Published in final edited form as:

IEEE Access. 2018 ; 6: . doi:10.1109/access.2018.2884906.

A Survey on Industrial Internet of Things: A Cyber-Physical Systems Perspective

Hansong Xu[*], **Wei Yu**[*], **David Griffith**[†], **Nada Golmie**[†]

[*]Towson University, MD, USA.

[†]National Institute of Standards and Technology.

Abstract

The vision of Industry 4.0, otherwise known as the fourth industrial revolution, is the integration of massively deployed smart computing and network technologies in industrial production and manufacturing settings for the purposes of automation, reliability, and control, implicating the development of an Industrial Internet of Things (I-IoT). Specifically, I-IoT is devoted to adopting the Internet of Things (IoT) to enable the interconnection of anything, anywhere, and at anytime in the manufacturing system context to improve the productivity, efficiency, safety and intelligence. As an emerging technology, I-IoT has distinct properties and requirements that distinguish it from consumer IoT, including the unique types of smart devices incorporated, network technologies and quality of service requirements, and strict needs of command and control. To more clearly understand the complexities of I-IoT and its distinct needs, and to present a unified assessment of the technology from a systems perspective, in this paper we comprehensively survey the body of existing research on I-IoT. Particularly, we first present the I-IoT architecture, I-IoT applications (i.e., factory automation (FA) and process automation (PA)) and their characteristics. We then consider existing research efforts from the three key systems aspects of control, networking and computing. Regarding control, we first categorize industrial control systems and then present recent and relevant research efforts. Next, considering networking, we propose a three-dimensional framework to explore the existing research space, and investigate the adoption of some representative networking technologies, including 5G, machine-to-machine (M2M) communication, and software defined networking (SDN). Similarly, concerning computing, we again propose a second three-dimensional framework that explores the problem space of computing in I-IoT, and investigate the cloud, edge, and hybrid cloud and edge computing platforms. Finally, we outline particular challenges and future research needs in control, networking, and computing systems, as well as for the adoption of machine learning, in an I-IoT context.

Keywords

Industrial Internet of Things; Industrial Cyber Physical Systems; Application and Service; Control; Networking; Computing; Machine Learning; Big Data Analytics; Survey; Future Research Directions

hxu2@students.towson.edu, wyu@towson.edu.

I. INTRODUCTION

In smart manufacturing systems [1], along with other typical cyber-physical systems (CPS) like the smart grid [2], [3], modern information communication technologies (computation, control, communication, etc.) can be leveraged to improve the monitoring and control abilities of physical systems (manufacturing equipment and workflow, electrical grid transmission and generation, etc.). To realize the vision of the next generation industrial revolution (known as Industry 4.0), smart manufacturing is a necessity, as massive numbers of smart sensors and actuators (otherwise known as machine devices) will be interconnected and integrated into industrial systems using the advanced technologies developed for the Internet of Things (IoT) and CPS [4]. Moreover, these technologies are becoming increasingly mature, reliable, and widely adopted, with the number of machine devices deployed worldwide projected to grow to 75.4 billion by 2025 according to a recent market research study [5]. In the context of Industry 4.0, the requirements of response time, network latency, and reliability are especially critical, as the entire workflow of the manufacturing process will be carried out automatically, without human intervention where possible. Thus, the data transmission and decision-making technologies shall be optimized to be as timely and accurate as possible.

In the recent past, IoT has become a highly active research area, as it enables the interconnection of anything, anytime and anywhere [2], [6], [7]. IoT has been applied to interconnect unprecedented quantities of devices for consumer applications (home appliances, transportation, mobile devices, etc.). Those consumer applications (e.g., smart home, smart city, smart grid, and smart transportation) can provide convenience, efficiency and intelligence to consumers to better manage their personal time and resources [8], [9], [10], [11], [12], [13], [14]. Extending the technology, Industry 4.0 envisions the adoption of IoT for use in manufacturing, and has great potential to improve the productivity, efficiency, safety and intelligence of industrial factories and plants [15], [16]. Thus, Industrial-IoT (I-IoT) indicates the nature of the application of IoT to be industrial manufacturing, facilitating the interconnection of “anything” (sensors, actuators, controllers, production lines, equipment, etc.) in an industrial production and automation context.

An I-IoT system, as a typical CPS, is composed of two key components: the cyber systems and the physical systems. The cyber systems include control, networking and computing infrastructures that enable the operation, interconnection, and intelligence of the industrial systems. The physical systems are the manufacturing and automation systems that leverage industrial devices to undertake designated production and automation tasks. There have been some recent research efforts towards investigating I-IoT (understanding the I-IoT system in general, investigating specific issues in I-IoT, leveraging state-of-the-art techniques for I-IoT, etc.). For instance, Su *et al.* [17] surveyed the challenges and research issues on data management in I-IoT and conducted a case study using a large-scale petrochemical plant. In addition, in investigating a specific I-IoT problem, Sun *et al.* [18] applied auction-based mechanisms to address the computing resource allocation problem, while Jeong *et al.* [1] addressed the trust issues in resource allocation. Moreover, some research efforts have leveraged advanced communication techniques, such as 5G and software-defined networking (SDN) for I-IoT [19], [20].

In this paper, we provide a comprehensive survey of I-IoT from a CPS perspective, focusing primarily on control, networking, and computing. In I-IoT, control systems play the critical role of operating massive number of industrial devices (sensors, actuators, equipment, etc.). Networking systems enable timely communication of data and control signals for diverse and dispersed tasks in industrial systems [21]. Computing systems provide the computational platform to enable timely collection, storage, processing, and analysis of data in an efficient, highly-reliable, and scalable manner [22], [23]. Notice that the adoption of machine learning can be incorporated into all systems in I-IoT. Finally, the physical components are the manufacturing and automation systems.

The primary contributions of this paper are three-fold:

- **I-IoT System Architecture, Physical Systems, and Requirements.** We present the I-IoT architecture, which consists of three layers (i.e., application layer, communication layer, and physical layer). We introduce some typical I-IoT physical systems (e.g., PA and FA) and their characteristics (e.g., number of nodes, cycle time, and reliability). We also identify I-IoT performance requirements from the communications perspective (e.g., latency and reliability).
- **Control, Networking and Computing Systems.** We conduct a survey of I-IoT from the three critical perspectives of control systems, networking systems, and computing systems. Concerning control systems, we investigate existing research efforts on industrial control systems, which play critical roles in the control and operation of industrial factories and plants. Those systems are categorized into centralized, decentralized, and hierarchical control systems. Regarding networking systems, we propose a three-dimensional framework to explore existing research efforts. We review some representative emerging networking technologies, including 5G, machine-to-machine (M2M) communication, and SDN for I-IoT. We also review some progress in the standardization of I-IoT. Considering computing systems, we propose a three-dimensional framework to investigate existing research efforts on computing in I-IoT. We review the state-of-the-art computing platforms for I-IoT, including cloud computing and hybrid cloud and edge-based computing. We also investigate the big data analysis supported by I-IoT computing systems.
- **Challenges and Future Directions** We present the challenges and future research needs of control, networking and computing systems in I-IoT, as well as in machine learning for I-IoT. Particularly, we present the challenges in control system of enabling self-awareness, self-diagnosis and self-healing, efficient management, effective resource utilization, and timely maintenance. In addition, concerning networking systems, we discuss the problems of conducting network deployment, resource scheduling, and security. Moreover, regarding computing systems, we outline the challenges of the deployment of computing system, seamless integration, and computing resource management. In terms of future directions for control, networking, and computing systems, we outline several critical research needs such as co-design, intelligent data management and analysis, and develop a theoretical foundation, models and

testbeds to allow design and analysis of these new types of systems. We further review recent progress on machine learning and illustrate an example of leveraging machine learning for networking in I-IoT. Finally, we outline research directions in machine learning for I-IoT, including machine learning for latency-guaranteed and ultra-reliable communications, machine learning-enabled cloud and edge computing, intelligent sensing and decision making, online learning and relearning, distributed machine learning, and light-weight learning platforms.

The remainder of this paper is organized as follows: In Section II, we present the architecture of I-IoT, along with its industrial applications and characteristics. In Section III, we review control systems in I-IoT from the perspectives of centralized, distributed and hierarchical control. In Section IV, we review research efforts on networking systems in I-IoT and consider some representative techniques, such as 5G, M2M, and SDN. In Section V, we review the research efforts on computing systems in I-IoT, such as cloud computing, edge computing, and hybrid cloud and edge computing, among others. In Section VI, we present challenges, possible solutions and future directions in the areas of control, networking, and computing systems in I-IoT, as well as the use of machine learning in I-IoT. In Section VII, we conclude the paper. Notice that all main acronyms used in the paper and their descriptions are listed in Table I.

II. ARCHITECTURE OF I-IOT, APPLICATIONS AND CHARACTERISTICS

Industry 4.0 represents the fourth industrial revolution looming on the horizon, in which information communication technologies are applied to industrial manufacturing and automation so that the productivity and efficiency can be improved. From Industry 4.0, there emerges two key paradigms: I-IoT and Industrial Cyber-Physical System (I-CPS). Generally speaking, I-IoT enables sensing and interconnection of industrial devices and equipment by applying emerging IoT technologies in industrial manufacturing and automation systems. Similarly, I-CPS is an extension of traditional CPS that was initially intended for critical systems (power generation, transportation, infrastructure, etc.), but has since been applied more broadly, defined by the intertwining of cyber and physical systems for command and control, security, resiliency and automation. I-CPS can be considered the merger of industrial cyber and physical systems that provide productive and efficient manufacturing and automation [2], [24], [25], [26], [27]. In the following, we present the architecture of I-IoT, and its applications and characteristics in more detail.

A. Architecture

We first consider the differences and relationships between IoT, I-IoT and I-CPS. Generally speaking, IoT is the interconnection of massively deployed and dispersed physical devices that can be used to monitor and control physical objects in CPS, such as a smart grid or smart transportation system, leading to a smart and connected world where vast numbers of everyday devices are interconnected [2], [28]. Distinct from IoT, which is directed toward consumer-based systems, I-IoT involves the interconnection of intelligent industrial devices with control and management platforms, which collectively improve the operational efficiency and productivity of industrial systems. Due to the autonomous nature of industrial

devices and processes, I-IoT is considered as an important application of IoT. Similarly, unlike CPS for critical infrastructures or consumer applications, I-CPS is designed to support the manufacturing and industrial production applications.

In I-IoT, the wide variety of industrial devices in an I-CPS, such as machines, assembly line monitors, and control devices, are interconnected and form a smart factory or plant. Moreover, the I-CPS is a vertical industrial system that consists of both cyber systems and physical systems. In this regard, the I-IoT is the integration of communication layers of I-CPS, which allow the interconnection of physical industrial objects so that a feasible manufacturing process can be enabled.

Additionally, I-IoT can be described as a three layer architecture, as shown in Figure 1. From the viewpoint of industrial systems, the three tiered architecture consists of the application layer, communication layer, and physical layer. The application layer consists of the various industrial applications, including smart factories, smart plants, smart supply chains, and others. Those smart industrial applications leverage numerous sensors and actuators for the purpose of timely monitoring, accurate control, and efficient management. The communication layer is the integration of numerous communication networks, such as wireless sensor and actuator networks (WSANs), 5G, M2M, SDN, and so on. A variety of network techniques will be necessarily to support the interconnection of a considerable volume of sensors and actuators in smart industrial applications. Finally, the physical layer is composed of these widely deployed physical devices, such as sensors, actuators, manufacturing equipment, facility utilities, and other industrial manufacturing and automation-related objects.

Figure 2 illustrates I-IoT from a CPS viewpoint. In the physical system (left), the various industrial applications, such as PA and FA, follow a production lifecycle (i.e., the cycle of prepare, produce, transport, utilize and recycle). During each step in the production lifecycle, a significant amount of data will be generated from different devices and equipment. Control, networking, and computing systems play important roles in the interconnection and integration of components and physical systems, and perform monitoring and control, leading to efficient operation of physical systems.

B. I-IoT Applications and Characteristics

The involvement of industrial applications in IoT makes I-IoT an entirely different world, in meaning and concept, and calls for a deep understanding of term “industrial”. Thus, we first outline some typical industrial applications and illustrate their characteristics. Industrial applications cover numerous critical production, manufacturing, and transportation systems, including power generation plants, power distribution networks, production facilities and factories, and so on.

First, PA is characterized by an industrial process, such as in chemical, oil, and power plants, which are autonomous, i.e., they are controlled and managed with little or no human intervention. A PA system often integrates sensors, controllers, and actuators for information collection, interaction and process actuation. Second, FA leverages robotic systems and assembly line machinery to enable automation of the manufacturing process

for the improvement of productivity and efficiency. For example, the robotic arms typically have similar appearance and actuation to their human counterparts, and are able to perform the functions as a human operator, but with greater robustness, productivity, precision and efficiency. With the same objectives, assembly lines often decompose complex tasks into smaller subtasks and perform step-by-step operations according the designed workflow [29], [30], [31].

An example of PA is power system automation (PSA), which aims to conduct automatic control, monitoring, and protection of power generation, distribution, and usage systems by various instruments and control devices. PSA contains three key components: data acquisition, remote monitoring, and control. The data acquisition is used to collect data from various sensing and control devices, which can be processed either locally or in a data center. Remote monitoring, which is used to monitor the status of the power systems, alerts the operation center to abnormal situations and prevents blackouts. Finally, PSA control plays the role of operating power systems, controlling substations from the operation center.

There are several key characteristics associated with industrial applications. The first characteristic is the cycle time, which means the time required to receive commands from the control center and send sensor data to the control center. The cycle time can depend on the I-CPS application. For example, the cycle time for PA is on the order of hundreds of milliseconds. The second characteristic is the number of nodes, which indicates the size of the system (i.e., the number of nodes covered by one controller in a working area). The third characteristic, reliability, is characterized as the quality of information transmission, and can be measured using the packet error rate (PER). For instance, a PER of 10^{-9} is considered acceptable [31], [32]. In addition, industrial applications are primarily concerned with accurate and timely operation and cooperation among numerous sensors and actuators. Hence, the performance requirements are significantly different from those for consumer-oriented IoT applications.

Table II illustrates the requirements of two types of industrial applications based on their characteristics. Some examples of performance requirements include latency and reliability from the perspective of communication. Latency, as a critical indicator, measures the performance of the data delivery based on the delay requirement. The cycle time indicates the time required for a process cycle, which varies by the particular industrial scenario. To guarantee the timely and accurate operations of I-IoT systems, the network shall have the capability to provide communications so that critical information can be delivered within the cycle time. Finally, reliability is used to qualify the importance of delivering critical information accurately. Highly reliable transmission requirement indicates that information (e.g., control messages) shall be transmitted with extremely low error rate.

III. CONTROL SYSTEMS IN I-IOT

The control systems in I-IoT environments play a crucial role in controlling and operating the critical infrastructures for factory manufacturing, power generation plants, oil and gas distribution systems, and so on. Generally speaking, the control systems can be categorized into three types: centralized control, decentralized control, and hierarchical control, based

on the overall system structure, as shown in Figures 3, 4 and 5 [33], [34]. Additionally, the network provides communication infrastructure for the data exchange between subsystems.

