smart vehicles, robots and other devices or equipment. By various types of wired networks (Fieldbus, Industrial Ethernet, Industrial Optical Fiber, *etc.*) or wireless networks (Wi-Fi, Bluetooth, RFID, NB-IoT, LoRa, 5G, *etc.*), these devices or equipment collect a large amount of parameter data by all kinds of sensors, transmit to the Edge Layer and wait

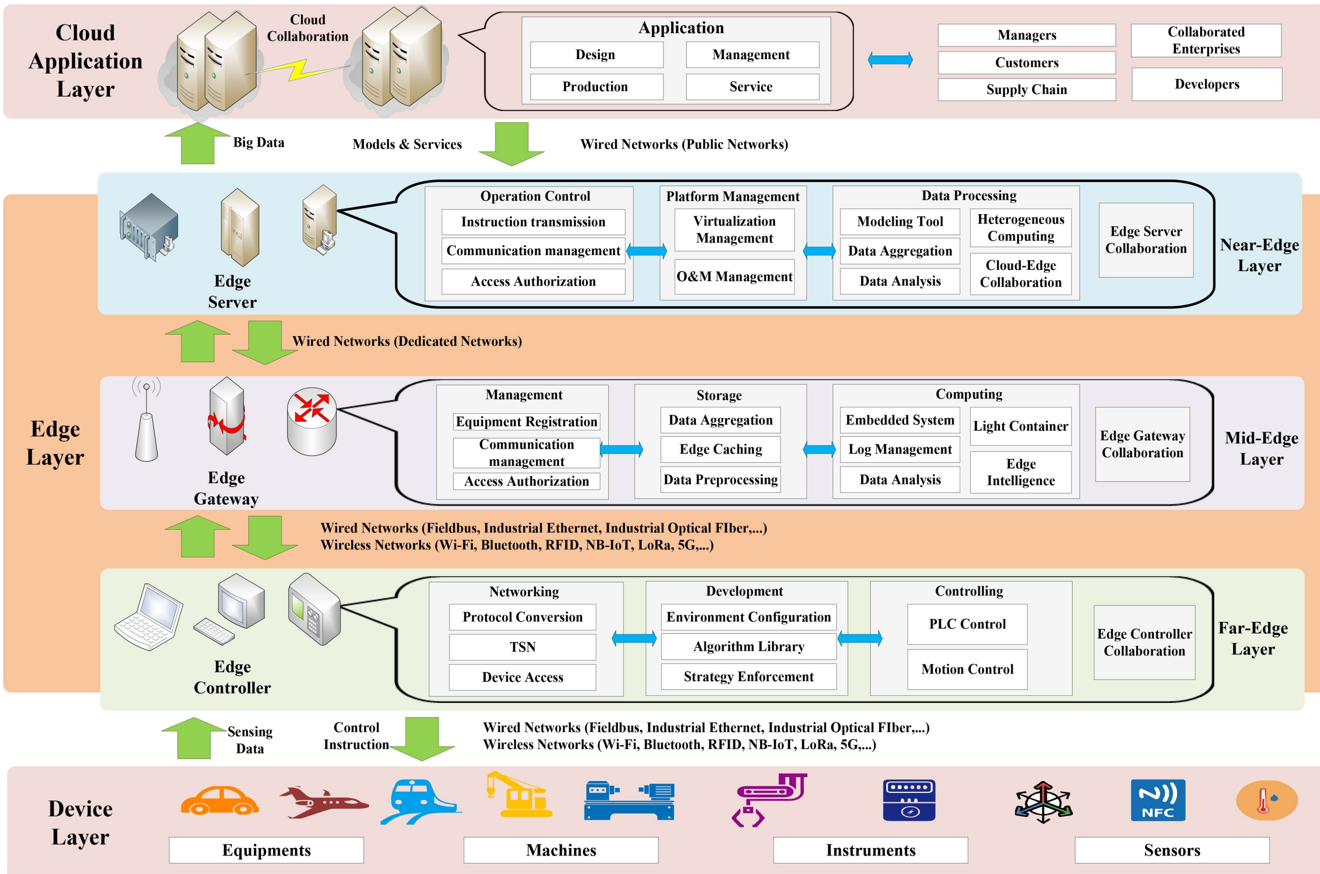

Fig. 2. Proposed Reference Architecture of Edge Computing in IIoT.

for the control instructions from the Edge Layer, realizing the connectivity of data flow and control flow between the Device Layer and the Edge Layer.

2) Edge Layer: The Edge Layer is the core layer of reference architecture of edge computing in IIoT. The Edge Layer is mainly responsible for receiving, processing and forwarding data flow from the Device Layer, providing time-sensitive services such as edge security and privacy protection, edge data analysis, intelligent computing, process optimization and real-time control. Considering the computing power of equipment in the Edge Layer sometimes may varies by several orders of magnitude, the Edge Layer can be divided into three sub-layers according to the data processing capacity of different equipment in the Edge Layer: The Near-Edge Layer, Mid-Edge Layer, and Far-Edge Layer.

a) Far-edge layer: The Far-Edge Layer contains some edge controllers that collect data from Device Layer, perform preliminary threshold judging or data filtering, and transfer control flow down to the Device Layer from the Edge Layer or Cloud Application Layer.

Due to the heterogeneity of sensors and devices in the device layer, the edge controllers in the Far-Edge Layer must be able to be compatible with various protocols downward and access various sensors or devices, so as to be able to collect data in real time from time-delay sensitive networks of the IIoT. After the data is collected from IIoT, it needs to be preprocessed for threshold judging or data filtering. Therefore, the edge controllers of the Far-Edge Layer need to integrate the algorithm library on the basis of the environment configuration to continuously enhance the strategy effectiveness. Meanwhile, the edge controllers of the Far-Edge Layer needs to transfer the control flow to the Device Layer through the PLC control or action control module after obtaining the decision from Far-Edge Layer or the upper layers. In addition, different edge controllers may need to collaborate on certain tasks.

The Far-Edge Layer usually has a *ms*-level latency for judgement and feedback, which is very important for some emergencies, such as the transient response of an unmanned vehicle in the event of a pedestrian suddenly entering the field of vision, or the instantaneous shutdown when a person's hair rolls into a lathe spindle. These emergencies must be processed in the Far-Edge Layer to reduce the delay and protect the safety of life and property.

b) Mid-edge layer: The Mid-Edge Layer mainly contains some edge gateways and is responsible for collecting data from Far-Edge Layer by wired networks (Fieldbus, Industrial Ethernet, Industrial Optical Fiber, *etc.*) or wireless networks (Wi-Fi, Bluetooth, RFID, NB-IoT, LoRa, 5G, *etc.*), caching the collected data and giving a heterogeneous computing. Meanwhile, the edge gateway in the mid-edge are also responsible for transferring control flow from the upper layers to Far-Edge Layer, managing the equipment in Mid-Edge Layer or Far-Edge Layer.

Different from the Far-Edge Layer only performing simple threshold judging or data filtering, the Mid-Edge Layer has more storage and computing resources to execute the collected data from IIoT. Heterogeneous data collected by Far-Edge Layer from the IIoT are preprocessed, fused and cached in the Mid-Edge Layer first. When enough data is obtained, the edge gateways of the Mid-Edge Layer will perform the steps of data processing deployed in the embedded system or the lightweight container, aggregating and analyzing the data in the way of traditional big data analysis or emerging edge intelligence technologies. Meanwhile, the data analysis log will be saved for future use. In addition, the Mid-Edge Layer also has the management module with many management functions (device management, access management, communication management, *etc*.) and the edge gateway collaboration module, so as to achieve multi-layer and multi-device collaboration. These events that allow a few seconds or minutes of delay can be handled perfectly at the Mid-Edge Layer.

The Mid-Edge Layer usually has a *s*-level or *min*-level latency and gives a more comprehensive judgment by combining information from multiple devices. For example, an RSU receives the location information of vehicles in its communicating coverage, analyzing and predicting the vehicle traffic; a smart gateway integrates the information of multiple cameras to judge the quality of products. These events that allow a few seconds or minutes of delay can be handled perfectly at the Mid-Edge Layer.

c) Near-edge layer: The Near-Edge Layer contains some powerful edge servers and is responsible for performing more complex and critical data processing and making directional decision guidance based on the data collected from the Mid-Edge Layer by dedicated networks. Meanwhile, the edge servers in Near-Edge Layer should have business application management and platform management functions.

The edge servers of the Near-Edge Layer are aggregated into a small computing platform, which has more powerful storage and computing resources than the equipment of the Far-Edge Layer and the Mid-Edge Layer. Therefore, the Near-Edge Layer is mainly used for bulk processing and operation of heterogeneous data, reasoning and training more accurate models to obtain better production scheduling decisions of edge network. Meanwhile, the Near-Edge Layer manages all kinds of resources in the whole Edge Layer, which requires the Near-Edge Layer have operation and virtualization management functions of the platform, as well as the deployment and scheduling functions of the edge side business application management, so as to realize the reasonable allocation of resources and the reasonable completion and delivery of tasks.

The Near-Edge Layer analyzes more data from different equipment to achieve the process optimization or get best measures to be taken over a wider area and a longer period of time, which usually has a *h*-level latency. For example, the edge server of a smart factory optimizes the product parameters according to the information collected from different production lines and equipment; the edge server of a smart grid aggregates the electricity consumption statistics of each community and optimizes the distribution of power.

3) Cloud Application Layer: The cloud application layer is mainly responsible for mining potential value from massive data and realizing optimal resource allocation across an enterprise, a region, or even nationwide. Therefore, the cloud application layer obtains data from the Edge Layer through the public network, supports the upper layer application such as product or process design, enterprise comprehensive management, sales and after-sales service, and gives feedback model and micro service to the Edge Layer. In addition, the cloud application layer can share data through cloud collaboration among groups of different attributes such as managers, cooperative enterprises, designers, and customers, to achieve more pluralistic and deeper data value mining. The decision times for such events are usually measured in *day*-level.

C. Application of Proposed Reference Architecture

The reference architecture proposed in Section III-B can be suitable for some typical IIoT scenarios. Therefore, we select smart vehicles and smart factory as cases to discuss how the proposed reference architecture is adapted to the IIoT scenarios.

1) Smart Vehicles: For smart vehicles, the Device Layer corresponds to the vehicles, the Far-Edge Layer corresponds to the on-board units (OBUs), the Mid-Edge Layer corresponds to the roadside units (RSUs), the Far-Edge Layer corresponds to the centralized dispatching edge servers in a certain area, and the Cloud Application Layer corresponds to the cloud computing platforms.

As the entity of Device Layer, the smart vehicle is equipped with sensors such as gyroscope, laser radar and HD cameras to collect various parameter data. Meanwhile, the smart vehicle is equipped with a variety of action actuators to execute the instructions from the upper layers.

As the entity of Far-Edge Layer, the vehicle controller, also called OBU, is responsible for receiving and recognizing heterogeneous data from different types of sensors, performing some simple data filtering and threshold judgment, and transmitting instructions based on the judgment or decision from the upper layers to various action actuators of the Device Layer. For example, when a vehicle suddenly encounters pedestrians or other vehicles scrambling for the lane while driving, OBU obtains environmental information by lidar and HD cameras, quickly analyzes the semantics of environmental information, and sends the instruction of immediate deceleration to ensure driving safety [47].

As the entity of the Mid-Edge Layer, the RSU receives data from OBUs of multiple vehicles, caches these heterogeneous data, and performs corresponding heterogeneous computing to provide valuable information. For example, the RSU collects the location and speed parameters from OBUs in its coverage range to provide relatively real-time driving parameters setting guidelines for different vehicles.

As the entity of the Near-Edge Layer, the area edge server can obtain all the data from RSUs and perform more comprehensive and complex data analysis, providing some real-time micro-services such as path planning and driving parameters pre-setting for vehicles. In addition, the regional edge server must have platform management and application optimization capabilities to manage the RSUs and OBUs in the region, so as to make reasonable and effective use of their storage and computing resources.

As the entity of the Cloud Application Layer, the cloud service platform obtains the historical data from the area edge servers in different regions and applies to the upper-level applications such as vehicles scheduling across regions, violation monitoring, traffic map construction and updating, *etc*.

2) Smart Factory: For smart factory, the Device Layer corresponds to the machines or robots with large numbers of sensors and actuators, the Far-Edge Layer corresponds to the controller units of machines or robots, the Mid-Edge Layer corresponds to the smart gateways, the Far-Edge Layer corresponds to the enterprise-level edge servers, and the Cloud Application Layer corresponds to the cloud computing platforms.

As the entities of Device Layer, the machines or robots with large numbers of sensors and actuators are responsible for sensing all kinds of operation parameters and executing the instructions from Far-Edge Layer.

As the entities of Far-Edge Layer, the controller units of machines or robots can collect sensing data from different sensors, give a data preprocessing and real-time threshold judgment [48]. When an emergency occurs, such as the temperature of a machine is out of the normal range or the hair gets sucked into the lathe, the controller units must be able to give a *ms*-level feedback to the actuators to execute emergency shutdown measures.

As the entity of Mid-Edge Layer, the edge gateway is usually responsible for collecting data from the controller units of machines or robots of a production workshop, caching heterogeneous data and performing corresponding heterogeneous computing. Therefore, the edge gateway in Mid-Edge Layer can monitor and optimize the parameters of different machines, identifying unqualified products in time to prevent the whole batch of products from being scrapped.

As the entity of Near-Edge Layer, the factory-oriented server has the platform management and application optimization capabilities to implement factory-level production process optimization based on the industrial big data. Therefore, the factory-oriented server is responsible for coordinating the process orchestration of different workshops, optimizing various production parameters, to improve the production efficiency of the factory.

As the entity of Cloud Application Layer, cloud computing platform collects data from factory-oriented servers and uses for some top-level decisions and applications, such as production process optimization, material rationing, logistics and selling strategy planning, *etc*.

There are just two application scenarios discussed above for the proposed reference architecture for edge computing in IIoT, including smart vehicles scenario and smart factory scenario. In fact, the proposed reference architecture is suitable for more IIoT application scenarios (e.g., remote monitoring, smart grid, smart logistic, *etc.*) based on existing cases study.

IV. State of the Art of Edge Computing in IIoT

Edge computing in IIoT uses sensing, communication, and data processing technologies to interconnect a large number of components, achieving many advances in diverse areas, which have strong performance impacts on edge computing in IIoT. For instance, the data generated from lots of sensors in the Far-Edge Layer needs to be uploaded to the Mid-Edge Layer, Far-Edge Layer, and Cloud Application Layer, and the strategy of routing will directly affect the delay performance. Task scheduling is to divide tasks to execute on different devices to make full use of idle resources to improve computing efficiency. The efficiency of scheduling scheme also affects the efficiency of task completion. Besides, Data storage and analytics are directly related to the timeliness and correctness of the decision, edge secure schemes and algorithms directly affect the reliability of edge networks or edge systems, and standardization directly affects the systematicness and extensibility of edge computing technologies in IIoT. Therefore, this section focuses on the above advances and gives a detailed discussion.

A. Routing

To enhance the flexibility of industrial processes and the intelligence of process control, large-scale sensor networks with complex topological structures and large amounts of real-time data are deployed in IIoT. By deploying edge computing in IIoT, preliminary sensory data can be processed near the sensor nodes, reducing the request-response time. Nevertheless, efficient and robust routing strategies can reduce the overhead and further reduce the latency. In the industrial field, routing is a necessary research topic for edge computing in IIoT.