A. Centralized Control

Figure 3 illustrates the structure of a centralized control system, which uses a centralized controller to monitor and control a number of subsystems. Each subsystem consists of sets of sensors and actuators, denoted as S and A, respectively. The sensors capture the operation status and condition and report the information to the centralized controller. The centralized controller sends control and command signals to the actuators in each entity in response to command and control decisions. The collection of sensing, analysis, and command transmission for all entities are carried out in the centralized controller. Supervisory Control And Data Acquisition (SCADA) is an example of a centralized control system.

SCADA has been widely used to monitor and control large-scale interconnected systems, such as those for water distribution, in oil, gas and electricity industries, etc. [35]. A typical SCADA system, as shown in Figure 6, consists of human machine interface (HMI), SCADA servers, remote terminal units (RTUs), sensors and actuators, and others [36]. In more detail, the HMI enables operators to direct command to the dispersed RTUs. The RTUs are often deployed in distributed sites to perform localized processing for monitoring and control. SCADA servers conduct information collection, analysis and command dissemination. The features of SCADA (i.e., data acquisition and supervisory control) enable the centralized monitoring and control on the dispersed assets in distributed locations.

Recall that the emerging IoT integrates various state-of-theart network technologies to provide ubiquitous connections for an enormous quantity of devices in a variety of application domains. A number of representative network technologies in IoT, such as 5G, WiFi, M2M communication, and SDN, among others, can be integrated into the SCADA system to provide ubiquitous connections for large numbers of industrial devices. In this case, the integration of IoT and SCADA can improve the interoperability of industrial applications along with optimized resource allocation [37]. For example, Lu *et al.* [38] presented the integration of IoT with the centralized control system to monitor the critical infrastructure of industrial applications, where they illustrated the design of I-IoT from an engineering perspective (e.g., power supply, connectivity options, hardware, software and data acquisition methodologies). In addition, Alhebshi *et al.* [39] leveraged IoT to monitor and respond to the failures of transmission lines in the smart grid.

Nonetheless, the integration of IoT and traditional SCADA expose industrial control systems to additional vulnerabilities. Particular to this issue, Sajid *et al.* [36] investigated the potential exposure of the critical industrial system to security issues in the IoT-cloud environment. Possible solutions to address these security vulnerabilities were also studied from two aspects. The first is the SCADA system security (e.g., policy management, data integrity, and weak communication), and the second is the SCADA system in the IoT-cloud environment (data integrity and privacy, data logging, and authentication encryption, etc.). In addition, Shahzad *et al.* [40] leveraged the advanced encryption standard (AES) algorithm to encrypt communication and prevent authentication and confidentiality attacks on IoT-SCADA systems.

B. Decentralized Control

As shown in Figure 4, the significant difference of decentralized control systems from centralized control systems is the distributed individual controllers. Individual controllers are often deployed in individual subsystems and perform control to the designated subsystems.

1) Distributed Control: The distributed control system (DCS) is one example of the general category of decentralized control systems. DCS is often designed to control the industrial process or production in one location, and can include electricity generation plants, oil refineries, and factory manufacturing, among others. For production and process control, the DCS can oversee multiple subsystems with supervisory level control, and controls the processes in subsystems [35]. Specifically, in DCS, controllers are deployed to provide specific production and process. Various controllers work together to carry out production or processes collaboratively. Such collaboration is enabled by a supervisory control loop to connect various localized controllers.

DCS operates a plant or a factory by various functional groups (FGs) that work together to accomplish the designated control missions. The different FGs perform segregated tasks and functions to improve productivity and efficiency. For example, as shown in a recent work by El-Shafei *et al.* [41], the liquid level process control plays an important role in PA systems. The authors implemented a DCS-controlled process station in a simulation environment for the study of liquid level process control. In their study, the control performance of DCS was compared with different proportional-integral-derivative (PID) controllers.

In addition, the programmable logic controller (PLC) is a system that plays the crucial role of providing regulatory control for specific applications. Particularly, PLC interprets signals from sensors and generates and transmits control signals to actuators corresponding to the targeted set points. As a standalone system, PLC is usually configured especially for specific tasks.

2) Integration with Radio Technologies: The DCS is often used in production systems for manufacturing control or automation control. At the field level, control systems (machine controller, PLC, process controller, etc.) use feedback or feedforward control loops to control the process or production at certain set points. In a complex manufacturing environment, radio technologies can be helpful to improve the flexibility and agility of the DCS. For example, Barenji *et al.* [42] proposed the design and implementation of DCS for manufacturing with the use of radio-frequency identification (RFID). In particular, the proposed multi-agent architecture captures the actions and interactions of various agents at station and shop sides of the system, including management agent, shop monitoring and command agent, station control agent and resource agent, and others. Different monitoring and control agents leverage the RFID technology to improve the accuracy and timeliness of data acquisition. With the RFID-enabled DCS, the performance of monitoring and control can be improved, as well as the flexibility and the agility of industrial systems.

C. Hierarchical Control

As seen in Figure 5, hierarchical control utilizes a multilayer control structure to deal with complex and large industrial systems. The lower level consists of local controllers, which directly interact with the subsystems and perform control tasks. The sensed results and control results will flow up to higher level for supervisory monitoring or efficient coordination for large-scale systems [34].

Different control systems (e.g., SCADA, DCS) serve distinct manufacturing or production systems with different control requirements. The integration of different control systems can be effective, productive and controllable for dealing with large-scale and complex manufacturing. Taking the power generation system as an example, electricity is generated from many types of power plants, in which the operation facilities can be controlled by DCS. In addition, SCADA can be used to monitor various power plants, and provide a high-level coordination and management of the plants. The integration of DCS and SCADA can improve the efficiency of electricity generation, transmission and distribution by leveraging the benefits of both.

1) Integration of SCADA and DCS: The complexity and scale of industrial systems calls for the seamless integration of SCADA and DCS to carry out high-performance monitoring and efficient control. To this end, Karnouskos *et al.* [43] introduced a vision and directions for designing the architecture of next-generation SCADA/DCS with considerations for information technology trends. This work pointed out that the monitoring, management and visualization, scalability, security and other aspects shall be investigated in the future complex and collaborative SCADA/DCS ecosystem. In addition, Lü *et al.* [44] proposed a heterogeneous large-scale SCADA/DCS architecture to operate, monitor and control large-scale systems (e.g., power plants, gas and air systems).

SCADA systems are also used in food production and can be extended with DCS. For instance, Selisteanu *et al.* [45] proposed a DCS/SCADA architecture to control the process of bread production (e.g., wheat grinding and bread production). The hierarchical architecture consists of five levels, including field level, data acquisition level, process supervision level, coordination level, and production control level.

2) Other Integrations: PLCs are often used as control components in SCADA and DCS systems to provide process control. In this case, similar to RTUs, the PLC plays the role of interconnection between control center and end-devices (e.g., sensors and actuators). As an example of integrating SCADA and PLC, Singh *et al.* [46] leveraged SCADA and PLC to conduct monitoring and control of DC motor speed. The PLC mainly generates control signals to adjust motor speed and the SCADA provides remote monitoring. In addition, Endi *et al.* [47] proposed a three-layer PLC/SCADA architecture, which consists of supervisory control layer, process control layer, and field instrumentation control layer. The three-layer architecture leverages open system technology (e.g., open standards protocol) to enable seamless communication between different layers, such that the scalability, compatibility and performance of remote control and monitoring can be improved.

IV. NETWORKING SYSTEMS IN I-IOT

With the support of communication networks, machine devices can collect and exchange data amongst themselves to support numerous smart-world systems such as smart manufacturing, smart grid, and many others [3], [48], [49]. The communication associated with those machine devices is denoted as M2M communication, otherwise referred to as machine-type communication, supporting ubiquitous connectivity among machine devices without human intervention [50], [51], [52], [53]. Along with the research and development of the 3rd Generation Partnership Project (3GPP) on Long-Term Evolution (LTE) and Long-Term Evolution Advanced (LTE-A) [54], and the fifth generation wireless network (5G), M2M has been identified as a key technology for the future of communication.

Recalling the I-IoT applications and characteristics in Section II-B, I-IoT is expected to interconnect a plethora of industrial devices and equipment from numerous previously isolated industrial systems. Such interconnections can improve the operability, productivity and resource efficiency of industrial applications. From the networking perspective, such an interconnection requires the design of high-capacity communication networks, which are capable of supporting industrial devices with strict quality of service (QoS) requirements. Moreover, the network shall improve its flexibility, scalability and interoperability to support connections in numerous isolated industrial systems so that flexible manufacturing can be supported [55].

We now investigate some of the representative network technologies mentioned, in the context of I-IoT. Specifically, we first introduce a three-dimensional framework, shown in Figure 7, from which to investigate the existing research works related to networking systems in I-IoT. The framework consists of three orthogonal dimensions (i.e., physical systems, information types, and networking requirements). Based on the defined framework, we consider the existing research efforts on the state-of-the-art networking technologies (i.e., 5G, M2M, and SDN) for networking systems in I-IoT. In addition, we review the recent progress toward standardization for I-IoT from the perspective of networking.

A. Problem Space of Networking in I-IoT

Figure 7 presents a framework to explore the problem space of networking systems in I-IoT. From the dimension of physical systems, we consider two types of system (i.e., PA, FA). In the information type dimension, we consider the different categories of information transmitted through the network, including control information, monitoring information, and others, which includes data sharing between subsystems. In the third dimension, we present the network performance requirements, including latency, reliability, and others (security, privacy, etc.), for the designated network system in I-IoT. For example, research efforts on leveraging 5G to improve the latency performance of real time monitoring of the production quality in manufacturing factories can be mapped into cube <Monitoring, Factory Automation, Latency> of Figure 7. In the following, we use this three-dimensional framework to investigate and map the research efforts on the networking technologies to be integrated in I-IoT (i.e., 5G, M2M, and SDN).

B. Next Generation Wireless Networks for I-IoT

5G, as the next generation wireless network, leverages various techniques (ultra-dense network (UDN), massive multiple-input and multiple-output (MIMO) and mmWave, etc.) to engender a 1,000-fold improvement in network capacity, a 100-fold increase in user data rate, and a 10-fold improvement in end-to-end delay [56], [57], [58]. It is worth noting that 5G is designed to satisfy the requirements of a variety of diverse applications that may require high network capacity, high throughput, low latency, and many others. Recall that typical requirements of I-IoT from the communication network perspective include low latency (milliseconds level) and high reliability for short packets (less than 10^2 Bits) [24]. Here, 5G has the potential to assist I-IoT applications, as it is able to provide the desired high network capacity and throughput, and low latency. Thus, it is necessary to investigate the existing research efforts that adapt and integrate the 5G techniques in I-IoT.

UDN, which leverages the dense deployment of small-cell Base Stations (BSs) to improve network capacity, is one of the key enablers of 5G [56]. UDN aims to connect a massive number of mobile devices, which can potentially fit the industrial application scenarios (i.e., the massively deployed sensors and actuators of I-IoT). Relevant to this aspect, Ding *et al.* [59] investigated the network performance of uplinks in UDN for IoT and pointed out several caveats (excessive inter-cell interference, among others).

Massive MIMO systems are equipped with an immense number of transmitter antennas at base stations, which could even exceed the number of receiver antennas of the massive number of served devices. In addition, mmWave, another important technique in 5G, offers much higher bandwidth to improve the communication performance for high throughput I-IoT applications (e.g., surveying and inspection). Nonetheless, in I-IoT scenarios, blockage is a critical issue that affects data transmission links. Thus, towards resolving this issue, Orsino *et al.* [60] investigated the possibilities of deviceto-device (D2D) communication in industrial environments. Specifically, they leveraged D2D on mmWave links to improve reliability and reduce latency. This work can be mapped to <Monitoring, FA, Latency> in Figure. 7.

Given the huge performance gain supported by massive MIMO (diversity gain, array gain, etc.), it can clearly provide connectivity to I-IoT devices. For example, Lee *et al.* [61] illustrated the feasibility of using massive MIMO in I-IoT scenarios and further defined several research problems and challenges. Moreover, their analysis and simulation results showed the capability of massive MIMO to support a large number of connections from I-IoT devices with moderate data rate at low cost. Nonetheless, a number of issues (device scheduling, power control, etc.) may be raised when the massive MIMO is used in I-IoT.

In summary, 5G has the potential to satisfy the communication requirements for numerous industrial applications. Taking the power grid as an example, Bag *et al.* [62] adopted 5G to improve the performance of protection, control, monitoring, and diagnostics. In their study, 5G was leveraged to provide high-speed communications between relays of distribution lines, which support fault current detection in a cost-efficient manner. This work can be mapped to the cube in <Controlling/Monitoring, PA, Latency/Reliability> in Figure. 7.

C. M2M for I-IoT

Communication in I-IoT is different from the communications for consumers, even in the case of consumer IoT. Specifically, I-IoT devices usually collect and transmit data via uplinks (UL) [59], a type of communication identified as machine-type communications. Indeed, there are some existing research efforts toward the study of M2M communication in I-IoT applications [53], [63], [64]. For instance, the co-design of both control system and network transmission is one effective approach to leverage M2M for I-IoT. In this direction, Lyu *et al.* [63] proposed the co-design of state estimation and wireless transmission in 5G machine-type communication enabled I-IoT systems to improve the accuracy of estimating state parameters over resource constrained wireless networks. Their approach consists of hierarchical state estimation and two-stage transmission that can adapt to system dynamics. By using the three-dimensional framework in Figure 7, this work can be mapped to cube <Monitoring, PA, Reliability>.

In addition, Navarro-Ortiz *et al.* [65] proposed the integration of the standardized low-power wide area networks (LoRaWAN) and 4G/5G. This integration leverages the benefits of LoRaWAN and the network infrastructure provided by 4G/5G to satisfy the requirements of massive machine-type communications (e.g., low power, long range, and low bandwidth). Compared to the LTE-WLAN integration, the integration of LoRaWAN and 4G/5G can satisfy the requirements of M2M for I-IoT. In addition, the LoRaWAN and 4G/5G integration requires minimal changes to the existing mobile networks, needing only the modification of the LoRaWAN gateway (i.e., modifying gateways to eNodeBs to the 4G/5G EPC and implementing the eNodeB protocol stack). This was tested as a proof-of-concept in an experimental testbed with promising results.

D. SDN for I-IoT

Existing network infrastructures are often statically deployed and application-specific, unable to support increasing numbers and types of industrial applications with diversified requirements. In addition, it is not cost-effective and efficient to deploy dedicated network infrastructures for massive industrial applications. This calls for a cost-effective and efficient network infrastructure that can enable dynamic configuration and interoperability for different industrial applications [66]. SDN, as a networking technique, can play a critical role in enabling the scalability and programmability of networks while coping with increasingly diverse and complex networking functions [67]. The key concept of SDN is to separate the control plane (algorithms, protocols, etc.) and the data plane (packet routing, forwarding, etc.). In this way, the implementation and configuration of network controls for individual applications can be deployed, modified, and updated.

Several efforts have been made to adopt SDN for I-IoT. For example, Henneke *et al.* [68] reviewed the applicability of SDN in networks for industrial systems and pointed out that the interoperability enabled by SDN could improve the network performance to satisfy the I-IoT requirements in heterogeneous and complex industrial systems. In particular, they identified the network challenges for industrial systems from the network perspectives (e.g., heterogeneity, QoS, reliability, and security, among others).

In addition, toward implementing SDN in I-IoT, Baddeley *et al.* [69] evaluated the performance of light-weight SDN with the layer-2 slicing mechanism defined in the IEEE 802.15.4 networks for I-IoT scenarios. In this case, SDN control slices are created for the controlling traffic, which prevents interference with network traffic. In addition, the recently standardized IEEE 802.15.4 – 2015 Time Scheduled Channel Hopping (TSCH) improved reliability and latency of communication paths in the lossy industrial environment [70].

Furthermore, leveraging SDN has been demonstrated to improve network performance with different delay requirements in heterogeneous I-IoT settings. For example, Li *et al.* [71] proposed an adaptive transmission architecture and algorithms, which adapts to different traffic flows. Particularly, an adaptive routing scheme was proposed to compute optimal routes for non-urgent and urgent data streams. This work can be mapped to <Control, PA/FA, Reliability> in Figure 7.

As a typical application in the utility industry, the smart gird will integrate a variety of energy resources, including traditional energy, renewable energy, electrical vehicles, and others [3]. The complex energy generation integration requires frequent information exchange, which poses a challenge to the traditional communication infrastructure. In response, Al-Rubaye *et al.* [72] utilized the SDN platform to improve the resiliency of power grid communications for enabling real-time monitoring and controlling capabilities. The proposed SDN platform includes an infrastructure layer, control layer, and application layer. The SDN controller plays a critical role in carrying out optimization and control. For instance, the SDN controller can reschedule traffic flows when failures occur. This work maps to <Control, PA/FA, Reliability> in Figure. 7.

SDN can be further integrated with network virtualization (NV) to provide service to I-IoT [73], [74]. For instance, Bizanis *et al.* [73] surveyed techniques in radio access networks (RANs) and core networks (CNs). The technique in RAN first uses network function virtualization (NFV) to effectively manage network resources in 5G [75]. Then, the concept of SDN is leveraged to create virtual network “slices” over the same physical network. The virtual network “slices” support different wireless technologies and standards to improve interoperability in heterogeneous networks. Towards the integration of SDN and NV for I-IoT, Ma *et al.* [74] proposed an SDN and NV integrated network architecture for the industrial environment. Their integrated architecture consists of software-defined infrastructure (SDI), virtualized network, control plane management, and network function virtualization in four different layers. The architecture was shown to improve the efficiency of network resource utilization, reduce the complexity of network design, and satisfy the requirements of various production processes. In addition, as a use case in the embryonic stage of I-IoT, Luo *et al.* [76] used SDN and NFV to improve the energy efficiency of industrial wireless sensor networks. In particular, the SDN controller was introduced to control and optimize the topology of sensor networks. The NFV was leveraged to enable functional replaceability of industrial devices.

E. Standardization Progress

Standardization can, in general, help progress the understanding, development, and resiliency of I-IoT. A number of standardization bodies across industry and academia, along

with various federations, including the Industrial Internet Consortium (IIC), The Institute of Electrical and Electronics Engineers (IEEE), and National Institute of Standards and Technology (NIST), have undertaken standardization efforts for I-IoT from a variety of perspectives. For example, the IIC released white papers and technical reports that provide guidance on understanding architectures, techniques, security and testbeds for I-IoT [77], [78], [79]. In addition, NIST released standards regarding industrial wireless systems and industrial control systems, among others, which play critical roles in I-IoT [35], [80]. For example, the recent standardization progress from NIST provides guidance for the deployment of wireless communication in various industrial plants and factories to improve production and reduce cost [80]. Also, IIC has specified factory and plant operations, control systems and backhaul networks for the wireless communication ecosystem [79].

In addition, IEEE has focused on the standardization progress of the Tactile Internet (i.e., IEEE 1918.1) by the Tactile Internet working group [81]. Notice that one application of the Tactile Internet is industrial manufacturing, denoted as Industrial-Tactile IoT [82]. IIC has also proposed a reference architecture (i.e., industrial Internet reference architecture (IIRA)) for general industrial applications in I-IoT [78]. In more detail, the IIRA is an open architecture for I-IoT, which aims to improve the interoperability and guide the application of technologies and standard development. The IIRA specifies the architecture framework, viewpoints from business, usage, function, implementation, and concerns. In addition, the IIC has proposed the edge computing architecture, viewpoints, and use cases for I-IoT, which aim to meet the high performance requirements of industrial applications [77]. Moreover, IIC investigated flexible manufacturing testbeds for automation and control systems in I-IoT ecosystems [79].

F. Summary

We develop the taxonomy to outline the broader research roadmap for networking in Figure 7, where existing research works can be mapped into individual cubes (i.e., research areas). The examples include <Control, FA, Latency> (e.g., [60], [71]), <Monitoring, FA, Latency> (e.g., [60], [68], [71]), <Control, PA, Latency> (e.g., [66], [71]), <Monitoring, PA, Latency> (e.g., [68], [69], [71]), <Monitoring, FA, Reliability> (e.g., [60], [61], [68]), <Monitoring, PA, Reliability> (e.g., [68], [69], [72]), and <Monitoring, PA, Others> (“Others” represents energy efficiency) (e.g., [63]).

It is worth noting that there are a number of cubes that have not been well explored. The example include <Others, FA, Latency> (e.g., “Others” can be reporting data), <Others, PA, Latency>, <Control, FA, Reliability>, <Control, PA, Reliability>, <Control, PA, Others>, <Monitoring, PA, Others> (e.g., “Others” can represents energy efficiency, security, etc.). To fill the gap, we outline several research challenges, which need extensive research efforts in Section VI-A2, including network deployment, resource scheduling and security and privacy.

V. COMPUTING SYSTEMS IN I-IOT

In this section, we first review the computing system in I-IoT and then investigate cloud computing and hybrid cloud and edge based computing architectures for I-IoT. Further, we investigate big data analysis in I-IoT and the necessary computing resources.

A. Overview

From the computing infrastructure perspective, as machine devices have limited capacity in terms of computation and storage, the deployment of computing infrastructure that can provide big data computing and storage for machine devices and support the computing needs for smart-world systems, including smart manufacturing systems, is paramount. Notice that a centralized architecture limits the applicability of cloud computing to machine devices for two reasons. First, the significant volume of data generated from vast numbers of machine devices in disparate geographical locations will be transmitted to the centralized cloud, which could overload the network infrastructure. Second, the centralized cloud is often located far away from machine devices, which could cause high latency during data transmission. For some smart-world systems (e.g., I-IoT), such a latency becomes unacceptable for data analysis and control decision making [83], [84].

Distinct from cloud computing, edge computing tends to leverage the computing and storage capabilities from edge devices (e.g., computing edge nodes). By doing this, edge computing has a great potential to support the computing needs of smart-world systems such as I-IoT. As edge devices are commonly deployed to the locations near to machine devices, some challenges issues (e.g., network overload, high latency) can be addressed [85], [86], [87]. Nonetheless, some challenges remain while leveraging edge computing in smart-world systems (e.g., I-IoT). Some challenges include system management, synchronization, security and privacy, and integration with other network technologies, among others [85], [88]. Indeed, a variety of relevant research efforts have been conducted in this direction. For example, Li *et al.* [71] addressed the issue of integrating SDN and edge computing in I-IoT, and designed an adaptive transmission architecture. Additionally, Tang *et al.* [89] designed a mobile cloud-based scheduling scheme for I-IoT and investigated the task scheduling problem. In their problem formalization, the energy consumption optimization, as well as a number of factors such as task dependency and constraints such as response time deadline are considered. To solve the problem, genetic algorithms were designed and their effectiveness validated.

We use Figure 8 and Figure 9 to illustrate the structures of cloud computing-based architectures and hybrid cloud and edge computing-based architectures for I-IoT, respectively. As shown in Figure 8, the data generated from components in the system will be gathered and transmitted to the cloud for processing, analysis and storage. In Figure 9, we can see that both edge devices and cloud computing facilities will be leveraged to handle data in a multi-tier fashion.

In addition, we propose a three-dimensional framework to explore the problem space of investigating computing systems in I-IoT as shown in Figure 10. The framework consists of three dimensions, including computing tasks, physical systems, and computing

requirements. Particularly, the computing resources are utilized for several computing tasks (i.e., storage, transmission and analysis). The FA and PA are typical examples in physical systems. The computing requirements are QoS-related metrics (latency, reliability, etc.) and others (security, etc.). With the proposed three-dimensional framework, we can investigate existing research efforts by mapping them into the specific cubes shown in the figure.

B. Cloud Computing

Leveraging computing resources from the cloud to aid industrial systems has received significant attention, and is the logical extension of cloud-based services in commercial industries. Applications include cloud manufacturing, among others [83], [84], [90], [91]. For example, Xu [90] presented the specifications of cloud computing and the adoption of cloud computing for manufacturing businesses. The cloud computing system provides computing services (computing, storage, etc.) from cloud resource pools to particular manufacturing tasks. Cloud computing has the advantages of high reliability, scalability, and interoperability, which can improve the efficiency of computing resource utilization in I-IoT. In addition, Tao *et al.* [83] presented a five-layer architecture of perception or access manufacturing resources for adopting cloud computing in manufacturing.

C. Edge Computing

In contrast, edge computing leverages computing resources from network edge devices. Compared to cloud computing, edge computing can provide computing services with much better latency performance, as they are usually located close to end-devices [88], [92]. Concerning general edge computing, Rehman *et al.* [93] proposed the concentric computing model (CCM). The CCM deploys the multi-granular interoperable computing devices and systems in the edge layer of a multilayer architecture. The design of the CCM considers the performance of devices and systems, locations of sensors, devices, servers and data centers, as well as the performance requirements of big data analysis applications, such as bandwidth utilization, latency, resource efficiency, etc. In addition, the challenges of real-time data analytics and streaming, data integration and extraction, and security and privacy were discussed. This work can be mapped to cube <Analysis, PA/FA, QoS> shown in Figure 10.

Furthermore, Chekired *et al.* [94] proposed a multi-tier edge computing architecture to reduce computation and communication latency. In particular, data was divided into two categories (i.e., high priority and low priority) to improve the efficiency of the data computation and transmission. Experiments were conducted to evaluate the effectiveness of two-tier, three-tier, and flat edge computing architectures. The results demonstrate improved performance in their multi-tier edge computing architecture with respect to latency, computational capacity, and other metrics with different workloads. This work can be mapped to the <Transmission, FA, QoS> space shown in Figure 10.

D. Integration of Cloud and Edge Computing

Regarding integration of cloud and edge computing, several research efforts have made strides, demonstrating improvements with respect to latency, reliability, and resource efficiency in I-IoT systems [95], [96], [97]. For example, Shi *et al.* [95] proposed a joint edge-cloud computing architecture to improve latency performance in I-IoT. In

particular, they investigated a load balancing strategy among various edge nodes and cloud servers, with the optimal strategy being derived through a proposed genetic algorithm. The evaluation results demonstrated that, with the increase in task-intensity, the joint edge-cloud computing architecture could outperform disjointed edge computing and cloud computing architectures with respect to delay performance. In addition, they leveraged reallocation and retransmission mechanisms to improve the reliability of the production system in cases of node failures. This work can be mapped into <Transmission, PA, QoS> in Figure 10.

In addition, Kuar *et al.* [96] investigated an edge-cloud integration to support big data streaming services in I-IoT. The interplay of cloud and edge has the benefits of energy efficiency, latency and rich computing resources. Besides, the integration of SDN, as middleware, introduces an architecture of three decoupled planes (i.e., data plane, control plane, and application plane). Further investigating flow scheduling in the control plane, they formalized an energy efficiency-bandwidth tradeoff problem and an energy efficiency-latency tradeoff problem to be solved via multi-objective optimization. Then, they proposed a dynamic flow scheduling and routing scheme to compute the optimal routing solutions, which could adapt to the categories of real-time workflows (e.g., batch processing and stream processing). In doing so, the energy efficiency of the integrated edge-cloud computing system could be improved. This work can be mapped into cube <Transmission, PA/FA, QoS> in Figure 10.

E. Big Data Analysis

Big data in I-IoT refers to the huge volume, velocity, veracity, etc. of data collected from substantial volume of industrial sensors, actuators and devices. Enabling big data sharing is important and the key techniques include the design trading platforms and algorithms [98], [99]. From a data analytics point of view, the available computing resources play a fundamental role in massive and complex data analysis. Particularly, I-IoT envisions the situational awareness, diagnosis, self-healing and prediction of industrial processes, which in turn requires powerful data analysis capabilities [100], [101].

The big data generated by I-IoT systems is heterogeneous in size, volume, velocity, delay and reliability requirements. Thus, it is critical to leverage both time-efficient edge computing and computationally powerful cloud computing to process, store, and retrieve data based on its performance requirements (i.e., time-sensitive and non-time-sensitive). To this end, Fu *et al.* [97] proposed a framework that consists of five entities (I-IoT, edge server, proxy server, cloud server, and data users). In their architecture, the edge server is deployed to extracts and processes data that is time-sensitive data (e.g., control information) so that timely control decisions can be enabled. The proxy server encrypts the data, and the encrypted data and index structure are outsourced to the cloud. The cloud server is also used for data storage and interacting with data users. This work can be mapped to <Storage, PA/FA, QoS> in Figure 10.

Other research efforts have leveraged big data analysis to improve the efficiency of I-IoT. For example, in the monitoring of large-scale industrial systems, we can preprocess collected data in edge devices and upload only critical fault reports and important information for cloud storage and control decisions. In this direction, Oyekanlu [102]

proposed a light-weight database with a small-size dictionary stored from the fully functional monitored machines (motor, turbines, etc.) on edge devices to improve the system efficiency. The edge devices are used to compute and analyze the differences between the machine signals and reference signals, and send only the alert signals and requisite recommendations to the operation center. This work can be mapped into cube <Transmission, FA, Others> in Figure 10.

F. Summary

We develop the taxonomy to outline the broader research roadmap for computing in Figure 10, where existing research works can be mapped into individual cubes (i.e., research areas). Examples include <Storage, FA, QoS> (e.g., [95]), <Transmission, FA, QoS> (e.g., [94], [95], [96]), <Analysis, FA, QoS> (e.g., [83], [90], [93]), <Storage, PA, QoS> (e.g., [97]), <Transmission, PA, QoS> (e.g., [95], [96]), <Analysis, PA, QoS> (e.g., [93]), <Storage, FA, Others> (e.g., [97]), <Transmission, FA, Others> (e.g., [102]). Notice that the element "Others" can represent resource efficiency, security, and others.

There are a number of cubes that have not been well explored. The example include <Analysis, FA, Others>, <Storage, PA, Others>, <Transmission, PA, Others>, <Analysis, PA, Others>, and others. To fill the gap, we outline several research challenges, which need extensive research efforts in Section VI-A3, including deployment, seamless integration and computing resource management.