1) Regular Routing Schemes: In the IIoT based on edge computing, regular routing schemes are usually designed with consideration of energy consumption, location and mobility of edge IIoT nodes.

Some regular routing schemes are mainly designed based on the location and energy of edge nodes, which are usually suitable for the situation that the IIoT edge nodes are fixed and energy-limited. For example, the new Stable Election Protocol (N-SEP) [49] comprehensively considers the factors of sensor nodes in the fog environment, such as the distance of the base station, the heterogeneity of the network, the remaining energy, the cluster head distance, *etc*., uses the heterogeneous energy threshold to select the best cluster head, and maintains the balanced energy consumption to extend the stability of the fog-supported sensor networks, so as to prepare for the establishment of an optimal routing link. the energy-aware real-time routing scheme (ERRS) [50] firstly clusters IIoT devices based on energy consumption and adds them into the cluster where the router is the cluster head (CH). When an IIoT device wants to send data to the gateway via routers, it sends the data to the CH. The CH searches all paths to the destination gateway through the existing node information, and selects the path with the least energy consumption and the least hops as the best routing path. In the fog computing scenario, the fog-based energy-efficient routing protocol (FERP) [51] considers dividing devices into advanced nodes and normal nodes according to the energy, and clustering devices with probability value based on energy. After devices clustered, the routing between Fog Nodes is completed by FECR Algorithm and the routing between Fog Node and cloud is completed by FEAR Algorithm. The GPSR-3D [52] routing algorithm for 3D smart factories uses two packet forwarding modes (greedy forwarding mode (GFP) and surface forwarding mode (SFP)) for routing. In GFP mode, the node forwards to the nearest neighbor in a greedy manner. When GFP fails, SFP mode is enabled, and the network space is divided into multiple subspaces according to the three-dimensional geometric structure. In the subspace, a parallel polyhedron traversal algorithm is used to restore the routing path.

In addition, there are some conventional routing schemes to study how to establish routing paths and improve routing stability under the strong mobility of edge IIoT nodes. These routing schemes are usually applicable to scenarios where nodes are vehicles, mobile users, and smart factory robots. For instance, the source vehicle uses Improved Geographic Routing (IGR) protocol [53] to select the next junction judging by score function based on vehicle location and vehicle density of junction, using improved greedy routing to forward the data packet from this junction to the next junction. If the destination vehicle is close to current junction or data packet delivering vehicle, the data packet will be delivered to the destination vehicle. The Collaborative Routing Protocol for Video Streaming (CRPV) [54] clusters the vehicles that record the emergency video streaming with the communication-enabled vehicles, and selects the vehicle with the highest gateway quality indicator (Based on the speed and position of vehicles) from the cluster to transmit the emergency video streaming. The Energy Efficient Multicast routing protocol based on Software Defined Networks and Fog computing for Vehicular networks (EEMSFV) [55] considers the deadline and bandwidth constraints, classifies the multicast session request according to the application type and duration constraints, and selects the optimal multicast path with the smallest energy by establishing a mathematical model. For high-priority critical multicast sessions, the appropriate path is preferentially selected based on the calculated remaining bandwidth of each link. The mobile clustering game theory-1 (MCGT-1) [56] considers the energy optimization problem in heterogeneous mobile sensor networks, and uses real-time parameters (predicted residual energy, distance between base stations and nodes, distance between nodes, moving speed, *etc*.) to establish a heterogeneous clustering game model to achieve efficient and energy-saving cluster head selection and multi-path routing.

In the regular routing schemes mentioned above, some are mainly designed based on the relative location and remaining energy of edge IIoT nodes, such as N-SEP [49], ERRS [50], FERP [51] and GPSR-3D [52]. The routing scheme based on the distance and remaining energy between the edge IIoT nodes usually assumes that the nodes use wireless communication, the location is fixed, the energy is limited, and the entire network is stable and robust. These schemes establish the energy model by comprehensively considering the location of nodes, remaining energy and other factors, elect the best cluster head for networking, and establish routing paths to balance the energy consumption of each node and extend the life of the entire sensor network. However, the disadvantage of this type of solution is that when the nodes in the network are displaced or broken due to external forces, the routing performance of the solution will be seriously degraded. In addition, in order to ensure the balance of the remaining energy of the node, the routing scheme needs to be updated frequently, which increases the energy consumption of the node to some extent.

Some regular routing schemes are mainly designed according to the real-time location and mobility of edge IIoT nodes, such as IGR [53], CRPV [54], EEMSFV [55] and MCGT-1 [56]. Unlike the routing scheme applicable to fixed nodes, the routing schemes designed considering node mobility cannot predict all nodes of data transmission path in advance. Therefore, these routing schemes usually use greedy methods to route and forward data. However, since the positions of the source node and the target node are usually easily obtained, the greedy forwarding can be optimized by comprehensively considering the position of the base station, the position between the nodes, the node speed, and the remaining energy. The disadvantage of this type of routing scheme is that the greedy forwarding method will consume more node transmission resources, and the burden of the self-organizing network is greater. When the greedy forwarding efficiency is improved by considering more factors, it will consume more computing resources. In addition, the scheme has higher requirements for real-time performance, and the delivery rate of data packets is relatively low.

2) SDN-Based Routing Approaches: As an emerging network technology, SDN is gradually being applied to edge computing in IIoT [61]. SDN splits the data plane and control plane, and the control plane coordinates all data routes of the network devices under its control. Therefore, SDN has obvious advantages for the scheduling and routing of data flows, especially for edge computing in IIoT, owing to the large number and weak processing capacities of far-edge nodes.

Many new routing schemes have been proposed based on SDN [57]–[60]. For instance, in time-sensitive software-defined network (TSSDN), the Incremental Flow Scheduling and Routing (IFSR) scheme [57] collects global knowledge of topology and traffic, computing schedules of time-triggered flows online and determining whether the data flow can be transmitted smoothly in the network based on the received request and the current network running state. In order to reduce the congestion of the edge network, SDN-based Edge-cloud Interplay Scheme (SEIS) [58] uses the multi-objective evolutionary algorithm based on Chebyshev decomposition, considering the balance between energy efficiency and delay, as well as the balance between energy efficiency and bandwidth as the evaluation index, to optimize the flow scheduling and routing of the edge network. The adaptive transmission optimization scheme (ATOS) [59] based on SDN divides the data flow into two groups (normal or emergency data flow) according to time constraints. Then, the path difference degree (PDD) of paths are calculated by using the information of time

TABLE IV
A SUMMARY OF SOLUTIONS FOCUSING ON ROUTING

Theme		Ref.	Solution	Advantages	Disadvantage
Regular Routing Protocol	Fixed Nodes	[49]	N-SEP	Balanceing energy consumption of nodes, extending the life of the entire sensor network.	Mobility constraint, frequently update the routing scheme result in the energy consumption increasing.
		[50]	ERRS		
		[51]	FERP		
		[52]	GPSR-3D		
	Mobile Nodes	[53]	IGR	Mobile self-organizing network adaptability.	Great load of the network, higher requirement of real-time attribute, higher delay.
		[54]	CRPV		
		[55]	EEMSFV		
		[56]	MCGT-1		
SDN-Based Routing Approaches		[57]	IFSR	Optimizing based on the global information, dividing the data flow and modify the routing path according to the demands.	Bandwidth and energy consumption, computing resources and greater decision delay.
		[58]	SEIS		
		[59]	ATOS		
		[60]	FDRS		

deadline, traffic load balances, and energy consumption collected by SDN from the whole world. All reasonable paths were found and the best routing path was selected from reasonable paths. The routing scheme based on the fuzzy Dijkstra algorithm (FDRS) [60] realizes the change of the existing path in the data transmission process by adopting the SDN method. The performance evaluation shows that the SDN network support structure based on the fuzzy Dijkstra algorithm is superior to the conventional Dijkstra algorithm in terms of energy consumption ratio, and can provide effective cluster routing while extending the network life cycle.

Compared with the regular routing schemes, the biggest advantage of the SDN-based routing schemes is that the schemes can be formulated and optimized based on the global network and node information, and can divide the data flow and modify the routing path according to the demands to achieve a more complex scheduling strategy. However, due to the continuous collection of node information from the entire edge network, the bandwidth energy consumption is increased to some extent. In addition, because SDN-based solutions usually consider more optimization goals, it will consume more computing resources and bring greater decision delay.

3) Lessons Learnt: For regular routing schemes in edge computing in IIoT, it is generally necessary to design the scheme according to the relevant attributes of the nodes, such as energy, location, mobility, *etc*. Some regular routing schemes are mainly suitable for the situation that the IIoT edge nodes are fixed and energy-limited, such as N-SEP [49], ERRS [50], FERP [51] and GPSR-3D [52]. some regular routing schemes are mainly designed for mobile edge IIoT nodes, such as IGR [53], CRPV [54], EEMSFV [55] and MCGT-1 [56]. In addition, emerging SDN technology will have a significant impact on the routing scheme and communication mode of edge network, and brings more comprehensive and in-depth routing schemes for edge computing in IIoT [57]–[60]. Research related to routing for edge computing in IIoT are summarized in Table IV.

B. Task Scheduling

Task scheduling concerns the upper design of data and resources. This involves making decisions about how data should be transmitted throughout the network and how resources are partitioned and utilized. There are large numbers of sensors, routers, switches, base stations, gateways, and access points in IIoT, deployed throughout industrial processes, which can be integrated with the underestimated computing power [62]. Owing to the huge differences in hardware configurations and software functions, the corresponding data computing, storage, and forwarding capabilities vary. The problem lies in how to effectively manage a large number of edge computing nodes, smoothly segment tasks, and merge calculation results, while at the same time minimizing energy consumption, reducing latency, and guaranteeing load balancing.

1) Latency Minimization Schemes: In the existing research on the task scheduling of edge computing in IIoT, some schemes are designed to minimize the end-to-end latency. For instance, the Fog Node Collaboration Policy (FNCP) [63] takes the task queue length and the task type into consideration and shares the tasks among the fog nodes to minimize the task delay. The FOG-to-FOG Communication Scheme (F2FCS) [64] considers categorizing task requests by deadline. If the deadline of task is long, it is allocated to the cloud. Otherwise, the task is processed in the fog layer. Tasks between different nodes can be scheduled according to node capabilities, so that the overall delay of task processing is minimized. By using PE-based progressive computing resources competition (PCRC) and QoE-oriented synchronized task scheduling (STS) algorithms, the Dispersive Stable Task Scheduling (DATS) scheme [65] synchronously offloads tasks to multiple adjacent nodes with heterogeneous capabilities, so that tasks can be executed in parallel and the task processing latency can be reduced. In the video data analysis system (VDAS) [66], the base station can redistribute the received video processing tasks to smart devices with sufficient resources for processing. By expressing the reallocation of tasks as a mixed integer nonlinear problem and solving it, jointly optimize the task offloading scheme and bandwidth allocation of smart cameras and base stations to minimize system delay. The Delay-Minimized Task Offloading (DMTO) [67] algorithm solves the IoT task offloading delay objective function to obtain the optimal solution including the subtask size and the terminal node transmission power, thus

TABLE V
A SUMMARY OF SOLUTIONS FOCUSING ON TASK SCHEDULING

<table>
<tr><th colspan="2">Theme</th><th>Ref.</th><th>Solution</th><th>Advantages</th><th>Disadvantages</th></tr>
<tr><td rowspan="5">Latency Minimization Schemes</td><td rowspan="2">One-to-One allocation</td><td>[63]</td><td>FNCP</td><td rowspan="2">No task fragmentation and low scheduling complexity.</td><td rowspan="2">Neighbor nodes may not be able to accept tasks, low efficient strategy.</td></tr>
<tr><td>[64]</td><td>F2FCS</td></tr>
<tr><td rowspan="3">One-to-Many allocation</td><td>[65]</td><td>DATS</td><td rowspan="3">Task fragmentation, more balanced node load and resource allocation.</td><td rowspan="3">More complex and consume more computing resources to get an optimal solution.</td></tr>
<tr><td>[66]</td><td>VDAS</td></tr>
<tr><td>[67]</td><td>DMTO</td></tr>
<tr><td colspan="2" rowspan="4">Energy-Latency Tradeoff Schemes</td><td>[68]</td><td>HyFog</td><td rowspan="4">Balance the energy consumption better and prolong the running time of the system on the premise of ensuring latency requirement.</td><td rowspan="4">Additional computing resource consumption and task scheduling execution time due to the more complex algorithms.</td></tr>
<tr><td>[69]</td><td>OWAS</td></tr>
<tr><td>[70]</td><td>DOTS</td></tr>
<tr><td>[71]</td><td>DEBTS</td></tr>
</table>

providing the best task scheduling strategy for delay sensitive tasks.

The FNCP and F2FCS can send tasks from one node to other fog nodes or cloud for execution. By communicating with adjacent fog nodes and task delivery, the best node for task execution is found to minimize task latency. However, both FNCP and F2FCS allow only one fog node to perform a task. Due to the limited computing power of a single fog node, it is possible that all adjacent nodes cannot meet the low latency requirements. The DATS, VDAS and DMTO enable tasks to be offloaded to multiple nodes for synchronous execution, and enable tradeoffs between computing resources and communication. However, compared with the task execution of a single task, these task scheduling algorithms are more complex and consume more computing resources to get an optimal solution. In addition, all the above schemes only take delay as the optimization objective. If the devices have limited energy, these schemes may cause unbalanced load among the devices and shorten the life-time of system.

2) Energy-Latency Tradeoff Schemes: In addition to the latency minimization, the energy-latency tradeoff is also need to be taken in to consideration for task scheduling. The HyFog framework [68] allows devices to choose the execution mode among local mode, D2D mode, and cloud mode. By transforming the minimum weight matching problem in the three-layer graph into the minimum weight matching problem and applying Edmonds's Blossom algorithm to solve it, the total task execution cost (including energy and delay) is minimized. The Optimal Workload Allocation Scheme (OWAS) [69] considers the problem of minimizing the power consumption of fog-cloud computing system while ensuring the required delay, decomposes the original problem into three sub-problems, which are solved by interior-point method, generalized Benders decomposition method and Hungarian method respectively. Then the optimal task scheduling strategy will be generated. The Delay-Optimal Task Scheduling (DOTS) [70] transforms the problem of the energy-latency tradeoff task scheduling between voluntary nodes (VNs) into the problem of maximizing the equivalent rate, and put forward the task scheduling algorithm to solve the problem optimally. The Delayed Energy Balance Task Scheduling (DEBTS) scheme [71] characterizes the energy and delay balance relationship of task scheduling in the fog network by defining control parameter V, and seeks to balance service delay and total energy consumption by optimizing this parameter, thereby providing better delay and energy performance for task scheduling.

Compared with the task scheduling schemes which only considers latency, the task scheduling schemes which comprehensively consider latency and energy can balance the energy consumption of the system better and prolong the running time of the system on the premise of ensuring latency requirement. However, additional computing resource consumption and task scheduling execution time are increased due to the more complex algorithms.

3) Lessons Learnt: For task scheduling in edge computing in IIoT, the schemes are usually designed according to the demand of latency and energy consumption. For example, the task scheduling schemes that consider minimizing latency include FNCP [63], F2FCS [64], DATS [65], (VDAS) [66], (DMTO) [67], *etc.* The task scheduling schemes that balance latency and energy consumption include HyFog [68], OWAS [69], DOTS [70], DEBTS [71], *etc.* The schemes that only consider the latency have obvious advantages in the speed of task scheduling, while the schemes that balance the latency and energy consumption have more advantages in the comprehensive performance of the system. Research related to task scheduling for edge computing in IIoT are summarized in Table V.