VI. CHALLENGES AND FUTURE DIRECTIONS

From the above investigation of state-of-the-art technologies for control, networking and computing systems for I-IoT, we now consider the open research challenges and necessary future research directions that are, as of yet, uninvestigated. We first present the challenges and future directions of each of the three types of systems (control, networking, and computing). We then present challenges to and future directions on adopting machine learning techniques to improve control, networking and computing systems in I-IoT.

A. Control, Networking and Computing Systems in I-IoT

1) Control: Recall that industrial control systems can be categorized into centralized, distributed, and hierarchical control systems. In I-IoT, a critical mission is to realize self-awareness, self-diagnosis and self-healing in control systems [44], [100], [101], [103]. With the enabling of self-awareness, the control system is cognizant of the health condition of manufacturing system and its production quality. With the capacity for self-diagnosis and self-healing, failures and faults can be detected and classified, and corresponding healing schemes can be implemented. Moreover, the requirements for resilience in industrial control systems, which face to multidimensional disturbances, raise additional challenges [104], [105].

In I-IoT systems, the computing platforms collect data from industrial devices and perform data analysis. These control systems operate the industrial systems, including the sensors, actuators and controllers. As can be seen in Figure 11a, control objectives are the enabling of awareness, diagnosis, healing and prediction for industrial control systems. In addition, as

shown in Figure 11b, the performance objectives are the realization of efficient management, effective utilization and timely maintenance.

As barriers to enabling self-awareness, self-diagnosis and self-healing in industrial control systems, significant overhead exists for data collection, processing, analysis and transmission. For example, continuous monitoring on the condition and health status of large-scale industrial systems will generate a significant volume data [106], [107]. The data analysis requires high-capacity computing resources (e.g., cloud computing). Moreover, the timely analysis and processing of the massive data is also important to the time-sensitive industrial systems.

Extracting useful information from big industrial data, such as hidden patterns and correlations, can assist control systems in making better decisions. One way to effectively process and analyze big data is to leverage predictive learning algorithms, such as supervised, unsupervised, semi-supervised and reinforcement learning, which are able to find and explore the hidden structure and correlations of the industrial data [108]. For example, Zhou *et al.* [109] designed an intelligence-based control strategy in a DCS-based grinding system. In their proposed system, set-point optimization module, soft-sensor module, and overload diagnosis and adjustment module are included. The system adjusts the set-points in the cases of boundary changes and overload conditions dynamically.

Towards the performance objectives of control systems, efficient management incurs close coordination in every step of the manufacturing lifecycle (i.e., prepare, produce, transport, utilize and recycle). For example, the information exchange between manufacturing lifecycle steps can increase its efficiency by balancing demand and supply. In addition, effective utilization means the full use of the production resources, maximizing productivity and minimizing time and resources wasted. Also, the timely maintenance ensures the health of critical infrastructure such that potential damage or risks can be avoided or minimized. Visualization, virtualization and interoperability are key factors to enabling efficient management, effective utilization and timely maintenance [43]. This visualization provides better presentation and understanding of the infrastructure and assists operators in making optimal decisions. Notice that the immense quantity of devices and equipment with different configurations will increase the complexity of control in terms of observability and controllability.

To satisfy the requirement of resilience on industrial control systems, we shall first understand the resilience of the I-IoT system. However, resilience is a multidimensional property that requires understanding of reactions in the control system to malfunctions, physical component failure, cyberattacks, and so on. The resilience in industrial control systems indicates the ability to survive disturbances [110], [111], [112], [113], [114]. Moreover, the resilience can be measured by the time of reaction for maintaining system functionality following the disturbances. For instance, Arghandeh *et al.* [110] presented a study to define the cyber-physical resilience for the power system. They proposed a framework to assess the resilience of the power system, including system identification, vulnerability analysis, and resilience operations. With the understanding of various disturbances, corresponding mechanisms can be developed to prevent and react

to disturbances. Likewise, to improve the resilience of control systems, Yuan *et al.* [115] leveraged game theory mechanisms to design a control method resilient to cyber-attacks (e.g., denial-of-service (DoS) attacks).

2) Networking: Adopting emerging and low-cost wireless networks in industrial manufacturing and processing systems affords multi-fold benefits. Specifically, it is difficult or infeasible to deploy wired systems in some working environments, such as those with high temperature, extreme locations, and high mobility conditions. In addition, network infrastructures in working environments incur installation and maintenance costs. The significant progress made in wireless network technologies for consumers has great potential for improving network performance and reducing the inherent deployment and maintenance costs, especially in specialized industrial environments.

Nonetheless, designing and deploying wireless communication technologies in the industrial environment is distinct from that of the consumer environment. Generally speaking, the characteristics of networking in industrial systems are small data volume, short communication distance and low mobility. The mobility patterns and traffic patterns shall be considered in the design of wireless networks for industrial systems. In the following, we illustrate the challenges from the perspectives of network deployment and routing optimization as examples.

Network Deployment.: The problem of network deployment is to identify the location of network nodes and access points (AP) with consideration for the densification, distribution, and mobility, of users (i.e., mostly machines) among others. To improve the delay performance and reliability of the wireless network, node placement shall consider different characteristics of industrial systems such as the wireless channel, including fading, multipath, and performance requirements. In particular, the mobility patterns of users in industrial networks are mostly static or near-static. In addition, the mobility of users is typically limited and regular (e.g., robotic arms in an assembly line). In addition, as mentioned above, traffic is characterized by small packets, small communication distance, etc.

To understand the network deployment problem, we show three typical deployment scenarios in industrial plants, which consist of wireless access points, sensors, and actuators in Figure 12. The first deployment scenario in Figure 12a indicates industrial processes that require both sensors and a single actuator. The second deployment scenario, shown in Figure 12b, indicates large numbers of both sensors and actuators involved in processing complex and comprehensive tasks. Furthermore, the third deployment scenario, shown in Figure 12c, illustrates information collection only (i.e., deploying a large number of sensors to collect data from different aspects of the industrial process, without actuation).

To design effective and efficient deployment schemes, the mobility and network traffic patterns of machine devices in I-IoT shall be understood, and all possible mobility scenarios should be covered. Then, the node placement problems can be reduced to optimization problems with the consideration of the mobility patterns and performance requirements [116], [117]. For example, Li *et al.* [116] studied the localization of both static and mobile

nodes with the consideration of interference and coverage in the industrial wireless network. The node placement was formalized as a coverage problem and solved through the proposed double-layer Tabu search.

Resource Scheduling.: The problem of resource scheduling plays a critical role in network performance and information delivery. Traffic scheduling schemes can manage a large amount of traffic with the consideration of system performance metrics and requirements, including latency, utilization of network resources, etc. In I-IoT, latency is a critical requirement, as most data and control information are time-sensitive. As a result, delayed delivery or lost communication may lead to reduced productivity, low efficiency, system failure and safety issues. Real-time information delivery requires that each traffic flow shall be delivered with latency guarantee requirements. Designing appropriate scheduling schemes to meet these performance requirements is challenging as I-IoT involves a massive number of devices (sensors, actuators, etc.) and those devices have diverse performance requirements.

Commonly, resource scheduling algorithms are devoted to solving channel contention or transmission conflicts. Channel contention causes transmission delay, because all channels are assigned to other transmissions, while transmission conflict indicates that multiple transmissions contend over a shared resource. There existing some research efforts toward conducted resource optimization via scheduling in I-IoT [104], [118], [119]. For instance, to solve the channel contention problem, Narayanan *et al.* [119] proposed a link selection mechanism to reduce the channel contention caused by unfair opportunities for channel access. Each gateway performs the link selection mechanism based on the multinomial probability to select a fixed link schedule. With the link selection mechanism, the data transmission in the network is maximized and channel contention is minimized. To address the transmission conflict delay, Wu *et al.* [104] proposed a conflict aware routing (CAR) algorithm for industrial networks. Likewise, Xia *et al.* [120] proposed the path selection algorithm (PSA) to improve the scheduling in industrial networks with enabled narrow band Internet of Things (NB-IoT) modules on sensor nodes.

Security and Privacy.: Ensuring security and privacy of the I-IoT system is a challenging task. Considering that the I-IoT system integrates information communication technologies to enable strong interconnection between industrial devices, the protection of the I-IoT system from cyber-attacks is crucial. Moreover, cyber-attacks on the I-IoT system may cause not only information delay and uncertainty, but also safety issues for humans, the environment, and the machines, as well. In addition, the data collected during industrial manufacturing and production is valuable and privacy-sensitive, which makes I-IoT systems valuable targets for attackers [2], [14], [105], [121], [122], [123], [124], [125], [126].

To investigate the challenges in I-IoT, Sadeghi *et al.* [105] reviewed the security and privacy challenges from three perspectives: attacks on I-IoT systems, attack surfaces, and security goals and requirements. To protect I-IoT systems from attacks, they proposed solutions to protect the industrial devices, including implementing security architectures, integrity verification and secure IoT device management.

As security and privacy of the I-IoT is extremely important, we outline the research directions to protect the security and privacy of I-IoT systems. First, we shall understand security features (e.g., confidentiality, integrity, availability, identification and authentication, privacy and trust, among others) in the context of I-IoT [2]. Then, towards ensuring security of I-IoT, we shall identify and understand security challenges (e.g., node capture attacks, false data injection attacks, DoS attacks, phishing attack, and so on). Towards ensuring data privacy in I-IoT, we shall understand the different steps of data processing (e.g., data collection, data aggregation, and data analysis) in I-IoT. Finally, with an understanding of the security and privacy challenges in I-IoT, corresponding defensive countermeasures and privacy-preserving mechanisms shall be developed to ensure effective security and privacy.

3) Computing: Advancements in computing technologies enable the handling of complex and large-volume industrial data in a timely and efficient manner [85], [88]. Cloud computing, which provides significant computing capabilities, has been adopted in a number of industrial systems, such as manufacturing, state monitoring [36], [127], [128]. Recall that centralized cloud computing will introduce delay to critical data transmissions, as it is often located far away and leads to heavy data traffic to reach the central cloud. In contrast, edge computing, which leverages computing resources from a number of edge servers and gateways, migrates computation tasks to the network edge. Such a distributed structure affords multi-fold benefits, including low transmission delay due to the smaller distance and low congestion at the remote cloud. Nonetheless, several challenges are raised from adopting integrated computing platforms into industrial systems, such as the seamless integration of the edge computing with I-IoT, and resource management and optimization in the distributed edge nodes, which will be further discussed.

Deployment.: One interesting problem is the issue of optimally deploying distributed edge nodes and allocating computing resources to individual machine devices. Given a number of edge nodes that are available in the system, each having different computing capabilities, it is critical to identify the location of edge nodes so that the overall system performance can be maximized. Additionally, given a number of machine devices associated with tasks that may have a variety of latency and reliability requirements, it is important to design effective schemes that are capable of carrying out the optimal assignment of edge nodes to individual machine devices [64]. Such optimal assignment needs to be adaptive to the dynamic environment of smart manufacturing systems. The edge nodes can perform computing tasks for a manufacturing system, such as monitoring and control of physical components, carrying out forecast based on measurements, identifying the root cause of failures and the bottleneck of deployed communication network, etc. It is worth noting that, as latency and reliability are essential requirements in manufacturing systems, the performance metrics that shall be considered include the time taken for the computing infrastructure to accomplish the demanded tasks and the accuracy of decisions. Other metrics to be considered include the energy consumption on machine devices and edge nodes, as well the performance gain of the manufacturing system.

Seamless Integration.: As low latency is one critical requirement in industrial services, the adoption of edge computing is promising. Nonetheless, it is challenging to seamlessly integrate edge computing and I-IoT. The edge nodes are usually light-weight and generally have low computing capacity, making them not well suited to process the massive data generated by the monitoring and control from I-IoT devices. In addition, the dynamic nature of edge servers and gateways usually provide unstable computing capabilities, which may fail to satisfy the requirements of computing services from I-IoT. To address the seamless integration challenges, leveraging the hybrid cloud-edge computing or multi-tier edge computing hierarchy, which integrates high capacity cloud computing and close proximity edge nodes, is promising for improving the stability and latency of computing platforms.

Nonetheless, there remain several challenges in the edge computing paradigm. Examples include programming for edge computing, edge device naming in networks, and others [88], [85]. In cloud computing infrastructures, the cloud platform supports various-purpose programs, typically using one programming language to allocate resources to programs. In contrast, in edge computing, the heterogeneous nature introduces difficulties, as the programming interfaces of deployed edge devices may not be uniform. In addition, as the mobility and availability of edge nodes are highly dynamic, the traditional device naming mechanisms face new challenges.

In Figure 13, we illustrate an example of adopting multi-tier edge and hybrid cloud and edge computing architecture. As can be seen in the figure, the computing resources at the edge (e.g., mobiles, edge nodes, and others) can help to process the data from industrial facilities. Leveraging the computing resources at close-to-end devices, the multi-tier edge computing architecture can effectively reduce the latency of data processing. In addition, the multi-tier architecture can improve the computing efficiency by offloading partial computing tasks from and to the cloud. In this way, high priority and delay sensitive tasks can be processed locally, and low priority and delay tolerant tasks can be processed in the cloud. The integration of multi-tier edge and I-IoT or hybrid cloud and edge computing architecture and I-IoT demands significant in-depth study and practical examination as well.

Computing Resource Management.: Efficient and effective resource allocation and management with regard to strict latency requirements in I-IoT systems can be challenging. One way to efficiently manage distributed computing resource is to design and implement distributed optimization algorithms [129], [130], [131]. For example, Sardellitti *et al.* [131] optimized the joint radio and computing resource allocation with the energy and latency constraints. Other ways to manage distributed computing resources include economic-driven resource allocation schemes, which employ economic mechanisms to determine the value of resources to providers and customers. Economic-driven schemes, such as price-based schemes [132] and auction-based edge resource allocation [133], [134], have been adopted to offload computing tasks to edge nodes. The objective of economic-driven schemes is to obtain overall maximum revenue for the edge computing resource providers. For example, in the context of I-IoT, Sun *et al.* [18] proposed a double auction scheme to determine the price for edge computing resources between the edge server and I-IoT mobile devices. The scheme considers the system efficiency of mobile edge computing (i.e., number of successful trades) as the optimization objective.

4) Research Directions of Control, Networking and Computing for I-IoT: In the following, we present the research needs and future directions of control, networking and computing for I-IoT, including co-design, intelligent data management and analysis, and theoretical foundation, model, and testbed.

- *Co-design of Control, Networking and Computing*: I-IoT is devoted to seamlessly interconnecting complex industrial systems and improving the reliability, efficiency and productivity of industrial systems. Based on the previous sections, we have identified control, networking and computing as the three key systems in I-IoT. Having considered these three systems in detail, it is clear from their interconnected nature that design solely on one aspect without considering others is not sufficient to make I-IoT implementation effective. Thus, the integrated design of control, networking, and computing is an important and promising direction for future research.
- *Intelligent Data Management and Analysis*: As the applications of I-IoT grow in both size and number, the generated data greatly increases in both complexity and variety. The performance requirements raise momentous challenges on existing control systems, communication networks, and computing platforms alike. Both laborious data handling and strict requirements pose difficulties on data management and analysis. As a solution, big data-driven analytics has the potential to transfer the complex datasets to accurate knowledge. Thus, leveraging the intelligent data management and analysis has the potential to improve the performance of control, networking and computing in I-IoT.
- *Theoretical Foundation, Model and Testbed*: Further research efforts shall necessarily focus on the design, implementation, testing and evaluation of various control, networking, and computing techniques for I-IoT. The theoretical foundation and models for the control, networking and computing in I-IoT provides further understanding more effective implementations for IoT in general. With the established theoretical foundation, researchers, engineers, business people, etc. can work together to address potential challenges. Moreover, real-world integrated simulation platforms and testbeds that are capable of implementing I-IoT systems are necessary to evaluate the performance of various techniques before widespread deployment can reliably take place.

B. Machine Learning for I-IoT

In the following, we first provide an overview of machine learning for IoT. We then identify several recent research efforts on machine learning. Furthermore, we use an example to illustrate the use machine learning for improving network performance in IoT. Finally, we present research directions on applying machine learning in I-IoT.

1) Overview: Recall the challenges described previously to control, networking and computing systems in I-IoT. Command and control on large-scale heterogeneous industrial systems is both complex and challenging. Necessarily, the computing platform is expected to be quite powerful and efficient in order to process, analyze and store the big industrial

data in a timely manner. Furthermore, networking systems shall be high in capacity and throughput, as well as provide high reliability and low latency of data transmission.

Machine learning has demonstrated great use in leveraging algorithms and mathematical models to gain the insight and intelligence of numerous systems, including image and video recognition, natural language and text analysis, robotics, autonomous vehicles, and others [135], [136], [137], [138], [139], [140], [141]. The same potential can be employed to aid in the design and operation of I-IoT systems, both holistically and individually in control, networking and computing systems [136], [141], [142], [143], [144]. Generally speaking, machine learning techniques can be categorized as supervised learning (SL), unsupervised learning (USL), and reinforcement learning (RL), with the tasks of machine learning are generalized to classification, prediction and decision. One significant advantage of machine learning is its capability to deal with complex and abstract problems, sometimes in a near-human or even super-human fashion.

In addition, the fields of big data analytics, cloud and edge computing, SDN, and other relevant technologies provide ripe opportunities for the application of machine learning in I-IoT system with the potential to optimize and improve performance and manageability. With machine learning, control, networking and computing in I-IoT systems can become cognizant and dynamic, implementing agile reconfiguration and optimization processes based on measured data. As a result, a better service can be enabled by learning the I-IoT system environment and by the continuous adaptation of I-IoT system parameters as the observed conditions evolve. Despite these achievements, the use of machine learning in I-IoT systems faces significant challenges and shall take into account the exceptional requirements for dependability, security, safety, accuracy, and real-time responsiveness that control systems, networks and computing platforms require. As I-IoT system are large, complex and multidisciplinary systems, how to integrate machine learning into the various components remains challenging and unresolved.

2) Some Relevant Research in Machine Learning: A variety of research investigations already exist towards utilizing machine learning for networking applications. For example, Jiang *et al.* [145] reviewed and investigated a variety of machine learning techniques (e.g., supervised learning, unsupervised learning and reinforcement learning) as tools to improve the performance of next generation networks with various compelling applications, such as massive MIMO, ultra-dense small cell network, issue, Zhang et al. [154] adopted adaptive dropout to prevent overfitting, where the dropout rate of each hidden layer is computed by the adaptive D2D, and so on. In addition, Zhu *et al.* [146] leveraged the reinforcement learning algorithms (i.e., Q-learning) to optimize the packet transmission scheduling in the cognitive network environment for IoT applications. The transmission scheduling algorithm selects the appropriate actions (transmission power, spectrum access, scheduling, etc.) for the cognitive nodes in the multi-channel environment to maximize the system throughput. Also, Lopez-Martin *et al.* [147] used neural networks to conduct traffic classification for IoT networks. The experimental results of their study demonstrated the fantastic detection accuracy by using the combination of different neural networks (recurrent neural network (RNN) and convolutional neural networks (CNN)), in which features were extracted from packet headers. Furthermore, Wang *et al.* [148] reviewed a promising means

of applying machine learning algorithms to address networking challenges and optimize the network design and management.

In addition, the existing research efforts have demonstrated the application of machine learning techniques for I-IoT systems [149], [150], [151], [152], [153]. For example, to facilitate power generation, monitoring, and control related to energy-based I-IoT systems, Mocanu *et al.* [149] designed different machine learning models to perform tasks, including energy disaggregation, flexibility classification and prediction. Likewise, Huang *et al.* [150] developed a deep learning-based scheme to conduct the forecast of electrical loads in the smart grid. Wang *et al.* [151] addressed the image classification issue and designed a feature fusion algorithm. In addition, Li *et al.* [152] proposed efficient and robust deep learning models to inspect and detect defects in manufactured products. Furthermore, Li *et al.* [153] designed a deep convolutional computation model, which can be used to perform hierarchical feature learning on big data in IoT.

In addition, research efforts have been devoted to improving machine learning performance in terms of efficiency and accuracy. For instance, the time and computation-consuming nature of the training phase raises efficiency issues for machine learning models, especially for big industrial data. To improve the efficiency of machine learning, Zhang *et al.* [144] proposed a tensor-train deep compression model to learn hierarchical features for industrial informatics in an efficient manner. The large number of parameters in the model were greatly compressed to decompose the tensors in the deep learning model and improve the speed. Another issue of adopting machine learning for industrial informatics is the lack of training samples. Because of this, deep learning models could degrade classification accuracy due to overfitting. To address this issue, Zhang *et al.* [154] adopted adaptive dropout to prevent overfitting, where the dropout rate of each hidden layer is computed by the adaptive distribution function.

3) Machine Learning for Networking in I-IoT: With the various advantages of machine learning techniques in terms of network performance improvement in I-IoT, a number of challenges need to be addressed before widely developing and adopting machine learning in I-IoT. For example, obtaining valuable and accurate data is critical for the training process of machine learning algorithms. In addition, direct collection of the traffic data is costly in high-speed network environments, posing additional demands on the data preprocessing, including data normalization, discretization, and others. This issue persists in the manufacturing system, in which the low-latency and high reliability of data transmission are critical, and collecting data for machine learning use incurs additional overhead to the network. Thus, how to identify the amount of data that is necessary to be collected and transmitted for machine learning is an important issue to be addressed.

Additionally, proper features for machine learning shall be carefully extracted, which requires an understanding of the specific problems of the system. Furthermore, the computation-hungry nature of machine learning algorithms poses challenges on the delay-sensitive requirements of complex networks in I-IoT systems that may require low-latency and ultra-high reliability for data transmission. Further, the accuracies of the machine learning algorithms, in terms of control, prediction and decision, are also important to

the management of communication networks in I-IoT systems. For example, to improve the efficiency of data transmission in the network, data size needs to be minimized and transmission efficiency needs to be maximized so that network load can be reduced. Nonetheless, when machine learning is used, more data can increase the learning accuracy, but collecting more data will incur additional overhead to the network. Thus, how to balance the need for machine learning (e.g., accuracy) and performance requirements of the network (quality of service, energy efficiency, etc.) becomes an important issue to address.

In applying machine learning in communication networks in I-IoT systems, it is critical to identify the proper machine learning algorithm (i.e., prediction, classification and decision) and its properties to match the needs of the particular network problem. Then, the specific network problem can be analyzed and characteristics can be extracted. In this way, machine learning algorithms having different tasks (e.g., supervised learning, unsupervised learning, and reinforcement learning) and incurring different degrees of overhead can be applied appropriately and individually. In the data collection and preprocessing phase, the data collected shall be accurate and relevant, and the extracted features shall describe the characteristics of the system properly. Furthermore, the proper machine learning model needs to be carefully selected based on the characteristics of the investigated network and system, as well as the particular problem. Finally, the proper machine learning model needs to be validated before wider application, and new data should be leveraged for model adaptation.

4) Research Directions of Machine Learning for I-IoT: To better address the requirements of I-IoT, various aspects of machine learning shall be improved, such as platform, algorithm, efficiency, etc. We thus observe several necessary research directions for machine learning as applied to I-IoT.

- *Machine Learning for Latency-Guaranteed and Ultra-Reliable Communications*: Recall that, in industrial systems, a number of processes will have strict latency, reliability, and other performance requirements. The techniques deployed in the network of an I-IoT system thus shall handle a number of issues, including network deployment, resource management, and so on. As previously mentioned, machine learning can be utilized to address problems and improve network performance. Nonetheless, the effectiveness and efficiency of machine learning in I-IoT scenarios are as of yet unknown, especially given the strict latency and reliability requirements. Thus, research efforts shall be established to study machine learning for latency-guaranteed and ultra-reliable communications.
- *Machine Learning-enabled Cloud and Edge Computing in I-IoT*: Similarly, computing is also a critical factor that affects the latency, reliability, and other performance metrics in I-IoT. Recall that I-IoT needs powerful and efficient computing platforms to provide storage, transmission and analysis of industrial big data. The hybrid cloud and edge computing platform has the capability and efficiency to offer a viable computing infrastructure for IoT. Nonetheless, for a sufficiently complex learning problem, it may be infeasible to carry out training in-device due to limits on the complexity, storage, and processing power. Thus,

the use of the edge computing infrastructure to reduce network latency could reduce the effectiveness of learning process. The integration of edge computing infrastructures and machine learning shall be studied, especially in an industrial big data context. Particularly, the implementation of parallel and distributed learning for edge architectures need to be considered and optimized for self-organization, efficiency, runtime, etc. In addition, machine learning algorithms with tunable parameters and platforms shall be investigated and optimized such that learning decisions can be made quickly.

- *Intelligent Sensing and Decision Making*: The control problems in I-IoT can be simplified to the sensing and decision processes among the massively dispersed sensors and actuators. Enabling intelligent sensing can bring the capabilities of classification, prediction and decision directly to the control systems. The requirements of sensing and decision making are extremely strict in a manufacturing environment, as the failure will cause economic loss and possible safety issues. Effectively transferring the capabilities of classification, prediction and decision from machine learning to the sensing and decision-making centers is a promising research direction.
- *Online Learning and Re-learning*: I-IoT enables highly scalable, interoperable and interconnected industrial systems, where the control, networking and computing systems are in dynamic environments. It is common practice that machine learning models require sufficient training to make sure that the output of learning processes are accurate and can be used in the decision process. Nonetheless, as the IoT system is dynamic and evolving, machine learning system shall be capable of adapting to such complex environments. One way to enable adaptability is to leverage online learning and re-training techniques to continuously update machine learning models, but additional study is required to realize this capability.
- *Distributed Machine Learning*: Distributed machine learning is devoted to addressing the problems of the large-scale machine learning process, such as long training times, large training datasets, etc. The methodology of distributed machine learning is the leveraging of multiple computing resources to collaboratively work on one task. Distributed machine learning places and processes data training and testing phases into a number of distributed nodes simultaneously to improve time efficiency. Moreover, distributed machine learning is expected to be a very important technique for machine learning in the I-IoT environment. One of the challenges for distributed machine learning is how to efficiently manage the distributed computing resources. There is a need to develop performance metrics to support resource optimization. Resource allocation may need for adaptation in some applications due to their dynamic (time-varying) nature.
- *Light-weight Learning Platform*: In I-IoT, a number of industrial devices are interconnected to form a fully interconnected smart industrial factory or plant. Most of the industrial devices, such as sensors, actuators and controllers are not

designed to run learning algorithms. Nonetheless, the computing capabilities enabled by smart industrial devices can be potentially leveraged for light-weighted learning platforms. Notice that those light-weight learning platforms with limited resources (e.g., computing, energy, and others) can be used to run light-weight learning tasks. In this way, the learning on industrial devices can be enabled to improve the intelligence and performance of I-IoT. One direction is to design hardware-in-the-loop (HIL) simulation platform for I-IoT, which integrates the computer simulation for I-IoT applications with hardware testbeds for sensors and actuators. The key of the HIL simulation platform is to use the real-world data produced from sensor and actuator hardware testbeds. Another direction is to design the integrated simulation framework for I-IoT, which can be used to capture the interaction and reciprocal effects of cyber and physical systems in I-IoT.

VII. FINAL REMARKS

In this paper, a comprehensive survey of I-IoT has been presented, including I-IoT architecture, applications and characteristics, existing research efforts on control, networking and computing systems in I-IoT, as well as challenges and future research needs. More specifically, the I-IoT architecture consists of application layer, communication layer and physical layer, and I-IoT applications can be categorized to process automation (PA) or factory automation (FA). Characteristics of I-IoT applications include the number of nodes, cycle time, and reliability, among others. From the I-IoT system perspective, we have considered the three critical components of control, networking and computing systems in I-IoT. Regarding control systems, we have investigated the centralized, decentralized and hierarchical industrial control architectures. In networking systems, we have reviewed some representative networking technologies (e.g., 5G, M2M and SDN) and discussed their uses in I-IoT. Considering computing systems, we have studied the recent advances in computing technologies (e.g., cloud computing, edge computing, and integration of cloud and edge computing), and their applicability for I-IoT.

In addition to assessing the current technological trends and their uses for I-IoT, we have carefully considered the challenges to networking and computing systems. These include the difficulties of network deployment and resource scheduling for networking systems, and the problems of seamless integration and computing resource management for computing systems. Reflecting the needs raised by these challenges, we have further outlined future research needs from the perspectives of control, networking and computing systems in I-IoT. Finally, we have made particular note of the emerging machine learning techniques for I-IoT, and extracted key future directions that need to be resolved for appropriate machine learning in I-IoT. The primary goals of this survey are to identify the key components of I-IoT systems, provide comprehensive and systematic review of the topic, and outline key research challenges that need to be addressed.

REFERENCES

[1]. Jeong S, Na W, Kim J, and Cho S, "Internet of Things for smart manufacturing system: Trust issues in resource allocation," IEEE Internet of Things Journal, 2018.

[2]. Lin J, Yu W, Zhang N, Yang X, Zhang H, and Zhao W, "A survey on Internet of Things: Architecture, enabling technologies, security and privacy, and applications," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125–1142, 2017.

[3]. Xu G, Yu W, Griffith D, Golmie N, and Moulema P, "Toward integrating distributed energy resources and storage devices in smart grid," IEEE Internet of Things Journal, vol. 4, no. 1, pp. 192–204, Feb 2017. [PubMed: 29354654]

[4]. Lu Y, "Industry 4.0: A survey on technologies, applications and open research issues," Journal of Industrial Information Integration, vol. 6, pp. 1–10, 2017.

[5]. Columbus L, "Roundup of Internet of Things forecasts and market estimates, 2016. forbes, november 27, 2016," https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#81d22e292d51, 2016.

[6]. Lee I. and Lee K, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," Business Horizons, vol. 58, no. 4, pp. 431–440, 2015.

[7]. Centenaro M, Vangelista L, Zanella A, and Zorzi M, "Long-range communications in unlicensed bands: The rising stars in the IoT and smart city scenarios," IEEE Wireless Communications, vol. 23, no. 5, pp. 60–67, 2016.