C. Data Storage and Analytics

Big data is the core of IIoT unquestionably. Industrial big data mainly stems from production and operational business data, equipment and object data, and enterprise external data generated by large numbers of devices and lengthy business processes. Therefore, industrial big data has the "4V characteristics" of general big data, namely Volume, Velocity, Variety, and Value. In addition, it also has some special characteristics such as real-time, accurate, and closed-loop [72]. For edge computing in IIoT, it is necessary to study the distributed storage and analysis of industrial big data.

1) Data Storage: In edge computing scenarios in IIoT, data-intensive applications require an increasing amount of data. The question of how to store data in distributed edge servers, and even devices with limited resources, is worthy of attention. An edge collaborative storage framework (ECSF) [73] shown in Figure 3 achieves edge server collaborative storage through an iterative algorithm that optimizes the data storage strategy between edge servers. In this scheme, neighboring servers

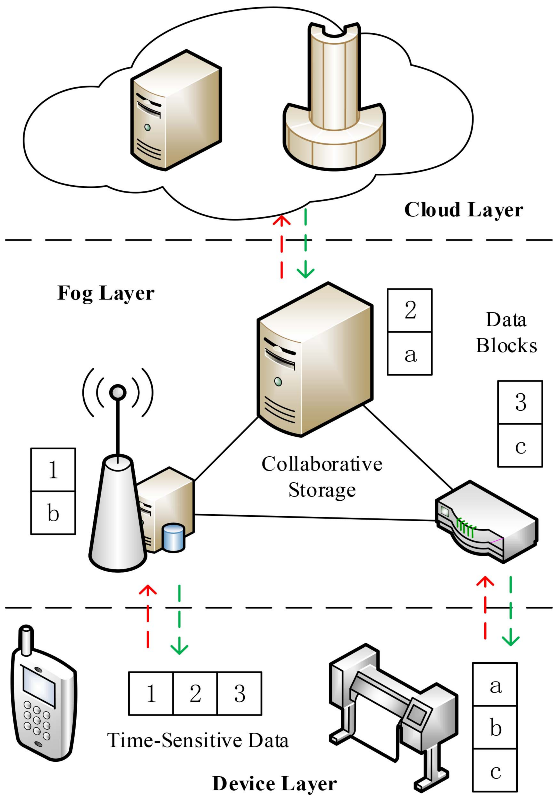

Fig. 3. The Edge Collaborative Storage Framework.

within one-hop range of an edge server are also available taken as one of the measurement criteria of storage strategy. A Score Function based on the cache hit indicator is established to measure the quality of a data storage strategy. Based on this index, the storage scheme is iteratively optimized to find the optimal storage strategy. Another collaborative storage approach is based on the distributed key-value storage platform (DKSP) [74]. DKSP collects edge servers, establishes upper level storage management and organizes distributed key-value stores in a unified namespace. The ELFStore [75] is an edge local federated storage solution that uses reliable devices in the fog layer to store data, and a bloom filter is designed to provide data indexes that can be found within two hops, thereby ensuring balanced use of edge device storage and providing good storage flexibility. The FogStore [76] uses NFV and stateful applications to achieve fog-aware replication placement and context-sensitive differential consistency in fog storage, thereby better deploying distributed data stores tool into fog computing storage systems.

The ECSF, ELFStore and FogStore can make optimal distributed storage decision by collecting the storage state and neighbor node information of each edge server. However, the disadvantage is the additional query and transmission overhead for searching on many edge servers frequently. In contrast, because of the establishment of the upper storage management function, the data storage information and node information of the edge servers in DKSP will be updated after the number of nodes changes or the period reaches, and there will be less additional information collection overhead. However, the DKSP used to do the experiment does not support fault-tolerance or access control, which may bring additional security risks.

2) Data Analytics: In addition to distributed data storage, there are also some studies on the data analytics on the edge computing in IIoT. For instance, the Edge random gradient descent (EdgeSGD) algorithm [77] is deployed on edge devices to solve the linear regression problem by edge node, so as to estimate the feature vectors of edge nodes, which may be used in further data processing. The Fog Linear Regression Component Decomposed Computing Program (FLRCDCP) [78] uses multiple linear regression fog-specific decomposition based on statistical query model and summation table as predictive analysis model, and deploys the decomposition method in the Internet of Things based on fog computing and runs in a distributed manner, so as to significantly reduce the amount of data sent to the cloud platform. The big data analysis architecture (BDAA) [79] reduces the transmission of information sent to the fog server by performing certain local processing and refining of data generated by edge devices. The fog server executes distributed machine learning algorithms to efficiently process streaming data and share the extracted knowledge with the lower layers. In [80], an efficient analysis platform for industrial big data have been proposed, which can provide big data analysis services through fog nodes and cloud computing to meet the different needs of data processing, analysis and management. The Energy-Saving Data Analytics (ESDA) fog service platform [81] combines multiple algorithms to train a deep self-encoding model on the local fog server, runs the service process, and solves the problem of time series sensor data loss completion.

The objective of data analytics schemes and platforms is to transfer part of the data analysis functions originally deployed in the cloud to the edge, which can obtain good real-time benefits of data analysis. However, these schemes or platforms usually ignore the security and adaptability problems of data analysis at the edge, which may lead to the risk of data analysis accuracy reduction and data leakage.

3) Lessons Learnt: With the continuous improvement of computing resources and the performance of various edge devices, it has become a very obvious trend for industrial big data to be processed closer and closer to the edge. As the basic resource of production monitoring and decision optimization, industrial big data based on edge computing has been studied in data storage and data analytics, *etc*. Distributed Data storage based on edge computing has a feature of strong distribution. When considering the storage scheme, we should not only consider how to save the storage space and balance the storage capability of edge nodes as much as possible, but also consider the security risk caused by the weak security protection capability of edge devices [73]–[76]. In addition, there is a growing trend to decentralize data to edge devices for analysis, but the applicability and safety of the solution still need to be considered [77]–[81]. Besides, with the development of artificial intelligence technology, big data can be exploited deeply and precisely, and various machine learning methods are tried to transplant and adapt to edge devices gradually by researchers. Therefore, edge intelligence will become a hot research trend and face some challenges in the future, and the topic will be discussed in Section V-C.

D. Security

Although applying edge computing to IIoT can reduce the transmitted data volume, to enhance the data security and privacy to some extent, traditional security protection methods cannot satisfy the protection requirements of edge computing, as the security risks cannot be fully considered at the start of the design. Moreover, the integration of various technologies has also intensified the security threats related to data, networks, and applications. Some typical security issues and solutions concerned in edge computing in IIoT are as follows.

1) Network Security: If a malicious attacker initiates an attack from the edge to control the communication network, such as eavesdropping or traffic injection [82], this is highly likely to threaten all the functional elements of the edge network and spread to the entire communication network. Nowadays, research on edge network security in IIoT mainly includes attack detection and defense.

Many network attack detection and defense solutions provide effective ways to protect the edge IIoT network. For instance, the LSTM-based fog network distributed network attack detection (LDNAD) scheme [83] uses machine learning algorithms to identify and detect key attacks against IIoT devices in the fog environment. By detecting various network attacks with high precision and take some specific measures, the security of the edge network is effectively improved. The hierarchical distributed intrusion detection system (HD-IDS) [84] based on the fog architecture guarantees the hierarchical protection detection level by deploying IDS in different network layers, thereby ensuring that smart meters in the power grid are protected from false data injection attacks. The routing attack detection scheme for in the edge-based IoT (RAD-EI) [86] provides an effective detection method for routing attacks by malicious neighbors that may occur in the edge-based IoT environment, thereby avoiding routing attacks affect the performance of edge networks such as throughput and latency. The real-time traffic monitoring system (RTMS) [85] performs a thorough inspection of the data packets and matches the SQLI pattern in the IDS database to form signature rules, avoids the workload of manually writing signature rules, and detects traffic injection attacks more efficiently. In the multi-layer DDoS mitigation framework (MDMF) [87], the cloud computing layer collects traffic data, detects and inhibits DDoS attack based on network traffic data. Meanwhile, the cloud computing layer analyzes DDoS attack behaviors by using powerful data analysis capability, and sends detection information to the fog computing layer to jointly resist DDoS attack. The fog-based DDoS mitigation solution (FDMS) [88] applies fog computing to DDoS mitigation, conducts traffic analysis based on offline specification through the virtual network function (VNFs) in the local server, and integrates the information from cloud server to effectively detect and resist DDoS attacks.

In the above solutions, LDNAD is used to resist key attacks. Due to the use of machine learning methods, LDNAD can obtain key attack knowledge through time series historical data and achieve higher attack detection accuracy. However, its training process consumes a lot of computing resources and is not suitable for deployment in lightweight edge devices. HD-IDS and RTMS are mainly used to defend against traffic injection attacks. HD-IDS deploys multiple IDSs in hierarchical network layers and performs detection by multiple layers collaboratively of traffic analysis, thereby providing real-time and precise protections. The disadvantage is that the real-time and collaboration requirement of multi-layer IDSs is high. The RTMS mainly updates the traffic injection signature rules through historical attack data analysis, which requires relatively low real-time requirements for rule updates. RAD-EI is used to prevent routing attacks. It is mainly deployed on edge servers to detect whether malicious nodes on the routing path have carried out malicious routing attacks on neighbors. Due to the Edge-IoT environment, RAD-EI needs to collect information from all routing nodes in a broadcast manner, which will cause additional network overhead and longer delay. MDMF and FDMS are mainly used to prevent DDoS attacks. Due to the combination of SDN technology and NFV technology, MDMF and FDMS can collect edge network and edge node information from the global, and perform traffic detection on the fog layer at the same time. The detection speed improvement of network attacks is very obvious, which provides a very good reference to improve the robustness of the edge network. However, these schemes collect and update node information and network information frequently, which increases the overhead on edge networks.

2) Data Security: Edge nodes have limited storage and data processing capabilities, being able to temporarily maintain data generated by devices. Although the data management complexity is reduced, many data security issues are also triggered such as data leakage.

In the research on data security of edge computing in IIoT, some concern about the issue of secure data storage. For instance, the local-cloud-fog three-layer framework (3LF) [89] desensitizes data by using local differential privacy algorithms and RS encoding, and uses a multi-party collaborative storage scheme based on AES-RS encoding to effectively protect data security and recoverability. The Data Security Storage Model based on Fog Computing (FCDSSM) [90] collects the status information of data storage nodes through SDN technology. By designing hierarchical trusted domains, collaborative working mechanisms and security policies, hierarchically managing and authorizing storage requests and status of data storage nodes, a large-scale secure storage mechanism for big data in the Internet of Things is realized.

Some solutions focus on secure data sharing of edge computing in IIoT. The efficient fog-based privacy protection data sharing (EP-DS) [91] scheme uses improved inadvertent transfer algorithms and edge low-latency services to provide a solution for vehicles to query the best driving route under the premise of anonymity and protection of location privacy. The fog-to-cloud-based VCC data sharing (FVDS) scheme [92] introduces the fog computing layer to hand over the data sharing requirements generated by the vehicles to the secure fog computing node. The scheme uses a

TABLE VI
A SUMMARY OF SOLUTIONS FOCUSING ON SECURITY

Theme	Topic	Ref.	Solution	Advantages	Disadvantages
Network Security	Key Attack	[83]	LDNAD	Improve key attack knowledge and achieve higher attack detection accuracy.	Not suitable for deploying in lightweight edge devices.
	Injection Attack	[84]	HD-IDS	Multiple layers-collaborative traffic analysis, real-time and precise protections.	Real-time and collaboration requirement is high.
		[85]	RTMS		
	Routing Attack	[86]	RAD-EI	Detect malicious routing attacks on neighbors.	Additional network overhead and longer delay to collect information.
	DDoS Attack	[87]	MDMF	Collect edge network information from the global to prevent DDoS attacks.	Collect and update network information frequently result in the high overhead.
		[88]	FDMS		
Data Security	Secure Data Storage	[89]	3LF	Guarantees storage security through hierarchical data encoding desensitization.	Only design the security strategy for the sensitivity and authority of the data, without considering the underlying design such as data format.
		[90]	FCDSSM	Design hierarchical storage management and authorization security policies.	
	Secure Data Sharing	[91]	EP-DS	Provide the service to query the best driving route under the premise of anonymity and protection of location privacy.	In addition to encryption algorithms and access control, more security factors should be considered, and the current research is insufficient.
		[92]	FVDS	Use a cryptography-based mechanism to provide fine-grained security access control.	
		[93]	FRVDS	Realize the data access control of the IoV system by designing a new CP-ABE strategy.	

cryptography-based mechanism to provide fine-grained security access control, and can review the fog server's calculation execution records, thereby ensuring the safety of data sharing under low latency. The fog-based reversible vehicle data sharing (FRVDS) scheme [93] realizes the data access control of the IoV system by designing a new multi-authority ciphertext policy attribute-based encryption (CP-ABE) strategy. Users can freely perform data access authorization and attribute revocation through this scheme to ensure delay-sensitive data sharing.

In the above-mentioned data security storage scheme, 3LF mainly guarantees storage security through hierarchical data encoding desensitization; FCDSSM ensures data storage security by designing hierarchical storage management and authorization security policies. In the data security sharing scheme (EP-DS, FVDS, FRVDS), it is mainly designed for the access rights of data sharing. At present, the relevant research on the data security of edge computing in IIoT is focused on how to store and share data securely, and the research depth and breadth need to be further explored.

3) Lessons Learnt: The security threats to devices, networks, and data exist in all areas. However, for security of edge computing in IIoT, the differences are lying on the importance of edge security has grown as data relegated to the edge devices. The complexity of edge computing-based IIoT networks is higher, but the protection capability of edge devices, networks and data is relatively weak, which makes the protection of edge network and data more difficult. For edge network security, it is usually necessary to prevent malicious attacks such as key attacks [83], traffic attacks [84], [85], routing attacks [86], DDoS attacks [87], [88], and the corresponding solutions should consider the balance between computing power, bandwidth, and latency of the edge network. The related research on the secure storage [89], [90] and data sharing [91]–[93] is mainly based on data desensitization and access permission control, and the related research work is currently limited, and needs to be further developed and explored. Besides, due to the IIoT requires a relatively high level of security protection, some new security-related technologies (e.g., blockchain) bring the new opportunities and challenges for data security management and sharing of edge devices, although more expense may be costed. Research related to security for edge computing in IIoT are summarized in Table VI.

E. Standardization

Edge computing in IIoT represents the organic integration of industrial Internet, IoT, and edge computing technologies. It involves the complex integration and application of software, hardware, communication, and system platforms. A necessary step is to set standards to make the edge computing in IIoT widely accepted, applied, and supported.

1) Organizations and Standards: At present, there exists a variety of competing standardization organizations focusing on the standardization of IIoT and edge computing, such as the European Telecommunications Standards Institute (ETSI), Institute of Electrical and Electronics Engineers (IEEE), Industrial Internet Consortium (IIC), and OpenFog Consortium. Standardization work on edge computing in IIoT must be conducted basing on the standardizations of IIoT and edge computing delivered by the organizations mentioned above.