[8]. Li B. and Yu J, "Research and application on the smart home based on component technologies and Internet of Things," Procedia Engineering, vol. 15, pp. 2087–2092, 2011.

[9]. Jie Y, Pei JY, Jun L, Yun G, and Wei X, "Smart home system based on IoT technologies," in Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on. IEEE, 2013, pp. 1789–1791.

[10]. Santoso FK and Vun NC, "Securing IoT for smart home system," in Consumer Electronics (ISCE), 2015 IEEE International Symposium on. IEEE, 2015, pp. 1–2.

[11]. Yun M. and Yuxin B, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in Advances in Energy Engineering (ICAEE), 2010 International Conference on. IEEE, 2010, pp. 69–72.

[12]. Lin J, Yu W, Yang X, Yang Q, Fu X, and Zhao W, "A real-time en-route route guidance decision scheme for transportation-based cyberphysical systems," IEEE Transactions on Vehicular Technology, vol. 66, no. 3, pp. 2551–2566, March 2017.

[13]. Rathore MM, Ahmad A, Paul A, and Jeon G, "Efficient graphoriented smart transportation using Internet of Things generated big data," in 2015 11th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS). IEEE, 2015, pp. 512–519.

[14]. Da Xu L, He W, and Li S, "Internet of Things in industries: A survey," IEEE Transactions on industrial informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[15]. Lee J, Bagheri B, and Kao H-A, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," Manufacturing Letters, vol. 3, pp. 18–23, 2015.

[16]. Lasi H, Fettke P, Kemper H-G, Feld T, and Hoffmann M, "Industry 4.0," Business & Information Systems Engineering, vol. 6, no. 4, pp. 239–242, 2014.

[17]. Shu L, Mukherjee M, Pecht M, Crespi N, and Han SN, "Challenges and research issues of data management in IoT for large-scale petrochemical plants," IEEE Systems Journal, no. 99, pp. 1–15, 2017.

[18]. Sun W, Liu J, Yue Y, and Zhang H, "Double auction-based resource allocation for mobile edge computing in industrial Internet of Things," IEEE Transactions on Industrial Informatics, 2018.

[19]. Duan P, Jia Y, Liang L, Rodriguez J, Huq KMS, and Li G, "Space-reserved cooperative caching in 5G heterogeneous networks for industrial IoT," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, p. 2715, 2018.

[20]. Chaudhary R, Aujla GS, Garg S, Kumar N, and Rodrigues JJ, "SDN-enabled multi-attribute-based secure communication for smart grid in IIoT environment," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2629–2640, 2018.

[21]. Wollschlaeger M, Sauter T, and Jasperneite J, “The future of industrial communication: Automation networks in the era of the Internet of Things and industry 4.0,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 17–27, 2017.

[22]. Tseng F-H, Tsai M-S, Tseng C-W, Yang Y-T, Liu C-C, and Chou LD, “A lightweight auto-scaling mechanism for fog computing in industrial applications,” IEEE Transactions on Industrial Informatics, 2018.

[23]. Mueller H, Gogouvitis SV, Seitz A, and Bruegge B, “Seamless computing for industrial systems spanning cloud and edge,” in High Performance Computing & Simulation (HPCS), 2017 International Conference on. IEEE, 2017, pp. 209–216.

[24]. Luvisotto M, Pang Z, and Dzung D, “Ultra high performance wireless control for critical applications: Challenges and directions,” IEEE Transactions on Industrial Informatics, vol. 13, no. 3, pp. 1448–1459, 2017.

[25]. Zhou K, Liu T, and Zhou L, “Industry 4.0: Towards future industrial opportunities and challenges,” in Fuzzy Systems and Knowledge Discovery (FSKD), 2015 12th International Conference on. IEEE, 2015, pp. 2147–2152.

[26]. Drath R. and Horch A, “Industrie 4.0: Hit or hype? [industry forum],” IEEE Industrial Electronics Magazine, vol. 8, no. 2, pp. 56–58, June 2014.

[27]. Leitão P, Colombo AW, and Karnouskos S, “Industrial automation” based on cyber-physical systems technologies: Prototype implementations and challenges,” Computers in Industry, vol. 81, pp. 11–25, 2016.

[28]. Gubbi J, Buyya R, Marusic S, and Palaniswami M, “Internet of Things (IoT): A vision, architectural elements, and future directions,” Future generation computer systems, vol. 29, no. 7, pp. 1645–1660, 2013.

[29]. Mumtaz S, Alsohaily A, Pang Z, Rayes A, Tsang KF, and Rodriguez J, “Massive Internet of Things for industrial applications: Addressing wireless I-IoT connectivity challenges and ecosystem fragmentation,” IEEE Industrial Electronics Magazine, vol. 11, no. 1, pp. 28–33, 2017.

[30]. Zhan M, Pang Z, Dzung D, and Xiao M, “Channel coding for high performance wireless control in critical applications: Survey and analysis,” IEEE Access, 2018.

[31]. Luvisotto M, Pang Z, Dzung D, Zhan M, and Jiang X, “Physical layer design of high-performance wireless transmission for critical control applications,” IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 2844–2854, 2017.

[32]. Frotzscher A, Wetzker U, Bauer M, Rentschler M, Beyer M, Elspass S, and Klessig H, “Requirements and current solutions of wireless communication in industrial automation,” in Communications workshops (ICC), 2014 IEEE international conference on. IEEE, 2014, pp. 67–72.

[33]. Yang TC, “Networked control system: a brief survey,” IEE Proceedings-Control Theory and Applications, vol. 153, no. 4, pp. 403–412, 2006.

[34]. Scattolini R, “Architectures for distributed and hierarchical model predictive control–a review,” Journal of process control, vol. 19, no. 5, pp. 723–731, 2009.

[35]. Stouffer K, Pillitteri V, Lightman S, Abrams M, and Hahn A, “Guide to industrial control systems (ICS) security,” NIST Special Publication, vol. 800, no. 82, 2015.

[36]. Sajid A, Abbas H, and Saleem K, “Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges,” IEEE Access, vol. 4, pp. 1375–1384, 2016.

[37]. Hunzinger R, “SCADA fundementals and applications in the IoT,” Internet of Things and Data Analytics Handbook, pp. 283–293, 2017.

[38]. Lu G. and Yang Y, “IoT and smart infrastructure,” Internet of Things and Data Analytics Handbook, pp. 481–493, 2017.

[39]. Alhebshi F, Alnabilsi H, Alzebaidi J, Bensenouci A, Brahimi T, and Bensenouci M-A, “Monitoring the operation of transmission line in a smart grid system through IoT,” in Learning and Technology Conference (L&T), 2018 15th. IEEE, 2018, pp. 139–146.

[40]. Shahzad A, Kim Y-G, and Elgamoudi A, “Secure IoT platform for industrial control systems,” in Platform Technology and Service (PlatCon), 2017 International Conference on. IEEE, 2017, pp. 1–6.

[41]. El-Shafei MA, El-Hawwary MI, and Emara HM, “Implementation of fractional-order PID controller in an industrial distributed control system,” in Systems, Signals & Devices (SSD), 2017 14th International Multi-Conference on. IEEE, 2017, pp. 713–718.

[42]. Barenji RV, Barenji AV, and Hashemipour M, “A multi-agent RFID-enabled distributed control system for a flexible manufacturing shop,” The International Journal of Advanced Manufacturing Technology, vol. 71, no. 9–12, pp. 1773–1791, 2014.

[43]. Karnouskos S. and Colombo AW, “Architecting the next generation of service-based SCADA/DCS system of systems,” in 37th annual conference of the IEEE industrial electronics society (IECON 2011), Melbourne, Australia, 2011, pp. 7–10.

[44]. Lü Z, L ü Y, Yuan M, and Wang Z, “A heterogeneous large-scalë parallel SCADA/DCS architecture in 5G OGCE,” in Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI), 2017 10th International Congress on. IEEE, 2017, pp. 1–7.

[45]. teanu D. Selis¸, Roman M, endrescu DS, Petre E, and Popa B, “A distributed control system for processes in food industry: Architecture and implementation,” in 2018 19th International Carpathian Control Conference (ICCC). IEEE, 2018.

[46]. Singh M, Sreejeth M, Singh P, Mathur R, and Ranjan R, “Implementation and analysis of PLC SCADA controlled closed loop four quadrant speed control of chopper fed DC motor,” in Electrical Power and Energy Systems (ICEPES), International Conference on. IEEE, 2016, pp. 327–332.

[47]. Endi M, Elhalwagy Y. et al., “Three-layer PLC/SCADA system architecture in process automation and data monitoring,” in Computer and Automation Engineering (ICCAE), 2010 The 2nd International Conference on, vol. 2. IEEE, 2010, pp. 774–779.

[48]. Linthicum DS, “Responsive data architecture for the Internet of Things,” IEEE Computer, vol. 49, no. 10, pp. 72–75, 2016.

[49]. Stankovic JA, “Research directions for the Internet of Things,” IEEE Internet of Things Journal, vol. 1, no. 1, pp. 3–9, 2014.

[50]. Huang J, Xing C-C, Shin SY, Hou F, and Hsu C-H, “Optimizing M2M communications and quality of services in the IoT for sustainable smart cities,” IEEE Transactions on Sustainable Computing, vol. 3, no. 1, pp. 4–15, 2018.

[51]. Xia N, Chen H-H, and Yang C-S, “Radio resource management in machine-to-machine communications: A survey,” IEEE Communications Surveys and Tutorials, vol. 20, no. 1, pp. 791–828, 2018.

[52]. Kim J, Lee J, Kim J, and Yun J, “M2M service platforms: Survey, issues, and enabling technologies.” IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 61–76, 2014.

[53]. Wu Y, Yu W, Griffith DW, and Golmie N, “Modeling and performance assessment of dynamic rate adaptation for m2m communications,” IEEE Transactions on Network Science and Engineering, pp. 1–1, 2018.

[54]. Laya A, Alonso L, and Alonso-Zarate J, “Is the random access channel of LTE and LTE-A suitable for M2M communications? a survey of alternatives.” IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 4–16, 2014.

[55]. Bi Z, Da Xu L, and Wang C, “Internet of things for enterprise systems of modern manufacturing,” IEEE Transactions on industrial informatics, vol. 10, no. 2, pp. 1537–1546, 2014.

[56]. Yu W, Xu H, Zhang H, Griffith D, and Golmie N, “Ultra-dense networks: Survey of state of the art and future directions,” in Computer Communication and Networks (ICCCN), 2016 25th International Conference on. IEEE, 2016, pp. 1–10.

[57]. Szymanski T, “Strengthening security and privacy in an ultra-dense green 5G radio access network for the industrial and tactile Internet of Things,” in Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International. IEEE, 2017, pp. 415–422.

[58]. Andrews JG, Buzzi S, Choi W, Hanly SV, Lozano A, Soong AC, and Zhang JC, “What will 5G be?” IEEE Journal on Selected Areas in Communications, vol. 32, no. 6, pp. 1065–1082, 2014.

[59]. Ding M. and Perez DL, “Promises and caveats of uplink IoT´ ultra-dense networks,” in Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE, 2018, pp. 1–6.

[60]. Orsino A, Kovalchukov R, Samuylov A, Moltchanov D, Andreev S, Koucheryavy Y, and Valkama M, "Caching-aided collaborative D2D operation for predictive data dissemination in industrial IoT," arXiv preprint arXiv:1802.06902, 2018.

[61]. Lee BM and Yang H, "Massive MIMO for industrial Internet of Things in cyber-physical systems," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2641–2652, 2018.

[62]. Bag G, Thrybom L, and Hovila P, "Challenges and opportunities of 5G in power grids," CIRED-Open Access Proceedings Journal, vol. 2017, no. 1, pp. 2145–2148, 2017.

[63]. Lyu L, Chen C, Zhu S, and Guan X, "5G enabled codesign of energyefficient transmission and estimation for industrial IoT systems," IEEE Transactions on Industrial Informatics, vol. 14, no. 6, pp. 2690–2704, 2018.

[64]. Wu Y, Yu W, Zhang J, Griffith D, Golmie N, and Lu C, "A 3d topology optimization scheme for m2m communications," in 2018 19th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), June 2018, pp. 15–20.

[65]. Navarro-Ortiz J, Sendra S, Ameigeiras P, and Lopez-Soler JM, "Integration of LoRaWAN and 4G/5G for the industrial Internet of Things," IEEE Communications Magazine, vol. 56, no. 2, pp. 60–67, 2018.

[66]. Lu C, Saifullah A, Li B, Sha M, Gonzalez H, Gunatilaka D, Wu C, Nie L, and Chen Y, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," Proceedings of the IEEE, vol. 104, no. 5, pp. 1013–1024, 2016.

[67]. Nunes BAA, Mendonca M, Nguyen X-N, Obraczka K, and Turletti T, "A survey of software-defined networking: Past, present, and future of programmable networks," IEEE Communications Surveys & Tutorials, vol. 16, no. 3, pp. 1617–1634, 2014.

[68]. Henneke D, Wisniewski L, and Jasperneite J, "Analysis of realizing a future industrial network by means of software-defined networking (SDN)," in Factory Communication Systems (WFCS), 2016 IEEE World Conference on. IEEE, 2016, pp. 1–4.

[69]. Baddeley M, Nejabati R, Oikonomou G, Gormus S, Sooriyabandara M, and Simeonidou D, "Isolating SDN control traffic with layer-2 slicing in 6TiSCH industrial IoT networks," in Network Function Virtualization and Software Defined Networks (NFV-SDN), 2017 IEEE Conference on. IEEE, 2017, pp. 247–251.

[70]. Watteyne T, Palattella M, and Grieco L, "Using IEEE 802.15. 4e time-slotted channel hopping (TSCH) in the Internet of Things (IoT): Problem statement," Internet Engineering Task Force (IETF), Request for Comments: 7554, 2015.

[71]. Li X, Li D, Wan J, Liu C, and Imran M, "Adaptive transmission optimization in SDN-based industrial Internet of Things with edge computing," IEEE Internet of Things Journal, 2018.

[72]. Al-Rubaye S, Kadhum E, Ni Q, and Anpalagan A, "Industrial Internet of Things driven by SDN platform for smart grid resiliency," IEEE Internet of Things Journal, 2017.

[73]. Bizanis N. and Kuipers FA, "SDN and virtualization solutions for the Internet of Things: a survey," IEEE Access, vol. 4, pp. 5591–5606, 2016.

[74]. Ma Y-W, Chen Y-C, and Chen J-L, "SDN-enabled network virtualization for industry 4.0 based on IoTs and cloud computing," in Advanced Communication Technology (ICACT), 2017 19th International Conference on. IEEE, 2017, pp. 199–202.

[75]. Granelli F, Gebremariam AA, Usman M, Cugini F, Stamati V, Alitska M, and Chatzimisios P, "Software defined and virtualized wireless access in future wireless networks: scenarios and standards," IEEE Communications Magazine, vol. 53, no. 6, pp. 26–34, 2015.

[76]. Luo S, Wang H, Wu J, Li J, Guo L, and Pei B, "Improving energy efficiency in industrial wireless sensor networks using SDN and NFV," in Vehicular Technology Conference (VTC Spring), 2016 IEEE 83rd. IEEE, 2016, pp. 1–5.