The standardization of IIoT is reasonably mature. ETSI released the Technical Report ETSI TR 103 375 [94] to provide a standard roadmap for IIoT. IEEE is strongly concerned about the industrial tactile Internet standardization process [95], [105]. IIC is a direct promoter of the development of IIoT and has published a series of white papers and technical reports in the field of IIoT concerning architecture [96], communication [97], and security [98], [99].

In comparison, the overall standardization process of edge computing remains in an immature evolution stage, and this mainly consists of standardization work on fog computing at present, which is a part of edge computing. The OpenFog Consortium released the OpenFog Reference Architecture

TABLE VII
A SUMMARY OF STANDARDIZATION WORKS ON IIOT AND EDGE COMPUTING

Theme	Document	Ref.	Organization	Year
IIoT	Technical Report ETSI TR 103 375	[94]	ETSI	2016
Tactile Internet	Tactile Internet: Application Scenarios, Definitions and Terminology, Architecture,Functions, and Technical Assumptions	[95]	IEEE	2016
IIoT Architecture	The Industrial Internet of Things Volume G1: Reference Architecture	[96]	IIC	2017
IIoT Communication	Industrial Networking Enabling IIoT Communication	[97]	IIC	2018
IIoT Security	Key Safety Challenges for the IIoT	[98]	IIC	2017
IoT Security	IoT Security Maturity Model -Description and Intended Use	[99]	IIC	2019
Edge Computing Architecture	Openfog Reference Architecture for Fog Computing	[100]	OpenFog Consortium	2017
Edge Computing Architecture	IEEE Standard for Adoption of Openfog Reference Architecture for Fog Computing	[101]	IEEE	2018
Edge Computing Communication	Signalling Requirements and Architecture of Intelligent Edge Computing	[102]	ITU	2018
IIoT & Edge Computing	Introduction to Edge Computing in IIoT	[103]	IIC	2018
IIoT & Edge Computing	The Edge Computing Advantage	[104]	IIC	2019

technical report [100] and OpenFog Security Approaches and Requirements technical report [106], which outline architecture and security issues. IEEE released the IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing [101] standard document in 2018, to officially adopt the OpenFog Consortium's fog computing reference architecture as the industry formal standard. The International Telecommunication Union (ITU) has released Signaling Requirements and Architecture of Intelligent Edge Computing [102], discussing intelligent edge computing (IEC). A summary of standardization in IIoT and edge computing is given in Table VII.

At present, IIC is the only organization to release white papers related to edge computing in IIoT [103], [104], which introduce the advantages of edge computing and provide practical guidance on the architecture and building blocks required to implement edge computing in IIoT. It defines the edge computing architecture capabilities, and emphasizes key use-case considerations, focusing on model deployment and edge computing implementation patterns across multiple horizontal functions.

2) Lessons Learnt: The standardization of the IIoT and edge computing is continuing to advance. As a subset of edge computing, the standardization of fog computing is progressing rapidly due to the efforts of the OpenFog Consortium [100]–[102], [106]. But the standardizations of merging MEC, fog computing, and edge computing are still in progress. In addition, edge computing in IIoT has attracted increasing attention, but the relevant standardizations remain limited. Strengthening communication and interactions among scholars and organizations in different research fields to perfectly deploy edge computing in IIoT systems based on the understanding of the edge computing and IIoT will play a powerful role in promoting the standardization process of edge computing in IIoT.

V. CHALLENGES AND OPPORTUNITIES

In the above section, advances in routing, task scheduling, data processing, security and standardization of edge computing in IIoT have been discussed. By analyzing the current advances progress, there are some shortcomings of various technologies in solving the corresponding problems. The emergence of new technologies has provided great opportunities and challenges for the development of advances (e.g., network, data processing, security, *etc.*) for edge computing in IIoT. In this section, we discuss some challenges and opportunities for edge computing in IIoT, including 5G-based edge communication, data offloading and load balancing, edge intelligence and data sharing security.

A. 5G-Based Edge Communication

At present, IIoT networks are structured by two modes: wired mode and wireless mode [107]. The wired mode in an IIoT network is more stable, while the wireless mode is developing slowly, owing to a low transmission rate and poor stability [108], [109]. In IIoT edge computing, frequent scheduling and data exchange is required between edge devices and edge servers at each layer, and a high transmission rate and low delay are the main requirements and goals. As a new generation of cellular mobile communication technology, the development and application of 5G will play a vital role in network organizing and information exchanging in the IIoT system based on edge computing [33]. The three characteristics of 5G technology, namely an ultra-high rate, super-large connection, and ultra-low delay [110], can precisely meet the requirements of an IIoT system based on edge computing in terms of the transmission rate and low delay required to reduce certain economic losses and life-threatening emergencies, such as the emergency stopping of industrial equipment or autopilot vehicles. In addition, 5G can free a large number of devices from cables, making physical deployment more flexible and consuming a lower maintenance cost. Despite the promising industrial prospects, the integration of 5G into edge-computing-based IIoT still faces many potential problems.

1) System QoS: In 5G-based IIoT edge computing systems, QoS characteristics include availability, throughput, delay, *etc* [111]. These characteristics will be linked to 5G's QoS standards [112]. The standardized 5G QoS indicator (5QI) mapping table of 5G QoS characteristics has been published by 3GPP and the characteristics in the table include 5QI value, priority level, packet delay budget, packet error rate, *etc.*, and give some example services for different 5QI value. Depending on the 5QI value, 5G can support a wide variety of services, especially those that are time-sensitive. For example, in the Internet of Vehicles, real-time fault monitoring, or smart grid [113], the services have strict requirements on delay and packet error rate. In these cases, the 5G network can provide the high quality and low delay services that latency is less than $10ms$ and the packet error rate is less than 10^{-6}.

2) Edge Node Management: In 5G-based IIoT edge computing systems, the node management strategy can be optimized using 5G core networks. In the current IIoT system, most of the edge nodes are fixed. The application of 5G can make the fixed nodes in IIoT gradually get rid of the shackles of cables and become movable edge nodes, making the production process more flexible [114]. Meanwhile, The edge node management issues will be easy to handle in a 5G network [115]. Specifically, 5G core network can collect status information of various nodes regularly (e.g., node location, resource use, task list, adjacent nodes, *etc.*), monitor and update node management information and strategies, and optimize other strategies such as data processing strategy and network protection strategy according to the collected information.

3) Network Slicing: One feature of the 5G network is that it can be sliced as shown in Figure 4. By using NFV technology, multiple networks of different application scenarios can be deployed in parallel under the same network resource pool, sharing the same network resources physically but separated logically [116]. The realization of three major 5G application scenarios, i.e., ultra-reliable and low latency communication (URLLC), massive machine-type communication (mMTC), and enhanced mobile broad-band (eMBB) [117], is based on the indispensable network slicing feature of 5G. The network slicing can make specific optimization and user-defined configuration for edge application scenarios, which can help further reduce the complexity of edge service and reduce service delay.

The fusion of 5G and IIoT based on edge computing can lead to development momentum for typical IIoT application scenarios, such as VANET, digital twin, remote control, and maintenance. However, long-term integration still has many of the above potential technical challenges to overcome.

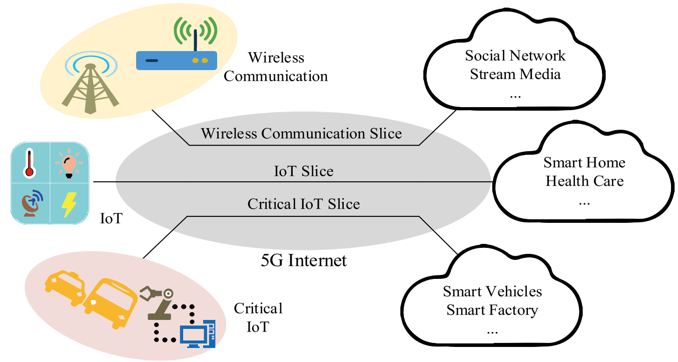

Fig. 4. 5G network slicing.

B. Data Offloading and Load Balancing

An IIoT system based on edge computing is a typically distributed system [118] and has a variety of data sources with distributed computing power. When the processing capacity of a single device or edge server reaches its limitation, task splitting and data offloading must be considered. The lower the equipment performance, the stronger the requirement for effective load balancing, such as in the MEC scenario [119]–[121]. That is, tasks and data are divided and distributed to multiple devices or servers, and the results from each part are merged to achieve the overall load balancing of the system. Load balancing and data offloading make the best use of the computing and storage resources in each layer to avoid the long-term overload of a single resource, thus reducing the time delay and improving the efficiency, improving the reliability, availability, and scalability of an IIoT system based on edge computing in a redundant manner. However, the data offloading and load balancing for edge computing in IIoT are facing many challenges and problems to be solved and improved.

1) Data Offloading: Although a general IIoT system contains a large number of devices, it is only necessary to consider data offloading between some large servers, and devices are not considered usually. However, in an IIoT system based on edge computing, where the data offloading of all devices with data processing capabilities should be considered, the difficulty of this problem will increase geometrically. In addition, owing to the limited computing and storage capacities of the edge devices, data offloading will occur frequently to balance the overall load of a system. This will lead to a large throughput in the edge network, serious bandwidth resource occupancy, and ultimately possibly to overall delay increases for tasks.

In order to solve the above problems, proper data offloading schemes should be designed for special requirements. In general, according to different offloading requirements and application scenarios, there are two modes of data offloading to solve data offloading problem: full offloading and partial offloading.

a) Full data offloading: Data offloading usually involves time delay and energy consumption. For full offloading, If the energy of devices is sufficient and the requirement for the delay is high, the offloading scheme can only consider the minimum delay. The best solution is to find the optimal full data offloading scheme based on task queue information, resource utilization information of edge node, edge server and routing status information [122]. Under the premise of meeting the delay requirement, expressing minimizing energy consumption the data offloading by the optimization problem may be a good solution [123].

b) Partial data offloading: For full offloading, the considered performance characters are time delay and energy consumption, but the division of data is also needed to be taken into consideration. Partial offloading usually splits data from the same task into blocks and only a part of blocks can be offloaded [124]. Besides, offloading decision needs to consider various parameters, including total data volume, resource use of devices, channel state, energy consumption, *etc* in [125]. Decisions are made with the above parameters fully been taken into account to jointly optimize the allocation of communications and computing resources. At present, the offloading applied to the IIoT is still not enough, and needs to be adapted and optimized according to the characteristics of IIoT.

2) Load Balancing: In the process of calculating the data offloading scheme, time delay and energy consumption are generally considered collaboratively. But the calculated scheme may lead to the overload of some devices, which raises a new problem, load balancing [24]. The purpose of load balancing is to make the load distribution among the edge nodes equal, and the communication link stable, so that the computing resources and network resources usage reaches a balance. Considering the scale and frequency of scheduling are significantly larger, it is necessary to improve the existing load balancing algorithms to adapt the characters of the IIoT edge system.

In IIoT based on edge computing, sing the task data and loading data from the equipment and edge servers of the far-edge, mid-edge, and near-edge layers, combined hierarchically with AI, a load balancing service can set up the load balancing scheme based on a machine learning model for each layer. In addition, SDN can be utilized to conduct load balancing scheduling from the global perspective of the edge network, to minimize the complexity of scheduling and routing.

C. Edge Intelligence

In current IIoT systems based on edge computing, edge devices can only perform lightweight computing tasks. To enable edge devices and edge servers to perform more complex tasks with a higher data processing performance and lower latency, edge intelligence (EI) is applied on the edge of IIoT to make edge devices and servers intelligent. This has become a developmental trend of edge computing in IIoT. However, An AI model can be trained to perform predictions and make decisions with high accuracy, but large amounts of training and verification data are needed. For edge devices, training and leverage the AI model are hard due to the limited computing and storage resources. To resolve the conflict between the limited resources of edge devices and the high complexity of the AI model. There are two basic approaches: enhancing the computing power of edge devices; simplifying or partitioning the AI model deployed on edge devices.

1) EI Devices: Edge devices can collect a large amount of data, and require fast and accurate computing models to provide feedback [126]. When the AI algorithm is deployed on the edge device, the AI model can obtain a large amount of source data from edge devices to improve the accuracy of the AI model, while the edge device can get more timely and accurate decisions made by the AI model. Therefore, deploying AI algorithms on edge devices can theoretically achieve the complementary combination of edge computing and AI [127]. However, developing devices more suited to edge AI and realizing the theoretical complementarity of edge computing and AI is a great challenge.

The main method for improving the computing power of edge devices is to add intelligent processing modules or intelligent chips to make them more powerful. the hardware of edge devices used in AI algorithms generally includes 1) general computing modules, such as CPU, GPU, FPGA; 2) customized AI processors, such as edge AI modules suitable for specific devices. General computing modules are the most widely used computing hardware of AI. At present, edge devices mainly use general computing modules for AI model training and fitting. Customized AI processors are better suited to specific edge devices and usage scenarios, some emerging technologies and architectures are under development.

2) EI Models: Machine learning is a representative theory that makes artificial intelligence gain practical application. As a new branch of machine learning method, deep learning uses artificial neural networks [128] to fit and learn features of historical data, which has achieved remarkable results in target detection, image recognition, and other fields. Due to the high complexity of deep learning in many machine learning methods, the deployment difficulty is also relatively high. Therefore, this part takes deep learning as an example to discuss the deployment of artificial intelligence in the edge.

a) Model Simplification: Due to the computing power of edge devices is generally weak, it is necessary to compress and simplify the model to adapt to the edge system, so as to improve the processing performance. The main methods of model simplification include weight pruning and data quantification. The weight pruning method sorts the neurons in the waiting simplified model firstly according to the contributions of different neurons. The neurons with small contribution will be removed from the model to reduce the volume of the model [129]. Another commonly used method of model simplification is data quantization. This method uses a data format with fewer bits to represent the input and output of the model input layer, output layer, and hidden layer, reducing the operation law, thus achieving the purpose of improving the operation speed [130].

b) Model Partition: There are three main architectures of deep learning model based on edge computing: 1) devices independent deployment architecture; 2) devices collaboration architecture; and 3) device-server collaboration architecture. In the first architecture, the same deep learning neural network is deployed independently in all edge devices, but it may lead to a serious overload of edge devices. The remain two architectures are proposed for Model Partition. In the second architecture, multiple edge devices jointly deploy a deep neural network and only several layers of the entire deep learning neural network deployed on each device. In the third architecture, edge devices and edge servers jointly deploy a deep learning neural network [127]. Some researches can be used to solve the model partition problem, but it remains in the initial stage and more efforts need to be made.

D. Data Sharing Security

One of the advantages of IIoT is the massive amount of real-time data from multiple devices, sites, and infrastructures. Mining data values and making multi-dimensional business decisions will significantly improve industrial production efficiency [131]. However, the traditional IIoT system is dominated by vertical, closed applications, only focusing on maintaining the proper functioning of a single machine or site, and so the IIoT system constantly creates data islands. Adding edge computing to IIoT subdivides the data and enhances its flexibility. However, the complexity of the data security sharing problem is increased to some extent. Successfully breaking data islands and sharing the same real-time data securely with any type and number of special applications and stakeholders will be a trend of edge-computing-based IIoT systems. There are two problems in edge data sharing: the inevitable increase of data interfaces may lead to more serious consequences, such as intrusion and destruction; and the performance of edge devices is limited, and powerful security algorithms are often difficult to run directly on edge devices. The introduction of blockchain in edge computing in IIoT brings new challenges and opportunities for the secure sharing of data [132].