[77]. "Introduction to Edge Computing in I-IoT an industrial Internet consortium white paper," https://www.iiconsortium.org/pdf/Introduction_to_Edge_Computing_in_I-IoT_2018-06-18.pdf, industrial Internet Consortium (IIC).

[78]. "The Industrial Internet of Things Volume G1: Reference architecture," https://www.iiconsortium.org/IICPUBG1V1.802017-01-31.pdf, industrial Internet Consortium (IIC).

[79]. "Time sensitive networks for flexible manufacturing testbed - description of converged traffic types," https://www.iiconsortium.org/pdf/IIC_TSN_Testbed_Traffic_Whitepaper_20180418.pdfIIC_TSN_Testbed_Traffic_Whitepaper_20180418.pdf, industrial Internet Consortium (IIC).

[80]. Candell R, Hany MT, Lee KB, Liu Y, Quimby JT, and Remley CA, "Guide to industrial wireless systems deployments," Tech. Rep, 2018.

[81]. "1918.1- tactile internet: Application scenarios, definitions and terminology, architecture, functions, and technical assumptions," https://standards.ieee.org/develop/project/1918.1.html, iEEE standards association.

[82]. Szymanski TH, "Securing the industrial-tactile Internet of Things with deterministic silicon photonics switches," IEEE Access, vol. 4, pp. 8236–8249, 2016.

[83]. Tao F, Zuo Y, Da Xu L, and Zhang L, "IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing," IEEE Transations on Industrial Informatics, vol. 10, no. 2, pp. 1547–1557, 2014.

[84]. Tao F, Cheng Y, Da Xu L, Zhang L, and Li BH, "CCIoT-CMfg: cloud computing and Internet of Things-based cloud manufacturing service system," IEEE Transactions on Industrial Informatics, vol. 10, no. 2, pp. 1435–1442, 2014.

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

[86]. Garcia Lopez P, Montresor A, Epema D, Datta A, Higashino T, Iamnitchi A, Barcellos M, Felber P, and Riviere E, "Edge-centric computing: Vision and challenges," ACM SIGCOMM Computer Communication Review, vol. 45, no. 5, pp. 37–42, 2015.

[87]. Patel P, Ali MI, and Sheth A, "On using the intelligent edge for IoT analytics," IEEE Intelligent Systems, vol. 32, no. 5, pp. 64–69, 2017.

[88]. Yu W, Liang F, He X, Hatcher WG, Lu C, Lin J, and Yang X, "A survey on the edge computing for the Internet of Things," IEEE Access, vol. 6, pp. 6900–6919, 2017.

[89]. Tang C, Wei X, Xiao S, Chen W, Fang W, Zhang W, and Hao M, "A mobile cloud based scheduling strategy for industrial Internet of Things," IEEE Access, vol. 6, pp. 7262–7275, 2018.

[90]. Xu X, "From cloud computing to cloud manufacturing," Robotics and computer-integrated manufacturing, vol. 28, no. 1, pp. 75–86, 2012.

[91]. Yu W, Xu G, Chen Z, and Moulema P, "A cloud computing based architecture for cyber security situation awareness," in 2013 IEEE Conference on Communications and Network Security (CNS), Oct 2013, pp. 488–492.

[92]. "A cloud/edge computing streaming system for network traffic monitoring and threat detection," Int. J. Secur. Netw, vol. 13, no. 3, pp. 169–186, Jan. 2018. [Online]. Available: 10.1504/IJSN.2018.10014317

[93]. ur Rehman MH, Ahmed E, Yaqoob I, Hashem IAT, Imran M, and Ahmad S, "Big data analytics in industrial IoT using a concentric computing model," IEEE Communications Magazine, vol. 56, no. 2, pp. 37–43, 2018.

[94]. Chekired DA, Khoukhi L, and Mouftah HT, "Industrial IoT data scheduling based on hierarchical fog computing: A key for enabling smart factory," IEEE Transactions on Industrial Informatics, 2018.

[95]. Shi C, Ren Z, Yang K, Chen C, Zhang H, Xiao Y, and Hou X, "Ultra-low latency cloud-fog computing for industrial Internet of Things," in Wireless Communications and Networking Conference (WCNC), 2018 IEEE. IEEE, 2018, pp. 1–6.

[96]. Kaur K, Garg S, Aujla GS, Kumar N, Rodrigues JJ, and Guizani M, "Edge computing in the industrial internet of things environment: Software-defined-networks-based edge-cloud interplay," IEEE Communications Magazine, vol. 56, no. 2, pp. 44–51, 2018.

[97]. Fu J, Liu Y, Chao H-C, Bhargava B, and Zhang Z, "Secure data storage and searching for industrial IoT by integrating fog computing and cloud computing," IEEE Transactions on Industrial Informatics, 2018.

[98]. Liang F, Yu W, An D, Yang Q, Fu X, and Zhao W, "A survey on big data market: Pricing, trading and protection," IEEE Access, vol. 6, pp. 15132–15154, 2018.

[99]. Gao W, Yu W, Liang F, Hatcher WG, and Lu C, “Privacy-preserving auction for big data trading using homomorphic encryption,” IEEE Transactions on Network Science and Engineering, pp. 1–1, 2018.

[100]. Wang Z, Chen B, Wang J, and Chen C, “Networked microgrids for self-healing power systems,” IEEE Transactions on smart grid, vol. 7, no. 1, pp. 310–319, 2016.

[101]. Wang Z. and Wang J, “Self-healing resilient distribution systems based on sectionalization into microgrids,” IEEE Trans. Power Syst, vol. 30, no. 6, pp. 3139–3149, 2015.

[102]. Oyekanlu E, “Predictive edge computing for time series of industrial IoT and large scale critical infrastructure based on open-source software analytic of big data,” in Big Data (Big Data), 2017 IEEE International Conference on. IEEE, 2017, pp. 1663–1669.

[103]. Wu Z, Wu Y, Chai T, and Sun J, “Data-driven abnormal condition identification and self-healing control system for fused magnesium furnace,” IEEE Transactions on Industrial Electronics, vol. 62, no. 3, pp. 1703–1715, 2015.

[104]. Wu C, Gunatilaka D, Sha M, and Lu C, “Real-time wireless routing for industrial Internet of Things,” in Internet-of-Things Design and Implementation (IoTDI), 2018 IEEE/ACM Third International Conference on. IEEE, 2018, pp. 261–266.

[105]. Sadeghi A-R, Wachsmann C, and Waidner M, “Security and privacy challenges in industrial Internet of Things,” in Design Automation Conference (DAC), 2015 52nd ACM/EDAC/IEEE. IEEE, 2015, pp. 1–6.

[106]. Lee J, Ardakani HD, Yang S, and Bagheri B, “Industrial big data analytics and cyber-physical systems for future maintenance & service innovation,” Procedia CIRP, vol. 38, pp. 3–7, 2015.

[107]. O’Donovan P, Leahy K, Bruton K, and O’Sullivan DT, “An industrial big data pipeline for data-driven analytics maintenance applications in large-scale smart manufacturing facilities,” Journal of Big Data, vol. 2, no. 1, p. 25, 2015.

[108]. Mohammadi M, Al-Fuqaha A, Sorour S, and Guizani M, “Deep learning for IoT big data and streaming analytics: A survey,” IEEE Communications Surveys and Tutorials, pp. 1–1, 2018.

[109]. Zhou P, Chai T, and Sun J, “Intelligence-based supervisory control for optimal operation of a DCS-controlled grinding system,” IEEE Transactions on Control Systems Technology, vol. 21, no. 1, pp. 162–175, 2013.

[110]. Arghandeh R, von Meier A, Mehrmanesh L, and Mili L, “On the definition of cyber-physical resilience in power systems,” Renewable and Sustainable Energy Reviews, vol. 58, pp. 1060–1069, 2016.

[111]. Li Y, Shi D, and Chen T, “False data injection attacks on networked control systems: A stackelberg-game analysis,” IEEE Transactions on Automatic Control, pp. 1–1, 2018.

[112]. Yang Q, Yang J, Yu W, An D, Zhang N, and Zhao W, “On false data-injection attacks against power system state estimation: Modeling and countermeasures,” IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 717–729, March 2014.

[113]. Lin J, Yu W, Yang X, Xu G, and Zhao W, “On false data injection attacks against distributed energy routing in smart grid,” in Proceedings of the 2012 IEEE/ACM Third International Conference on Cyber-Physical Systems, ser. ICCPS ‘12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 183–192. [Online]. Available: 10.1109/ICCPS.2012.26

[114]. Kriaa S, Pietre-Cambacedes L, Bouissou M, and Halgand Y, “A survey of approaches combining safety and security for industrial control systems,” Reliability Engineering & System Safety, vol. 139, pp. 156–178, 2015.

[115]. Yuan Y, Yuan H, Guo L, Yang H, and Sun S, “Resilient control of networked control system under DoS attacks: A unified game approach,” IEEE Transactions on Industrial Informatics, vol. 12, no. 5, pp. 1786–1794, 2016.

[116]. Li X, Li D, Dong Z, Hu Y, and Liu C, “Efficient deployment of key nodes for optimal coverage of industrial mobile wireless networks,” Sensors, vol. 18, no. 2, p. 545, 2018.

[117]. Wang L, An L, Ni H-Q, Ye W, Pardalos PM, and Fei M-R, “Pareto-based multi-objective node placement of industrial wireless sensor networks using binary differential evolution harmony search,” Advances in Manufacturing, vol. 4, no. 1, pp. 66–78, 2016.

[118]. Li B, Ma Y, Westenbroek T, Wu C, Gonzalez H, and Lu C, “Wireless routing and control: a cyber-physical case study,” in CyberPhysical Systems (ICCPS), 2016 ACM/IEEE 7th International Conference on. IEEE, 2016, pp. 1–10.

[119]. Narayanan R, Srinivasan M, Karthikeya SA, and Murthy CSR, “A novel fairness-driven approach for heterogeneous gateways’ link scheduling in IoT networks,” in Communications (ICC), 2017 IEEE International Conference on. IEEE, 2017, pp. 1–7.

[120]. Xia C, Jin X, Kong L, Zeng P, and Guan D, “Scheduling for heterogeneous industrial networks based on NB-IoT technology,” in Industrial Electronics Society, IECON 2017–43rd Annual Conference of the IEEE. IEEE, 2017, pp. 3518–3523.

[121]. Liu Y, Ning P, and Reiter MK, “False data injection attacks against state estimation in electric power grids,” ACM Trans. Inf. Syst. Secur, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011. [Online]. Available: 10.1145/1952982.1952995

[122]. Humayed A, Lin J, Li F, and Luo B, “Cyber-physical systems securitya survey,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1802–1831, Dec 2017.

[123]. Ling Z, Luo J, Xu Y, Gao C, Wu K, and Fu X, “Security vulnerabilities of internet of things: A case study of the smart plug system,” IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1899–1909, Dec 2017.

[124]. Soltan S, Mittal P, and Poor HV, “Blackiot: Iot botnet of high wattage devices can disrupt the power grid,” in 27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018, pp. 15–32. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/soltan

[125]. Celik ZB, Babun L, Sikder AK, Aksu H, Tan G, McDaniel P, and Uluagac AS, “Sensitive information tracking in commodity iot,” in 27th USENIX Security Symposium (USENIX Security 18). Baltimore, MD: USENIX Association, 2018, pp. 1687–1704. [Online]. Available: https://www.usenix.org/conference/usenixsecurity18/presentation/celik

[126]. Wurm J, Hoang K, Arias O, Sadeghi A-R, and Jin Y, “Security analysis on consumer and industrial IoT devices,” in Design Automation Conference (ASP-DAC), 2016 21st Asia and South Pacific. IEEE, 2016, pp. 519–524.

[127]. Tao F, Zuo Y, Da Xu L, and Zhang L, “Iot-based intelligent perception and access of manufacturing resource toward cloud manufacturing.” IEEE Trans. Industrial Informatics, vol. 10, no. 2, pp. 1547–1557, 2014.

[128]. Hossain MS and Muhammad G, “Cloud-assisted Industrial Tnternet of Things (I-IoT)–enabled framework for health monitoring,” Computer Networks, vol. 101, pp. 192–202, 2016.

[129]. Pham Q-V, LeAnh T, Tran NH, and Hong CS, “Decentralized computation offloading and resource allocation in heterogeneous networks with mobile edge computing,” arXiv preprint arXiv:1803.00683, 2018.

[130]. Cui Y, He W, Ni C, Guo C, and Liu Z, “Energy-efficient resource allocation for cache-assisted mobile edge computing,” in Local Computer Networks (LCN), 2017 IEEE 42nd Conference on. IEEE, 2017, pp. 640–648.

[131]. Sardellitti S, Scutari G, and Barbarossa S, “Joint optimization of radio and computational resources for multicell mobile-edge computing,” IEEE Transactions on Signal and Information Processing over Networks, vol. 1, no. 2, pp. 89–103, 2015.

[132]. Nguyen DT, Le LB, and Bhargava V, “Price-based resource allocation for edge computing: A market equilibrium approach,” IEEE Transactions on Cloud Computing, 2018.

[133]. Luong NC, Xiong Z, Wang P, and Niyato D, “Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach,” arXiv preprint arXiv:1711.02844, 2017.

[134]. Jiao Y, Wang P, Niyato D, and Xiong Z, “Social welfare maximization auction in edge computing resource allocation for mobile blockchain,” arXiv preprint arXiv:1710.10595, 2017.

[135]. Witten IH, Frank E, Hall MA, and Pal CJ, Data Mining: Practical machine learning tools and techniques. Morgan Kaufmann, 2016.

[136]. Booz J, Yu W, Xu G, Griffith D, and Golmie N, “A deep learning-based weather forecast system for data volume and recency analysis,” in Proc. of IEEE International Conference on Computing, Networking and Communications (ICNC). IEEE, 2019.

[137]. Ge L, Zhang H, Xu G, Yu W, Chen C, and Blasch EP, “Towards mapreduce based machine learning techniques for processing massive network threat monitoring data,” Networking for Big Data, published by CRC Press & Francis Group, USA, Yu S. (Ed.), Lin X. (Ed.), Misic J. (Ed.), Shen, 2015.

[138]. Robert C, “Machine learning, a probabilistic perspective,” 2014.

[139]. Yu W, An D, Griffith D, Yang Q, and Xu G, “Towards statistical modeling and machine learning based energy usage forecasting in smart grid,” SIGAPP Appl. Comput. Rev, vol. 15, no. 1, pp. 6–16, Mar. 2015. [Online]. Available: 10.1145/2753060.2753061

[140]. Buczak AL and Guven E, “A survey of data mining and machine learning methods for cyber security intrusion detection,” IEEE Communications Surveys & Tutorials, vol. 18, no. 2, pp. 1153–1176, 2016.

[141]. Hatcher WG and Yu W, “A survey of deep learning: Platforms, applications and emerging research trends,” IEEE Access, vol. 6, pp. 24411–24432, 2018.