1) Access Control: The essence of secure data sharing lies in reasonably opening and utilizing data access control, and therefore, access control schemes are the core of data sharing providing the basis and data security. For instance, in IoV the security schemes of edge data sharing must be considered from all angles [92], [133], [134]. The application of the blockchain network to the edge computing system can solve some security problems of the data, but the data can be viewed and verified by all nodes in the system, thus data is exposed to the public and some serious privacy issues raised. Therefore, it is necessary to consider the access control problem under the combination of blockchain and edge computing. Combining the attribute-based access control model and the blockchain may achieve an ideal access control effect, and is worth studying and optimizing. However, the strong distribution and heterogeneity of edge computing need to be specifically considered, so they can be used in the edge computing system based on blockchain.

2) Distributed Storage: The premise of data sharing based on blockchain is the blockchain-based distributed data storage. Following the introduction of blockchain, data generated by edge devices become tamper-proof after being stored using blockchain. Recent researches on distributed storage based on blockchain shows that the InterPlanetary File System (IPFS) combines many excellent protocols and is an ideal distributed storage solution at present. The blockchain data storage based

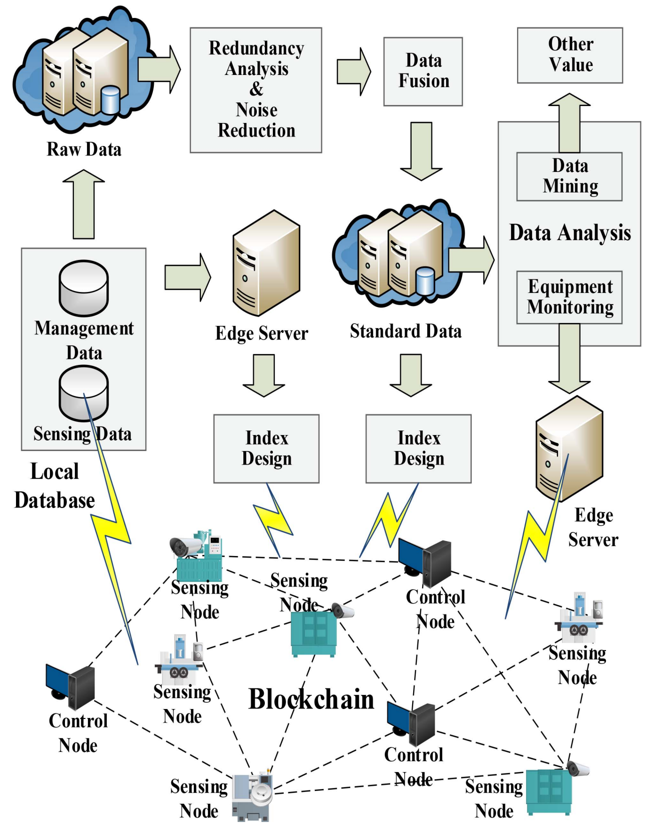

Fig. 5. The Data Flow of Edge Computing in IIoT Based on Blockchain.

on IPFS can store the data generated by the transaction in IPFS and package the returned IPFS hash value into the block, thus greatly reducing the blockchain data volume.

Moreover, blockchain offers business possibilities in various development modes, such as charging for IIoT services in the future. Therefore, blockchain is highly promising for applications in ensuring the security of edge data sharing. However, there has been little research so far discussing the details of systematically incorporating blockchain into edge computing in IIoT to ensure secure edge data sharing. Thus, many problems remain to be researched and solved. The typical data flow in edge computing in IIoT based on blockchain is shown in Figure 5.

E. Summary

In this section, we discuss some challenges and potential solutions of some of applying some new technologies to edge-based IIoT detailedly, including 5G-based edge communication, data offloading and load balancing, edge artificial intelligence and data sharing security. Based on what has been discussed above, the typical challenges and research directions are summarized as follows.

1) 5G-Based Edge Communication Related: For the application of 5G in the IIoT based on edge computing, the most important thing is to greatly improve the communication mode and communication performance. 5G frees most devices from fiber optic cables, making the industrial processes more flexible. With the super-large bandwidth and super-dense base station deployment supported by 5G, more edge devices can be managed and data transmission will be reduced efficiently. The challenges to applying 5G in the edge computing in IIoT focus on QoS, nodes management and network slicing. the QoS standards and schemes are different to 5G and edge computing, the common problems need to be considered comprehensively. A large number of 5G base stations makes it easy to collect and manage edge nodes information, but innovation in edge nodes management scheme should be carried out according to local conditions. The network slicing feature of 5G allows multiple services to be deployed in parallel, but the architectures of the different systems still need to be tailored according to the actual situation. In addition, the hardware transformation of traditional equipment and the remote maintenance schemes for 5G infrastructure are also worthy of attention.

2) Data Offloading and Load Balancing Related: Data offloading and load balancing are always great challenges in IIoT systems based on edge computing because the devices are too many, and the computing resources needed to be scheduled are too distributed. To solve these problems, data offloading and load balancing schemes should be designed for special requirements. As for data offloading, the schemes currently applicable to conventional edge networks can be divided into two categories: full data offloading and partial data offloading. Full data offloading schemes offload all data from a device or edge server to others; while the partial data offloading schemes first divide the task data, and then offload a part data to different devices. The worst case is to offload all the data to other devices. The main objective of the load balancing method is to balance the unbalanced load distribution due to the different storage and computing resources of the edge device and the offloading schemes. In brief, load balancing based on specific characteristics and scenarios combining new technologies is a significant research direction.

3) Edge Artificial Intelligence Related: Edge artificial intelligence provides new opportunities and challenges for data processing in the edge of the system. The challenges mainly focus on two aspects: first, the computing power of edge devices is generally weak, and it is difficult to complete a large amount of computation quickly on edge devices; The second is that the model of edge artificial intelligence is generally complex, which requires more computing resources to complete the training and inference of the model. Based on the existing researches and considering the characteristics of edge computing in IIoT, it is a promising research direction to combine the artificial intelligence and edge computing better.

4) Data Sharing Security Related: The introduction of edge computing enables IIoT data to be processed in real-time on the edge. However, due to the limited resources and huge number of edge devices, many tasks have to be done in collaboration between multiple devices. Therefore, data needs to be securely shared between edge devices to collaborate on tasks. IIoT has high requirements for security, and blockchain can provide security for edge data sharing to some extent. However, the computing resources of edge devices are generally limited, so the design and optimization of edge IIoT architecture based on blockchain are great challenges in access control and secure storage based on blockchain, and more attention should be paid to the direction of the edge IIoT based on blockchain.

VI. Application Scenarios

In this section, several application scenarios, including prognostics and health management (PHM), smart grid, manufacturing, intelligent connected vehicles (ICV), and smart logistics, are presented to demonstrate how edge computing in IIoT is implemented in real-world applications. The application abovementioned scenarios are illustrated in Figure 6.

A. PHM

PHM is a new solution valued by companies globally that using the operation information of system components collected by various sensors, monitoring and evaluating the overall health of the system, predicting and taking appropriate measures before system failure [135]. The PHM system should generally have the capabilities of performance detection, fault detection, fault isolation, fault prediction, enhanced diagnosis, health management, component life tracking, *etc*. PHM links the autonomous support system with the joint distributed information system (JDIS) to predict the time and location of a failure in advance, saving the maintenance costs, improving the operational reliability, and achieving condition-based maintenance.

The purpose of PHM is to monitor the wear and tear, aging, corrosion, and failure of components during the operation of the equipment, to prevent unplanned downtime, which is a serious threat to life and property. The PHM system uses a large number of sensors to monitor the status of components in real-time, which is an important application scenario of IIoT [136]. Owing to the huge volume of sensors and data, and the unforeseen consequences possibly resulting from a delay of the uploading and final decision in the cloud, introducing edge computing to PHM and performing initial processing of data close to sensors will significantly reduce the amount of data uploaded to the cloud, and reduce the decision delays of emergency events.

At present, applications of edge computing in IIoT in PHM are reasonably extensive, and the safety detection of railway tracks is one of the major application cases. The advantages of edge computing are utilized for real-time feature extraction [137] and anomaly detection of railway tracks, monitoring the real-time performance of railway and train operations, and predicting potential failures to prevent unplanned downtime and support optimization decisions. In addition, drones can be used as a source of information for railway track detection [138].

B. Smart Grid

The smart grid is a typical application scenario of IIoT. Its purpose is to achieve node monitoring and information interactions for electrical energy transmission from the power plant to the users [139]. Compared with the traditional power grid, the advantage of a smart power grid lies in the integration of the production, transmission, distribution, security protection

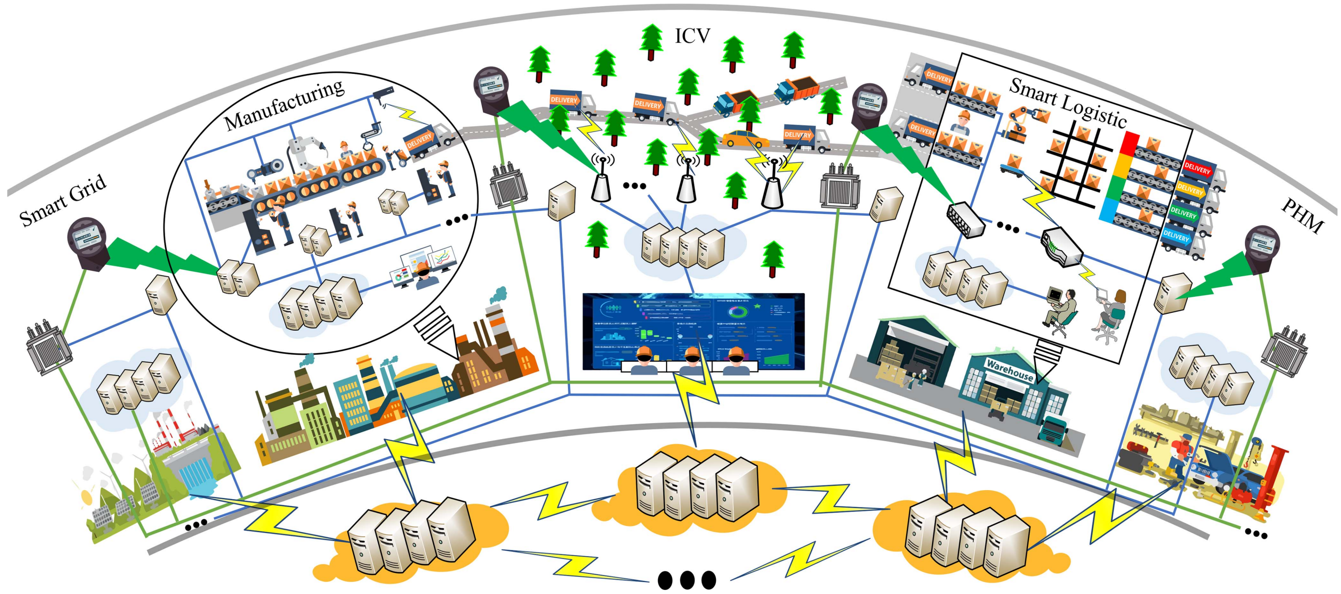

Fig. 6. Application Scenarios of Edge Computing in IIoT.

and other links of power by using advanced information technology. Power grid companies and users can obtain the status of the power grid and electricity consumption information in real-time, so as to improve the overall efficiency of the power grid. At present, a large number of smart meters and various types of sensing devices are deployed in the smart grid. The overall structure is complex, the data types are heterogeneous, and the instantaneous data volume is huge. An edge server can be deployed in the vicinity of the smart meters and sensing devices to solve the problems described above. The collected data is analyzed in situ, and part of the decision is made, to realize regional equipment management and energy efficiency optimization, thus improving the management efficiency and meeting real-time requirements. Each edge server acquires and uploads the data required for equipment maintenance and structure optimization to the cloud center, which processes, analyzes, and trains the collected data centrally.

The smart grid system based on edge computing can intelligently detect the grid structure [140]; distribute the computing, storage, and control services to the edge network; effectively dispense the intelligent resources of the whole power system closer to end-users [15]; and achieve high-demand functions, such as intelligent low-voltage area management, user power management, and distribution of external force damage risk monitoring [141].

C. Manufacturing

There exist many kinds of industrial devices, a huge volume of real-time data, complex communication network topologies and protocols, and high-performance requirements for the real-time and accurate transmission of information [142]. Realizing industrial site coordination of production equipment and software management systems is a considerable challenge. The deployment of edge computing in an industrial manufacturing site, especially combined with NFV technology and real-time network transmission technology, can establish a high-quality network connection from the cloud platform to the industrial field edge computing platform, achieve flexible and isolated application deployment capabilities, and provide intelligent, real-time, secure, and quality-guaranteed manufacturing site industrial network and edge computing services.

A typical application of manufacturing site coordination is the real-time processing of images or videos, which can be applied to product defect detection and classification [19], worker motion correction, or equipment component assembly error checking [143]. The process of image and video processing involves image acquisition, preprocessing, image segmentation, feature extraction, and matching recognition [144], combined in general with an artificial intelligence algorithm, and the image detection model is trained in advance using industrial images or video datasets. To achieve a better performance, it is often necessary to use an incremental learning algorithm to continually modify the model to improve the recognition accuracy [145]. The introduction of edge computing technology can keep the training process on the cloud platform, and the matching recognition process is placed on the edge computing platform, to guarantee the recognition accuracy and reduce the recognition delay.

There are various network access methods in manufacturing sites, such as industrial Ethernet or Fieldbus, and each access method includes multiple protocols, making them difficult to interconnect. The edge computing platform can convert different protocols into a common protocol, to solve the connectivity problem between the various networks of an industrial network. At the same time, a manufacturing site edge computing platform provides management and data interfaces and uses a lightweight network and application virtualization management to remotely manage, upgrade, and maintain a massive number of devices and applications for remote configuration and monitoring. In addition, it can clean and desensitize the collected data to ensure data availability and that sensitive information will not be leaked and combine chip-level secure booting and secure key authentication to provide a secure environment for industrial networks.

D. ICV

With the advent of the 5G era, ICV will become an important IIoT scenario in the future [146]. The Edge-Cloud collaboration will be the core solution for ICV. Cloud computing is equivalent to the super brain of vehicles, dealing with relatively complex processes, such as traffic forecasting in a certain area [14], [147]. Furthermore, edge computing is equivalent to the nerve endings of vehicles, carrying out certain "subconscious" reactions, such as obtaining driving information on surrounding cars or automatic emergency braking.

Automatic driving is a major thread of research in edge computing applied to ICV. Regional automatic driving is relatively simple. In general, the environment information of the entire running area acts as input to the system, and subsequently, the path and speed of a vehicle are planned in advance, to realize the automatic operation of the vehicle in the designated area (such as a small amusement park). In the case of sudden entry of pedestrians or vehicles, edge computing technology is used to compare the image information obtained from the camera with the existing road information in the onboard system and make a judgment, realizing an immediate response. Compared to regional automatic driving, adaptive automatic driving in any environment is rather complex and changeable, with various scenarios and factors to be considered, including vehicle cruising, lane changing assistance, intersection passage, automatic parking, speed control, and path planning. Under these conditions, the detection of surrounding vehicles, identification of traffic lights, and intrusion of emergency obstacles cannot endure delays in uploading data to the cloud. Therefore, edge computing will become the processing center in the above situation. Determining which events are processed on the edge server and which are processed on the on-board system still requires the prioritization of events.

For ICV, on-board entertainment and service are indispensable. A vehicle travels at high speed on the road, and the edge server is fixed on the roadside to support real-time communication with the vehicle. This is similar to the service mode of a mobile phone, except that a mobile phone and car have different moving ranges and speeds. Therefore, the application scenario of ICV is reasonably consistent with research on MEC [32]. Frequent interactions between vehicles, edge servers, and the cloud platform usually require efficient data routing, caching, and offloading strategies to meet the needs of this scenario.

E. Smart Logistic

The logistics industry is becoming one of the important application scenarios of IIoT. The traditional logistics industry, based on RFID technology, only records the storage and distribution information of goods and performs simple replacement and management of goods, and it is difficult to realize logistics storage and distribution operations without manual intervention. With the rapid development of the commodity economy, the full automation of logistics and storage is becoming an important demand, and the recording and management of complete logistics process data is becoming a new trend, such as the recording of relevant data including transportation routes, vehicle statuses, driving behaviors, and goods storage environments.

For the warehousing and distribution of logistics, goods generally pass through the processes of packaging, sorting, stacking, loading, and so on, using RFID tags to identify the information on goods. Robotic arms and seat belts can automate cargo packing, stacking, and loading to reduce manual intervention in traditional logistics. The addition of a logistics robot can optimize the classification and sorting processes of goods, to realize the full automation of warehousing and distribution. In the sorting process, the logistics robot, as an intelligent terminal device, tells the edge server the types of goods it has recognized by RFID tags. The edge server plans the path of the goods from the shelf to the logistics vehicle and passes this back to the robot, which transports the goods according to the instructions, and verifies whether the goods and vehicles match locally [148].

Logistics vehicles transport goods from one warehouse to another, mostly on roads where edge servers or base stations are sparse. To effectively record the status, route, and other information on logistics vehicles, and achieve real-time responses to emergencies, it is necessary to use the on-board intelligent terminal based on edge computing. The on-board intelligent terminal should be able to monitor the whole process for the vehicle status. If any abnormal parts are found, then a real-time alarm and measures should be available, and data should be stored and uploaded to the cloud service platform for data analysis. Monitoring and warning should be performed concerning driver behaviors to reduce the probability of accidents. For some goods requiring special environment transportation, the storage environment can be monitored in real-time to reduce transportation losses. Specific data can be exchanged when a vehicle passes a roadside base station or edge server.

VII. Conclusion

As an emerging industrial solution, IIoT connects devices through advanced communication technologies, enabling the system to monitor, collect, exchange and analyze data, and provide high-value decisions in an unprecedented way, making the industry productivity and performance more efficient than ever. Applying edge computing technology in IIoT can process part of large-scale real-time sensing data on the edge of network close to the data source, solving the key problem of limited transmission bandwidth and long latency making decision from cloud platform.

In this paper, through a comprehensive review of edge computing in IIoT, the development and integration process of IIoT and edge computing are expounded, and the reference architecture of edge computing in IIoT is proposed. Edge computing reference architecture in IIoT is divided into cloud layer and edge layer, and the edge layer can also be subdivided

TABLE VIII
SUMMARY OF IMPORTANT ACRONYMS

Acronym	Defination
3GPP	3rd Generation Partnership Project
AI	Artificial Intelligence
CPS	Cyber-Physical System
ETSI	European Telecommunications Standards Institute
ICV	Intelligent Connected Vehicles
IEEE	Institute of Electrical and Electronics Engineers
IIC	Industrial Internet Consortium
IIoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
IoT	Internet of things
IoV	Internet of Vehicles
ITU	International Telecommunication Union
LPWAN	Low-Power Wide Area Networks
M2M	Machine to Machine
MEC	Mobile Edge Computing (before 2017) Multi-access Edge Computing (after 2017)
NFV	Network Function Virtualization
PHM	Prognostic and Health Management
QoS	Quality of Service
RAMI	The Reference Architecture Model Industry 4.0
RFID	Radio Frequency Identification
RSU	Road Side Units
SDN	Software Defined Networks
SITAM	The Stuttgart IT-Architecture for Manufacturing
UDN	Ultra-Dense Network
VANET	Vehicular Ad-hoc Networks
WSN	Wireless Sensing Networks

into Near-Edge, Mid-Edge and Far-Edge. For the advanced technologies of edge computing in IIoT, we have made a comprehensive elaboration from the perspectives of routing, task scheduling, data storage and analytics, security and standardization. The challenges of edge computing in IIoT are analyzed and discussed from the perspectives of 5G-based edge communication, load balancing, edge AI and secure data sharing. The combination of edge computing with blockchain, machine learning, SDN and 5G will become an obvious trend. In addition, we discussed several typical scenarios of application, hoping to be helpful to the promotion and application of edge computing in IIoT. Different from other IIoT or edge computing survey papers, the main contribution of this paper is to emphasize the fusion application of IIoT and edge computing, trying to clarify the importance of the future of edge computing in IIoT, so as to make the topic obtain more attention from other researchers and make industry development more rapid and convenient.

APPENDIX

Some important acronyms appeared in paper are listed in Table VIII.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of Things: A survey on enabling technologies, protocols, and applications," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2347–2376, 4th Quart., 2015.

[2] E. Sisinni, A. Saifullah, S. Han, U. Jennehag, and M. Gidlund, "Industrial Internet of Things: Challenges, opportunities, and directions," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4724–4734, Nov. 2018.

[3] P. P. Gaikwad, J. P. Gabhane, and S. S. Golait, "A survey based on smart homes system using Internet-of-Things," in *Proc. Int. Conf. Comput. Power Energy Inf. Commun. (ICCPEIC)*, Chennai, India, 2015, pp. 0330–0335.

[4] L. Xu, W. He, and S. Li, "Internet of Things in industries: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2233–2243, Nov. 2014.

[5] D. S. Nunes, P. Zhang, and J. S. Silva, "A survey on human-in-the-loop applications towards an Internet of all," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 2, pp. 944–965, 2nd Quart., 2015.

[6] I. Stojmenovic, "Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems," *IEEE Internet Things J.*, vol. 1, no. 2, pp. 122–128, Apr. 2014.

[7] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," *J. Inf. Security Appl.*, vol. 38, pp. 8–27, Feb. 2018.

[8] A. C. Panchal, V. M. Khadse, and P. N. Mahalle, "Security issues in IIoT: A comprehensive survey of attacks on IIoT and its countermeasures," in *Proc. IEEE Global Conf. Wireless Comput. Netw. (GCWCN)*, Lonavala, India, 2018, pp. 124–130.

[9] H. Xu, W. Yu, D. Griffith, and N. Golmie, "A survey on Industrial Internet of Things: A cyber-physical systems perspective," *IEEE Access*, vol. 6, pp. 78238–78259, 2018.

[10] Y. Lu, "Industry 4.0: A survey on technologies, applications and open research issues," *J. Ind. Inf. Integr.*, vol. 6, pp. 1–10, Jun. 2017.

[11] J. Li, F. R. Yu, G. Deng, C. Luo, Z. Ming, and Q. Yan, "Industrial Internet: A survey on the enabling technologies, applications, and challenges," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1504–1526, 3rd Quart., 2017.

[12] T. Qiu, B. Li, X. Zhou, H. Song, I. Lee, and J. Lloret, "A novel shortcut addition algorithm with particle swarm for multisink Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 16, no. 5, pp. 3566–3577, May 2020.

[13] P. K. Illa and N. Padhi, "Practical guide to smart factory transition using IoT, big data and edge analytics," *IEEE Access*, vol. 6, pp. 55162–55170, 2018.

[14] A. Thakur and R. Malekian, "Fog computing for detecting vehicular congestion, an Internet of Vehicles based approach: A review," *IEEE Intell. Transp. Syst. Mag.*, vol. 11, no. 2, pp. 8–16, Mar. 2019.

[15] H. Wang, Q. Wang, Y. Li, G. Chen, and Y. Tang, "Application of fog architecture based on multi-agent mechanism in CPPS," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Beijing, China, 2018, pp. 1–6.

[16] N. Yoshikane *et al.*, "First demonstration of geographically unconstrained control of an industrial robot by jointly employing SDN-based optical transport networks and edge compute," in *Proc. 21st OptoElectron. Commun. Conf. (OECC) Held Jointly Int. Conf. Photon. Switching (PS)*, Niigata, Japan, 2016, pp. 1–3.

[17] I. A. Tsokalo, H. Wu, G. T. Nguyen, H. Salah, and F. H. P. Fitzek, "Mobile edge cloud for robot control services in industry automation," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2019, pp. 1–2.

[18] T. M. Jose, "A novel sensor based approach to predictive maintenance of machines by leveraging heterogeneous computing," in *Proc. IEEE SENSORS*, New Delhi, India, 2018, pp. 1–4.

[19] L. Li, K. Ota, and M. Dong, "Deep learning for smart industry: Efficient manufacture inspection system with fog computing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4665–4673, Oct. 2018.

[20] W. Shi, J. Cao, Q. Zhang, Y. Li, and L. Xu, "Edge computing: Vision and challenges," *IEEE Internet Things J.*, vol. 3, no. 5, pp. 637–646, Oct. 2016.

[21] B. Flavio, M. Rodolfo, Z. Jiang, and A. Sateesh, "Fog computing and its role in the Internet of Things," in *Proc. 1st Edition MCC Workshop Mobile Cloud Comput.*, 2012, pp. 13–16.

[22] L. M. Vaquero and L. Rodero-Merino, "Finding your way in the definition fog: Towards a comprehensive of fog computing," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 44, no. 5, pp. 27–32, 2014.

[23] A. C. Baktir, A. Ozgovde, and C. Ersoy, "How can edge computing benefit from software-defined networking: A survey, use cases, and future directions," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 4, pp. 2359–2391, 4th Quart., 2017.

[24] P. Mach and Z. Becvar, "Mobile edge computing: A survey on architecture and computation offloading," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1628–1656, 3rd Quart., 2017.

[25] M. Mukherjee, L. Shu, and D. Wang, "Survey of fog computing: Fundamental, network applications, and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 1826–1857, 3rd Quart., 2018.
[26] R. K. Naha *et al.*, "Fog computing: Survey of trends, architectures, requirements, and research directions," *IEEE Access*, vol. 6, pp. 47980–48009, 2018.
[27] C. Mouradian, D. Naboulsi, S. Yangui, R. H. Glitho, M. J. Morrow, and P. A. Polakos, "A comprehensive survey on fog computing: State-of-the-art and research challenges," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 1, pp. 416–464, 1st Quart., 2018.
[28] T. Taleb, K. Samdanis, B. Mada, H. Flinck, S. Dutta, and D. Sabella, "On multi-access edge computing: A survey of the emerging 5G network edge cloud architecture and orchestration," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 3, pp. 1657–1681, 3rd Quart., 2017.
[29] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018.
[30] I. Sitton-Candanedo, R. S. Alonso, S. Rodriguez-Gonzalez, J. A. Garcia Coria, and F. De La Prieta, "Edge computing architectures in industry 4.0: A general survey and comparison," in *Proc. 14th Int. Conf. Soft Comput. Models Ind. Environ. Appl.*, vol. 950, 2020, pp. 121–131.
[31] J. Moura and D. Hutchison, "Game theory for multi-access edge computing: Survey, use cases, and future trends," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1, pp. 260–288, 1st Quart., 2019.
[32] F. Giust *et al.*, "Multi-access edge computing: The driver behind the wheel of 5G-connected cars," *IEEE Commun. Stand. Mag.*, vol. 2, no. 3, pp. 66–73, Sep. 2018.
[33] M. Agiwal, A. Roy, and N. Saxena, "Next generation 5G wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1617–1655, 3rd Quart., 2016.
[34] F. Lingen *et al.*, "The unavoidable convergence of NFV, 5G, and fog: A model-driven approach to bridge cloud and edge," *IEEE Commun. Mag.*, vol. 55, no. 8, pp. 28–35, Aug. 2017.
[35] R. Cziva and D. P. Pezaros, "Container network functions: Bringing NFV to the network edge," *IEEE Commun. Mag.*, vol. 55, no. 6, pp. 24–31, Jun. 2017.
[36] X. Huang, R. Yu, J. Kang, Y. He, and Y. Zhang, "Exploring mobile edge computing for 5G-enabled software defined vehicular networks," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 55–63, Dec. 2017.
[37] J. Zhang, B. Chen, Y. Zhao, X. Cheng, and F. Hu, "Data security and privacy-preserving in edge computing paradigm: Survey and open issues," *IEEE Access*, vol. 6, pp. 18209–18237, 2018.
[38] J. Ni, X. Lin, and X. S. Shen, "Toward edge-assisted Internet of Things: From security and efficiency perspectives," *IEEE Netw.*, vol. 33, no. 2, pp. 50–57, Mar./Apr. 2019.
[39] Y. Guan, J. Shao, G. Wei, and M. Xie, "Data security and privacy in fog computing," *IEEE Netw.*, vol. 32, no. 5, pp. 106–111, Sep./Oct. 2018.
[40] M. Aazam, S. Zeadally, and K. A. Harras, "Deploying fog computing in Industrial Internet of Things and industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4674–4682, Oct. 2018.
[41] R. Basir, S. Qaisar, M. Ali, M. Aldwairi, M. I. Ashraf, A. Mahmood, and M. Gidlund, "Fog computing enabling Industrial Internet of Things: State-of-the-art and research challenges," *Sensors (Switzerland)*, vol. 19, no. 21, p. 4807, 2019.
[42] D. Georgakopoulos, P. P. Jayaraman, M. Fazia, M. Villari, and R. Ranjan, "Internet of Things and edge cloud computing roadmap for manufacturing," *IEEE Cloud Comput.*, vol. 3, no. 4, pp. 66–73, Jul./Aug. 2016.
[43] A. Seitz, D. Buchinger, and B. Bruegge, "The conjunction of fog computing and the Industrial Internet of Things—An applied approach," in *Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops*, Athens, Greece, 2018, pp. 812–817.
[44] W. Steiner and S. Poledna, "Fog computing as enabler for the Industrial Internet of Things," *Elektrotechnik und Informationstechnik*, vol. 133, no. 7, pp. 310–314, 2016.
[45] J. M. Talavera *et al.*, "Review of IoT applications in agro-industrial and environmental fields," *Comput. Electron. Agric.*, vol. 142, pp. 283–297, Nov. 2017.
[46] C. Weber, J. Köenigsberger, L. Kassner, and B. Mitschang, "M2DDM—A maturity model for data-driven manufacturing," *Procedia CIRP*, vol. 63, pp. 173–178, May 2017.
[47] J. Wang, J. Liu, and N. Kato, "Networking and communications in autonomous driving: A survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1243–1274, 2nd Quart., 2019.
[48] A. Ahmadi, M. Moradi, C. Cherifi, V. Cheutet, and Y. Ouzrout, "Wireless connectivity of CPS for smart manufacturing: A survey," in *Proc. 12th Int. Conf. Softw. Knowl. Inf. Manag. Appl. (SKIMA)*, Phnom Penh, Cambodia, Dec. 2018, pp. 1–8.
[49] P. G. V. Naranjo, M. Shojafar, A. Abraham, and E. Baccarelli, "A new stable election-based routing algorithm to preserve aliveness and energy in fog-supported wireless sensor networks," in *Proc. IEEE Int. Conf. Syst. Man Cybern. (SMC)*, Budapest, Hungary, 2016, pp. 002413–002418.
[50] N. B. Long, H. Tran-Dang, and D. Kim, "Energy-aware real-time routing for large-scale Industrial Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2190–2199, Jun. 2018.
[51] E. M. Borujeni, D. Rahbari, and M. Nickray, "Fog-based energy-efficient routing protocol for wireless sensor networks," *J. Supercomput.*, vol. 74, no. 12, pp. 6831–6858, 2018.
[52] J. Fu, B. Cui, N. Wang, and X. Liu, "A distributed position-based routing algorithm in 3-D wireless Industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5664–5673, Oct. 2019.
[53] T. Lu, S. Chang, and W. Li, "Fog computing enabling geographic routing for urban area vehicular network," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 4, pp. 749–755, 2018.
[54] P. Bezerra, A. Melo, A. Douglas, H. Santos, D. D. Rosário, and E. Cerqueira, "A collaborative routing protocol for video streaming with fog computing in vehicular ad hoc networks," *Int. J. Distrib. Sens. Netw.*, vol. 15, no. 3, p. 1, 2019.
[55] A. J. Kadhim and S. Hosseini-Seno, "Energy-efficient multicast routing protocol based on SDN and fog computing for vehicular networks," *Ad Hoc Netw.*, vol. 84, pp. 68–81, Mar. 2019.
[56] P. Thandapani, M. Arunachalam, and D. Sundarraj, "An energy-efficient clustering and multipath routing for mobile wireless sensor network using game theory," *Int. J. Commun. Syst.*, vol. 33, no. 7, p. e4336, 2020.
[57] N. G. Nayak, F. Duerr, and K. Rothermel, "Incremental flow scheduling and routing in time-sensitive software-defined networks," *IEEE Trans. Ind. Inf.*, vol. 14, no. 5, pp. 2066–2075, May 2018.
[58] K. Kaur, S. Garg, G. S. Aujla, N. Kumar, J. J. P. C. Rodrigues, and M. Guizani, "Edge computing in the Industrial Internet of Things environment: Software-defined-networks-based edge-cloud interplay," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 44–51, Feb. 2018.
[59] X. Li, D. Li, J. Wan, C. Liu, and M. Imran, "Adaptive transmission optimization in SDN-based Industrial Internet of Things with edge computing," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1351–1360, Jun. 2018.
[60] M. Al-Hubaishi, C. Çeken, and A. B. Al-Shaikhli, "A novel energy-aware routing mechanism for SDN-enabled WSAN," *Int. J. Commun. Syst.*, vol. 32, no. 17, p. e3724, 2019.
[61] F. Y. Okay and S. Ozdemir, "Routing in fog-enabled IoT platforms: A survey and an SDN-based solution," *IEEE Internet Things J.*, vol. 5, no. 6, pp. 4871–4889, Dec. 2018.
[62] L. Yin, J. Luo, and H. Luo, "Tasks scheduling and resource allocation in fog computing based on containers for smart manufacturing," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4712–4721, Oct. 2018.
[63] A. Yousefpour, G. Ishigaki, and J. P. Jue, "Fog computing: Towards minimizing delay in the Internet of Things," in *Proc. IEEE Int. Conf. Edge Comput. (EDGE)*, Honolulu, HI, USA, 2017, pp. 17–24.
[64] W. Masri, I. A. Ridhawi, N. Mostafa, and P. Pourghomi, "Minimizing delay in IoT systems through collaborative fog-to-fog (F2F) communication," in *Proc. 9th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Milan, Italy, 2017, pp. 1005–1010.
[65] Z. Liu, X. Yang, Y. Yang, K. Wang, and G. Mao, "DATS: Dispersive stable task scheduling in heterogeneous fog networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3423–3436, Apr. 2019.
[66] Z. Fei, Y. Wang, R. Sun, and Y. Liu, "Delay-oriented task scheduling and bandwidth allocation in fog computing networks," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Waikoloa, HI, USA, 2019, pp. 1–6.
[67] G. Zhang, F. Shen, Y. Zhang, R. Yang, Y. Yang, and E. A. Jorswieck, "Delay minimized task scheduling in fog-enabled IoT networks," in *Proc. 10th Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Hangzhou, China, 2018, pp. 1–6.
[68] X. Chen and J. Zhang, "When D2D meets cloud: Hybrid mobile task offloadings in fog computing," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.
[69] R. Deng, R. Lu, C. Lai, T. H. Luan, and H. Liang, "Optimal workload allocation in fog-cloud computing toward balanced delay and power consumption," *IEEE Internet Things J.*, vol. 3, no. 6, pp. 1171–1181, Dec. 2016.

[70] G. Zhang, F. Shen, N. Chen, P. Zhu, X. Dai, and Y. Yang, "DOTS: Delay-optimal task scheduling among voluntary nodes in fog networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 3533–3544, Apr. 2019.

[71] Y. Yang, S. Zhao, W. Zhang, Y. Chen, X. Luo, and J. Wang, "DEBTS: Delay energy balanced task scheduling in homogeneous fog networks," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 2094–2106, Jun. 2018.

[72] P. Basanta-Val, "An efficient industrial big-data engine," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1361–1369, Apr. 2018.

[73] Y. Li, J. Luo, J. Jin, R. Xiong, and F. Dong, "An effective model for edge-side collaborative storage in data-intensive edge computing," in *Proc. IEEE 22nd Int. Conf. Comput. Supported Cooperative Work Design (CSCWD)*, Nanjing, China, 2018, pp. 92–97.

[74] T. Nagato, T. Tsutano, T. Kamada, Y. Takaki, and C. Ohta, "Distributed key-value storage for edge computing and its explicit data distribution method," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Kuala Lumpur, Malaysia, 2019, pp. 147–152.

[75] S. K. Monga, S. K. Ramachandra, and Y. Simmhan, "ElfStore: A resilient data storage service for federated edge and fog resources," in *Proc. IEEE Int. Conf. Web Serv. (ICWS)*, Milan, Italy, Jul. 2019, pp. 336–345.

[76] R. Mayer, H. Gupta, E. Saurez, and U. Ramachandran, "FogStore: Toward a distributed data store for fog computing," in *Proc. IEEE Fog World Congr. (FWC)*, Santa Clara, CA, USA, 2017, pp. 1–6.

[77] G. Kamath, P. Agnihotri, M. Valero, K. Sarker, and W. Song, "Pushing analytics to the edge," in *Proc. IEEE Global Commun. Conf. (GLOBECOM)*, Washington, DC, USA, 2016, pp. 1–6.

[78] M. Taneja, N. Jalodia, and A. Davy, "Distributed decomposed data analytics in fog enabled IoT deployments," *IEEE Access*, vol. 7, pp. 40969–40981, 2019.

[79] G. Li, P. Zhao, X. Lu, J. Liu, and Y. Shen, "Data analytics for fog computing by distributed online learning with asynchronous update," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, 2019, pp. 1–6.

[80] Y. Han, B. Park, and J. Jeong, "Fog based IIoT architecture based on big data analytics for 5G-networked smart factory," in *Proc. 19th Int. Conf. Comput. Sci. Appl. (ICCSA)*, Saint Petersburg, Russia, Jul. 2019, pp. 44–52.

[81] T. Zhang, Z. Shen, J. Jin, A. Tagami, X. Zheng, and Y. Yang, "ESDA: An energy-saving data analytics fog service platform," in *Proc. 17th Int. Conf. Serv. Orient. Comput. (ICSOC)*, Toulouse, France, Oct. 2019, pp. 171–185.

[82] T. Qiu, J. Liu, W. Si, and D. O. Wu, "Robustness optimization scheme with multi-population co-evolution for scale-free wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 27, no. 3, pp. 1028–1042, Jun. 2019.

[83] A. Diro and N. Chilamkurti, "Leveraging LSTM networks for attack detection in fog-to-things communications," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 124–130, Sep. 2018.

[84] D. A. Chekired, L. Khoukhi, and H. T. Mouftah, "Fog-based distributed intrusion detection system against false metering attacks in smart grid," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Shanghai, China, 2019, pp. 1–6.

[85] T. Singh and B. Aksanli, "Real-time traffic monitoring and SQL injection attack detection for edge networks," in *Proc. 15th ACM Int. Symp. QoS Security Wireless Mobile Netw.*, Miami Beach, FL, USA, Nov. 2019, pp. 29–36.

[86] M. Wazid, P. R. Dsouza, A. K. Das, V. Bhat K., N. Kumar, and J. J. P. C. Rodrigues, "RAD-EI: A routing attack detection scheme for edge-based Internet of Things environment," *Int. J. Commun. Syst.*, vol. 32, no. 15, p. e4024, 2019.

[87] Q. Yan, W. Huang, X. Luo, Q. Gong, and F. R. Yu, "A multi-level DDOS mitigation framework for the Industrial Internet of Things," *IEEE Commun. Mag.*, vol. 56, no. 2, pp. 30–36, Feb. 2018.

[88] L. Zhou, H. Guo, and G. Deng, "A fog computing based approach to DDOS mitigation in IIoT systems," *Comput. Security*, vol. 85, pp. 51–62, Aug. 2019.

[89] J. Liu, C. Yuan, Y. Lai, and H. Qin, "Protection of sensitive data in industrial Internet based on three-layer local/fog/cloud storage," *Security Commun. Netw.*, vol. 2020, Apr. 2020, Art. no. 2017930.

[90] S. He, B. Cheng, H. Wang, X. Xiao, Y. Cao, and J. Chen, "Data security storage model for fog computing in large-scale IoT application," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Honolulu, HI, USA, 2018, pp. 39–44.

[91] Y. Ming and X. Yu, "Efficient privacy-preserving data sharing for fog-assisted vehicular sensor networks," *Sensors*, vol. 20, no. 2, p. 514, 2020.

[92] K. Xue, J. Hong, Y. Ma, D. S. L. Wei, P. Hong, and N. Yu, "Fog-aided verifiable privacy preserving access control for latency-sensitive data sharing in vehicular cloud computing," *IEEE Netw.*, vol. 32, no. 3, pp. 7–13, May/Jun. 2018.

[93] K. Fan, J. Wang, X. Wang, H. Li, and Y. Yang, "Secure, efficient and revocable data sharing scheme for vehicular fogs," *Peer-to-Peer Netw. Appl.*, vol. 11, no. 4, pp. 766–777, 2018.

[94] *SmartM2M; IoT Standards Landscape and Future Evolutions*, Eur. Telecommun. Stand. Inst., Sophia Antipolis, France, Oct. 2016. [Online]. Available: https://www.etsi.org

[95] *Tactile Internet: Application Scenarios, Definitions and Terminology, Architecture, Functions, and Technical Assumptions*, Inst. Elect. Electron. Eng., Piscataway, NJ, USA, Mar. 2016. [Online]. Available: https://standards.ieee.org

[96] *The Industrial Internet of Things Volume G1: Reference Architecture*, Ind. Internet Consortium, Needham, MA, USA, Jan. 2017. [Online]. Available: https://www.iiconsortium.org

[97] *Industrial Networking Enabling IIoT Communication*, Ind. Internet Consortium, Needham, MA, USA, Aug. 2018. [Online]. Available: https://www.iiconsortium.org

[98] *Key Safety Challenges for the IIoT*, Ind. Internet Consortium, Needham, MA, USA, Dec. 2017. [Online]. Available: https://www.iiconsortium.org

[99] *IoT Security Maturity Model Description and Intended Use*, Ind. Internet Consortium, Needham, MA, USA, Feb. 2019. [Online]. Available: https://www.iiconsortium.org

[100] *OpenFog Reference Architecture for Fog Computing*, OpenFog Consortium, Fremont, CA, USA, Feb. 2017. [Online]. Available: https://www.iiconsortium.org

[101] *IEEE Standard for Adoption of OpenFog Reference Architecture for Fog Computing*, Inst. Elect. Electron. Eng., Piscataway, NJ, USA, Jun. 2018. [Online]. Available: https://standards.ieee.org

[102] *Signalling Requirements and Architecture of Intelligent Edge Computing*, Int. Telecommun. Union, Geneva, Switzerland, Oct. 2018. [Online]. Available: https://www.itu.int

[103] *Introduction to Edge Computing in IIoT*, Industrial Internet Consortium, Needham, MA, USA, Jun. 2018. [Online]. Available: https://www.iiconsortium.org

[104] *The Edge Computing Advantage*, Industrial Internet Consortium, Needham, MA, USA, Oct. 2019. [Online]. Available: https://www.iiconsortium.org

[105] A. Aijaz, Z. Dawy, N. Pappas, M. Simsek, S. Oteafy, and O. Holland, "Toward a tactile Internet reference architecture: Vision and progress of the IEEE p1918.1 standard," 2018. [Online]. Available: https://arxiv.org/abs/1807.11915.

[106] B. A. Martin *et al.*, "OpenFog security requirements and approaches," in *Proc. IEEE Fog World Congr. (FWC)*, Santa Clara, CA, USA, 2017, pp. 1–6.

[107] N. Chen, T. Qiu, X. Zhou, K. Li, and M. Atiquzzaman, "An intelligent robust networking mechanism for the Internet of Things," *IEEE Commun. Mag.*, vol. 57, no. 11, pp. 91–95, Nov. 2019.

[108] S. Vitturi, C. Zunino, and T. Sauter, "Industrial communication systems and their future challenges: Next-generation ethernet, IIoT, and 5G," *Proc. IEEE*, vol. 107, no. 6, pp. 944–961, Jun. 2019.

[109] T. Qiu, B. Li, W. Qu, E. Ahmed, and X. Wang, "TOSG: A topology optimization scheme with global small world for industrial heterogeneous Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 15, no. 6, pp. 3174–3184, Jun. 2019.

[110] J. G. Andrews *et al.*, "What will 5G be?" *IEEE J. Sel. Areas Commun.*, vol. 32, no. 6, pp. 1065–1082, Jun. 2014.

[111] T. O. Olwal, K. Djouani, and A. M. Kurien, "A survey of resource management toward 5G radio access networks," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1656–1686, 3rd Quart., 2016.

[112] L. Chettri and R. Bera, "A comprehensive survey on Internet of Things (IoT) toward 5G wireless systems," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 16–32, Jan. 2020.

[113] G. Bag, L. Thrybom, and P. Hovila, "Challenges and opportunities of 5G in power grids," *CIRED Open Access Proc. J.*, vol. 2017, no. 1, pp. 2145–2148, Oct. 2017.

[114] A. Santoyo González and C. Cervelló Pastor, "Edge computing node placement in 5G networks: A latency and reliability constrained framework," in *Proc. 6th IEEE Int. Conf. Cyber Security Cloud Comput. (CSCloud) 5th IEEE Int. Conf. Edge Comput. Scalable Cloud (EdgeCom)*, Paris, France, Jun. 2019, pp. 183–189.

[115] N. Kumareshan and P. Poongodi, "Dynamic mobility management architecture to improve quality of experience (QOE) in wireless networks," in *Proc. 10th Int. Conf. Intell. Syst. Control (ISCO)*, Coimbatore, India, Jan. 2016, pp. 1–4.

[116] S. Dawaliby, A. Bradai, and Y. Pousset, "Network slicing optimization in large scale LoRa wide area networks," in *Proc. IEEE Conf. Netw. Softw. (NetSoft)*, Paris, France, Jun. 2019, pp. 72–77.

[117] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.
[118] D. Puthal, M. S. Obaidat, P. Nanda, M. Prasad, S. P. Mohanty, and A. Y. Zomaya, "Secure and sustainable load balancing of edge data centers in fog computing," *IEEE Commun. Mag.*, vol. 56, no. 5, pp. 60–65, May 2018.
[119] E. E. Haber, T. M. Nguyen, and C. Assi, "Joint optimization of computational cost and devices energy for task offloading in multi-tier edge-clouds," *IEEE Trans. Commun.*, vol. 67, no. 5, pp. 3407–3421, May 2019.
[120] L. Liu, S. Chan, G. Han, M. Guizani, and M. Bandai, "Performance modeling of representative load sharing schemes for clustered servers in multiaccess edge computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4880–4888, Jun. 2019.
[121] Y. Dai, D. Xu, S. Maharjan, and Y. Zhang, "Joint load balancing and offloading in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4377–4387, Jun. 2019.
[122] J. Liu, Y. Mao, J. Zhang, and K. B. Letaief, "Delay-optimal computation task scheduling for mobile-edge computing systems," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Barcelona, Spain, Jul. 2016, pp. 1451–1455.
[123] M. Kamoun, W. Labidi, and M. Sarkiss, "Joint resource allocation and offloading strategies in cloud enabled cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, London, U.K., Jun. 2015, pp. 5529–5534.
[124] S. Cao, X. Tao, Y. Hou, and Q. Cui, "An energy-optimal offloading algorithm of mobile computing based on hetnets," in *Proc. Int. Conf. Connected Veh. Expo (ICCVE)*, Shenzhen, China, Oct. 2015, pp. 254–258.
[125] O. Muñoz, A. Pascual-Iserte, and J. Vidal, "Joint allocation of radio and computational resources in wireless application offloading," in *Proc. Future Netw. Mobile Summit*, Lisboa, Portugal, Jul. 2013, pp. 1–10.
[126] T. Qiu, H. Wang, K. Li, H. Ning, A. K. Sangaiah, and B. Chen, "SIGMM: A novel machine learning algorithm for spammer identification in industrial mobile cloud computing," *IEEE Trans. Ind. Informat.*, vol. 15, no. 4, pp. 2349–2359, Apr. 2019.
[127] Z. Zhou, X. Chen, E. Li, L. Zeng, K. Luo, and J. Zhang, "Edge intelligence: Paving the last mile of artificial intelligence with edge computing," *Proc. IEEE*, vol. 107, no. 8, pp. 1738–1762, Aug. 2019.
[128] D. Svozil, V. Kvasnicka, and J. Pospichal, "Introduction to multi-layer feed-forward neural networks," in *Proc. Chemomet. IV Conf.*, vol. 39, 1997, pp. 43–62.
[129] S. Han, J. Pool, J. Tran, and W. J. Dally, "Learning both weights and connections for efficient neural networks," in *Proc. 29th Annu. Conf. Neural Inf. Process. Syst.*, vol. 1, 2015, pp. 1135–1143.
[130] H. Yan, E. C. Ahn, and L. Duan, "Work-in-progress: Enabling nvm-based deep learning acceleration using nonuniform data quantization," in *Proc. Int. Conf. Compilers Archit. Synth. Embedded Syst. (CASES)*, Seoul, South Korea, Oct. 2017, pp. 1–2.
[131] M. Jbair, B. Ahmad, M. H. Ahmad, and R. Harrison, "Industrial cyber physical systems: A survey for control-engineering tools," in *Proc. IEEE Ind. Cyber Phys. Syst. (ICPS)*, St. Petersburg, Russia, 2018, pp. 270–276.
[132] M. Frey *et al.*, "Security for the industrial IoT: The case for information-centric networking," in *Proc. IEEE 5th World Forum Internet Things (WF-IoT)*, Limerick, Ireland, 2019, pp. 424–429.
[133] Q. Zhang, Q. Zhang, W. Shi, and H. Zhong, "Firework: Data processing and sharing for hybrid cloud-edge analytics," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 9, pp. 2004–2017, Sep. 2018.
[134] J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.
[135] X. Yi, Y. Chen, P. Hou, and Q. Wang, "A survey on prognostic and health management for special vehicles," in *Proc. Prognostics Syst. Health Manag. Conf. (PHM-Chongqing)*, Chongqing, China, 2018, pp. 201–208.
[136] A. L. Ellefsen, V. Æsøy, S. Ushakov, and H. Zhang, "A comprehensive survey of prognostics and health management based on deep learning for autonomous ships," *IEEE Trans. Rel.*, vol. 68, no. 2, pp. 720–740, Jun. 2019.
[137] Z. Liu *et al.*, "Industrial AI enabled prognostics for high-speed railway systems," in *Proc. IEEE Int. Conf. Prognostics Health Manag. (ICPHM)*, Seattle, WA, USA, 2018, pp. 1–8.
[138] J. Yang, X. Cheng, Y. Wu, Y. Qin, and L. Jia, "Railway comprehensive monitoring and warning system framework based on space-air-vehicle-ground integration network," in *Proc. Prognostics Syst. Health Manag. Conf. (PHM-Chongqing)*, Chongqing, China, 2018, pp. 1314–1319.
[139] H. Farhangi, "The path of the smart grid," *IEEE Power Energy Mag.*, vol. 8, no. 1, pp. 18–28, Jan./Feb. 2010.
[140] G. Lin *et al.*, "Community detection in power grids based on louvain heuristic algorithm," in *Proc. IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Beijing, China, 2017, pp. 1–4.
[141] C. Jinming, J. Wei, J. Hao, G. Yajuan, N. Guoji, and C. Wu, "Application prospect of edge computing in smart distribution," in *Proc. China Int. Conf. Elect. Distrib. (CICED)*, Tianjin, China, 2018, pp. 1370–1375.
[142] F. Shrouf, J. Ordieres, and G. Miragliotta, "Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the Internet of Things paradigm," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manag.*, Bandar Sunway, Malaysia, 2014, pp. 697–701.
[143] H. Kanzaki, K. Schubert, and N. Bambos, "Video streaming schemes for industrial IoT," in *Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Vancouver, BC, Canada, 2017, pp. 1–7.
[144] A. Sabu and K. Sreekumar, "Literature review of image features and classifiers used in leaf based plant recognition through image analysis approach," in *Proc. Int. Conf. Invent. Commun. Comput. Technol. (ICICCT)*, Coimbatore, India, 2017, pp. 145–149.
[145] Y. Wang and M. Weyrich, "An adaptive image processing system based on incremental learning for industrial applications," in *Proc. IEEE Emerg. Technol. Factory Autom. (ETFA)*, Barcelona, Spain, 2014, pp. 1–4.
[146] C. Chen, J. Hu, T. Qiu, M. Atiquzzaman, and Z. Ren, "CVCG: Cooperative V2V-aided transmission scheme based on coalitional game for popular content distribution in vehicular ad-hoc networks," *IEEE Trans. Mobile Comput.*, vol. 18, no. 12, pp. 2811–2828, Dec. 2019.
[147] S. Yang, Y. Su, Y. Chang, and H. Hung, "Short-term traffic prediction for edge computing-enhanced autonomous and connected cars," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3140–3153, Apr. 2019.
[148] C. Lin and J. Yang, "Cost-efficient deployment of fog computing systems at logistics centers in industry 4.0," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4603–4611, Oct. 2018.

Tie Qiu (Senior Member, IEEE) received the Ph.D. degree in computer science from the Dalian University of Technology in 2012. He is currently a Full Professor with the School of Computer Science and Technology, College of Intelligence and Computing, Tianjin University, China. He held an Assistant Professor in 2008 and an Associate Professor in 2013 with the School of Software, Dalian University of Technology. He was a Visiting Professor of electrical and computer engineering with Iowa State University, USA, from 2014 to 2015. He serves as a general chair, a program chair, a workshop chair, a publicity chair, a publication chair, or a TPC member of a number of international conferences. He has authored/coauthored nine books, over 100 scientific papers in international journals and conference proceedings, such as the IEEE/ACM TRANSACTIONS ON NETWORKING, the IEEE TRANSACTIONS ON MOBILE COMPUTING, TKDE TII, TIP, TCY, TITS, TVT, IEEE COMMUNICATIONS SURVEYS AND TUTORIALS, *IEEE Communications Magazine*, INFOCOM, and GLOBECOM. There are ten papers listed as ESI highly cited papers. He has contributed to the development of three copyrighted software systems and invented 14 patents. He serves as an Associate Editor for the IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, an Area Editor for *Ad Hoc Networks* (Elsevier), an Associate Editor for IEEE ACCESS, *Computers and Electrical Engineering* (Elsevier), and *Human-Centric Computing and Information Sciences* (Springer), and a Guest Editor for *Future Generation Computer Systems*. He is a Senior Member of the China Computer Federation and ACM.

Jiancheng Chi received the bachelor's degree from the School of Mechanical Engineering, Dalian University of Technology, Dalian, China, in 2017. He is currently pursuing the Doctoral degree in computer science and technology with the School of Computer Science and Technology, College of Intelligence and Computing, Tianjin University, Tianjin, China. He is a member of Tianjin Advanced Networking Key Laboratory and his researches focus on the Industrial Internet of Things, the industrial big data, and the industrial edge computing based on artificial intelligence.

Xiaobo Zhou (Senior Member, IEEE) received the B.Sc. degree in electronic information science and technology from the University of Science and Technology of China, Hefei, China, in 2007, the M.E. degree in computer application technology from the Graduate University of Chinese Academy of Science, Beijing, China, in 2010, and the Ph.D. degree in information science from the School of Information Science, Japan Advanced Institute of Science and Technology, Ishikawa, Japan, in 2013. From April 2014 to March 2015, he was a Researcher with the Department of Communications Engineering, University of Oulu, Oulu, Finland. He is currently an Associate Professor with the School of Computer Science and Technology, College of Intelligence and Computing, Tianjin University, Tianjin, China. His research interests include cooperative wireless communications, wireless networks, data center networks, vehicular networks, and mobile-edge computing.

Zhaolong Ning (Senior Member, IEEE) received the M.S. and Ph.D. degrees from Northeastern University, China. He was a Research Fellow with Kyushu University, Japan. He is an Associate Professor with the School of Software, Dalian University of Technology, China. He has published over 120 scientific papers in international journals and conferences. His research interests include mobile-edge computing, Internet of Things, and machine learning. His five papers are ESI 0.1% hot papers, 25 papers are ESI highly cited papers, one journal paper wins the Best Paper Award of IEEE Systems Journal in 2018, one journal paper wins the Top 100 most Influential International Academic Papers China in 2018, one journal paper is the Top Downloaded Paper of IJCS 2018, and three conference papers win the Best Paper Award. He is elected to be the Young Elite Scientists Sponsorship Program by CAST and Hong Kong Scholar. He serves as an Associate Editor or a Guest Editor of several journals, such as the IEEE Transactions on Industrial Informatics, *The Computer Journal*, IEEE Access, *Wireless Communications and Mobile Computing*, and the *International Journal of Communication Systems*. He is the outstanding Associate Editor of IEEE Access 2018.

Mohammed Atiquzzaman (Senior Member, IEEE) received the M.S. and Ph.D. degrees in electrical engineering and electronics from the University of Manchester, U.K. He currently holds the Edith Kinney Gaylord Presidential professorship with the School of Computer Science, University of Oklahoma. His research has been funded by the National Science Foundation, National Aeronautics and Space Administration (NASA), U.S. Air Force, Cisco, Honeywell, Oklahoma Department of Transportation, and Oklahoma Highway Safety Office through numerous grants. He has coauthored the book *Performance of TCP/IP Over ATM networks* and has over 270 refereed publications, which are accessible at www.cs.ou.edu/∼atiq. His research interests are in communications switching, transport protocols, wireless and mobile networks, ad hoc networks, satellite networks, quality of service, and optical communications. In recognition of his contribution to NASA research, he received the NASA Group Achievement Award for "Outstanding Work to Further NASA Glenn Research Center's effort in the area of Advanced Communications/Air Traffic Management's Fiber Optic Signal Distribution for Aeronautical Communications" Project. He received from IEEE the 2018 Satellite and Space Communications Technical Recognition Award for valuable contributions to the Satellite and Space Communications Scientific Community. He also received the 2017 Distinguished Technical Achievement Award from the IEEE Communications Society in recognition of outstanding technical contributions and services in the area of communications switching and routing. He serves on the review panels of funding agencies, such as the National Science Foundation and National Research Council, Canada, and Australian Research Council, Australia. He is the Editor-in-Chief of *Journal of Networks and Computer Applications*, a Founding Editor-in-Chief of *Vehicular Communications* and has served/serving on the editorial boards of *IEEE Communications Magazine*, the IEEE Transactions on Mobile Computing, the IEEE Journal on Selected Areas in Communications, the *International Journal on Wireless and Optical Communications*, *Real Time Imaging Journal*, the *Journal of Communication Systems*, the *Journal of Communication Networks and Distributed Systems*, and the *Journal of Sensor Networks*. He also guest edited many special issues in various journals.

Dapeng Oliver Wu (Fellow, IEEE) received the B.E. degree in electrical engineering from the Huazhong University of Science and Technology, Wuhan, China, in 1990, the M.E. degree in electrical engineering from the Beijing University of Posts and Telecommunications, Beijing, China, in 1997, and the Ph.D. degree in electrical and computer engineering from Carnegie Mellon University, Pittsburgh, PA, USA, in 2003. He is a Professor with the Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL, USA. His research interests are in the areas of networking, communications, signal processing, computer vision, machine learning, smart grid, and information and network security. He received the University of Florida Term Professorship Award in 2017, the University of Florida Research Foundation Professorship Award in 2009, the AFOSR Young Investigator Program (YIP) Award in 2009, the ONR YIP Award in 2008, the NSF CAREER Award in 2007, the IEEE Circuits and Systems for Video Technology Transactions Best Paper Award for Year 2001, and the Best Paper Awards in IEEE GLOBECOM 2011 and International Conference on Quality of Service in Heterogeneous Wired/Wireless Networks in 2006. He has served as the Chair for the Award Committee, and the Chair of Mobile and Wireless Multimedia Interest Group, Technical Committee on Multimedia Communications, and IEEE Communications Society. He was an Elected Member of Multimedia Signal Processing Technical Committee, IEEE Signal Processing Society from January 2009 to December 2012. He has served as a Technical Program Committee (TPC) Chair for IEEE INFOCOM 2012, and a TPC Chair for IEEE International Conference on Communications in 2008, Signal Processing for Communications Symposium, and as a member of executive committee and/or technical program committee of over 80 conferences. He was elected as a Distinguished Lecturer by IEEE Vehicular Technology Society in 2016. He currently serves as an Editor-in-Chief for the IEEE Transactions on Network Science and Engineering, and an Associate Editor for the IEEE Transactions on Communications, the IEEE Transactions on Signal and Information Processing Over Networks, and *IEEE Signal Processing Magazine*. He was the founding Editor-in-Chief of the *Journal of Advances in Multimedia* from 2006 and 2008, and an Associate Editor for the IEEE Transactions on Circuits and Systems for Video Technology, the IEEE Transactions on Wireless Communications, and the IEEE Transactions on Vehicular Technology. He is also a Guest-Editor for the IEEE Journal on Selected Areas in Communications, Special Issue on Cross-layer Optimized Wireless Multimedia Communications.