[142]. Luo X, Liu J, Zhang D, and Chang X, “A large-scale web qos prediction scheme for the industrial Internet of Things based on a kernel machine learning algorithm,” Computer Networks, vol. 101, pp. 81–89, 2016.

[143]. Lavassani M, Forsstrom S, Jennehag U, and Zhang T, “Combining¨ fog computing with sensor mote machine learning for industrial IoT,” Sensors, vol. 18, no. 5, p. 1532, 2018.

[144]. Zhang Q, Yang LT, Chen Z, and Li P, “A tensor-train deep computation model for industry informatics big data feature learning,” IEEE Transactions on Industrial Informatics, 2018.

[145]. Jiang C, Zhang H, Ren Y, Han Z, Chen K-C, and Hanzo L, “Machine learning paradigms for next-generation wireless networks,” IEEE Wireless Communications, vol. 24, no. 2, pp. 98–105, 2017.

[146]. Zhu J, Song Y, Jiang D, and Song H, “A new deep-q-learning-based transmission scheduling mechanism for the cognitive internet of things,” IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2375–2385, Aug 2018.

[147]. Lopez-Martin M, Carro B, Sanchez-Esguevillas A, and Lloret J, “Network traffic classifier with convolutional and recurrent neural networks for Internet of Things,” IEEE Access, vol. 5, pp. 18042–18050, 2017.

[148]. Wang M, Cui Y, Wang X, Xiao S, and Jiang J, “Machine learning for networking: Workflow, advances and opportunities,” IEEE Network, vol. 32, no. 2, pp. 92–99, 2018.

[149]. Mocanu DC, Mocanu E, Nguyen PH, Gibescu M, and Liotta A, “Big IoT data mining for real-time energy disaggregation in buildings,” in Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on. IEEE, 2016, pp. 003765–003769.

[150]. Huang Y, Ma X, Fan X, Liu J, and Gong W, “When deep learning meets edge computing,” in 2017 IEEE 25th International Conference on Network Protocols (ICNP). IEEE, 2017, pp. 1–2.

[151]. Wang Y, Song B, Zhang P, Xin N, and Cao G, “A fast feature fusion algorithm in image classification for cyber physical systems,” IEEE Access, vol. 5, pp. 9089–9098, 2017.

[152]. Li L, Ota K, and Dong M, “Deep learning for smart industry: Efficient manufacture inspection system with fog computing,” IEEE Transactions on Industrial Informatics, 2018.

[153]. Li P, Chen Z, Yang LT, Zhang Q, and Deen MJ, “Deep convolutional computation model for feature learning on big data in Internet of Things,” IEEE Transactions on Industrial Informatics, vol. 14, no. 2, pp. 790–798, 2018.

[154]. Zhang Q, Yang LT, Chen Z, Li P, and Bu F, “An adaptive droupout deep computation model for industrial IoT big data learning with crowdsourcing to cloud computing,” IEEE Transactions on Industrial Informatics, 2018.

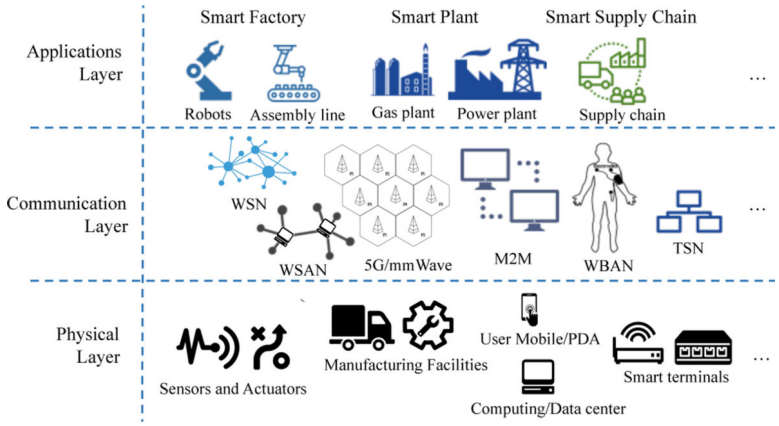

Fig. 1:
I-IoT System Architecture

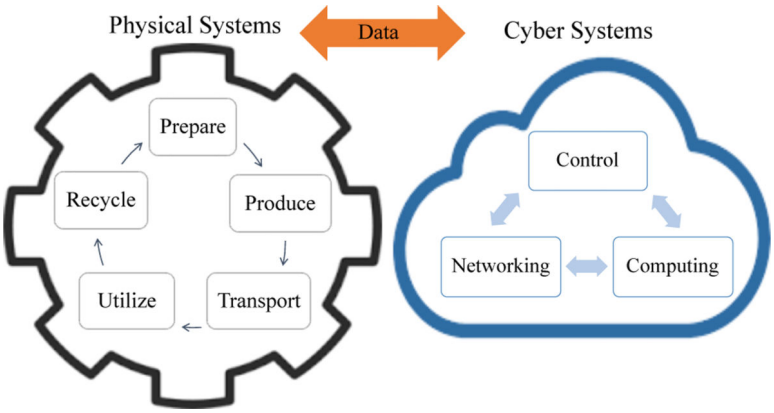

Fig. 2:

I-IoT from a CPS Perspective: the gear on the left encapsulates the lifecycle of physical systems, while the cloud figure on the right describes the cyber systems (i.e., the interplay between control, networking and computing systems)

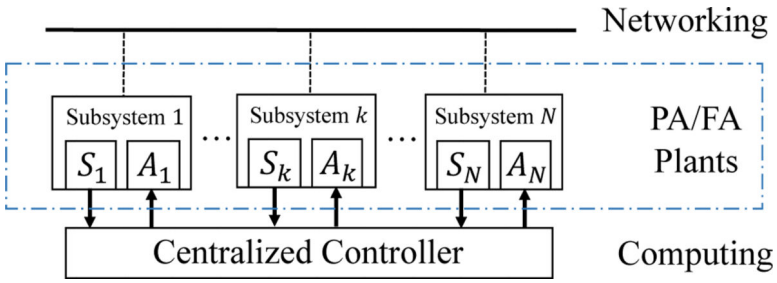

Fig. 3:
Structure of Centralized Control

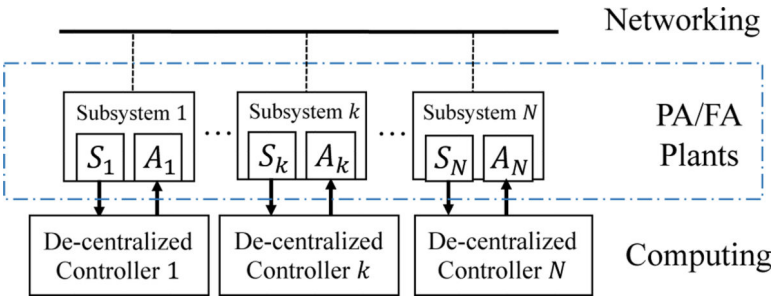

Fig. 4:
Structure of Decentralized Control

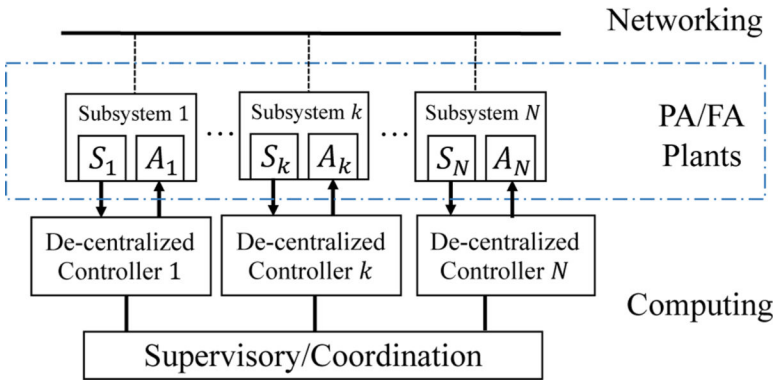

Fig. 5:
Structure of Hierarchical Control

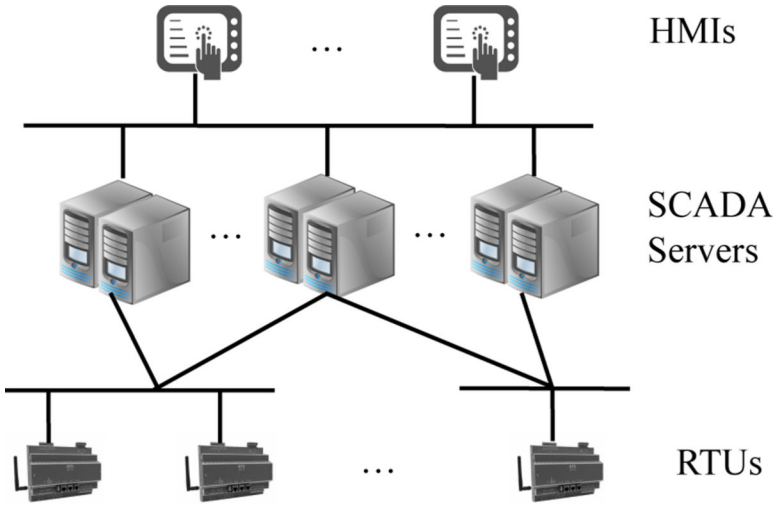

Fig. 6:
Simplified SCADA Architecture

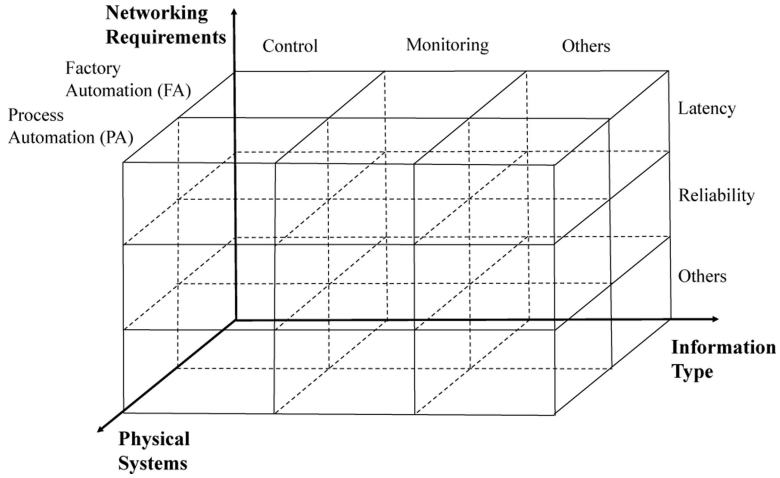

Fig. 7:
Taxonomy of Networking in I-IoT

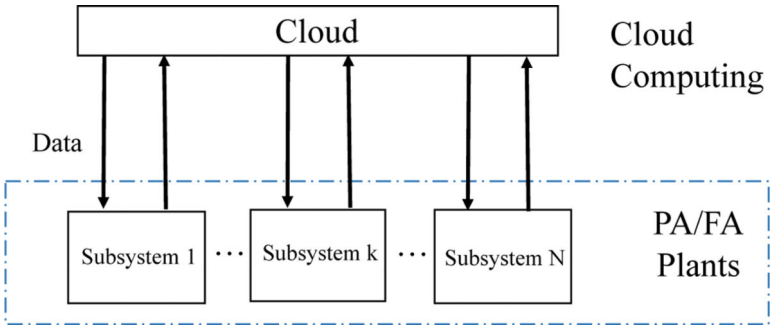

Fig. 8:
Structure of Cloud Computing for I-IoT

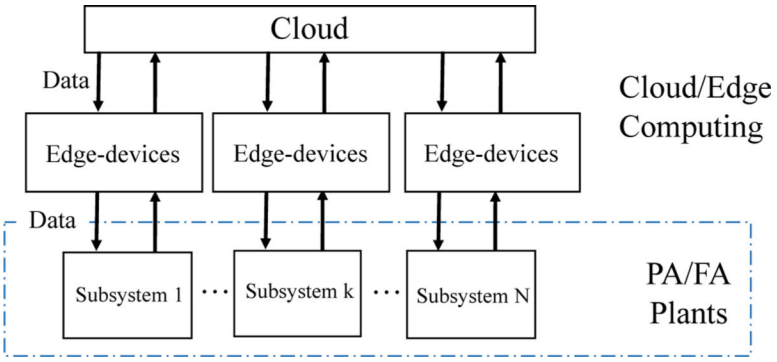

Fig. 9:
Structure of Hybrid Cloud and Edge Computing for I-IoT

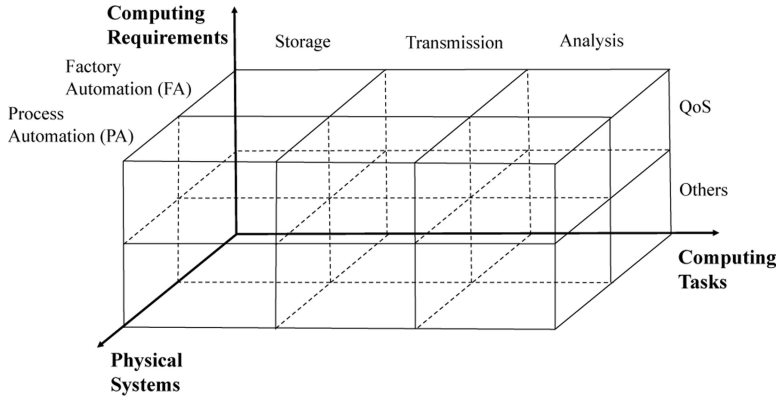

Fig. 10:
Taxonomy of Computing Systems in I-IoT

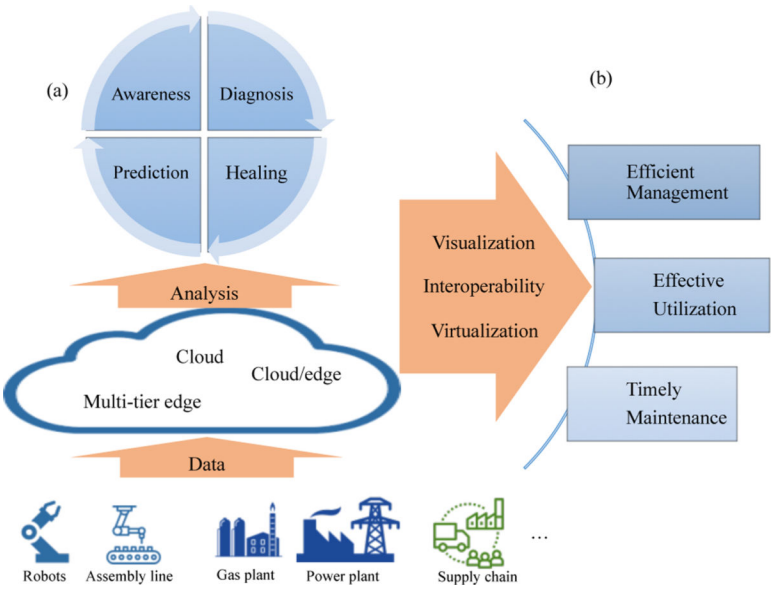

Fig. 11:

Objectives of Control Systems in I-IoT System: (a) Control Objectives, (b) Performance Objectives

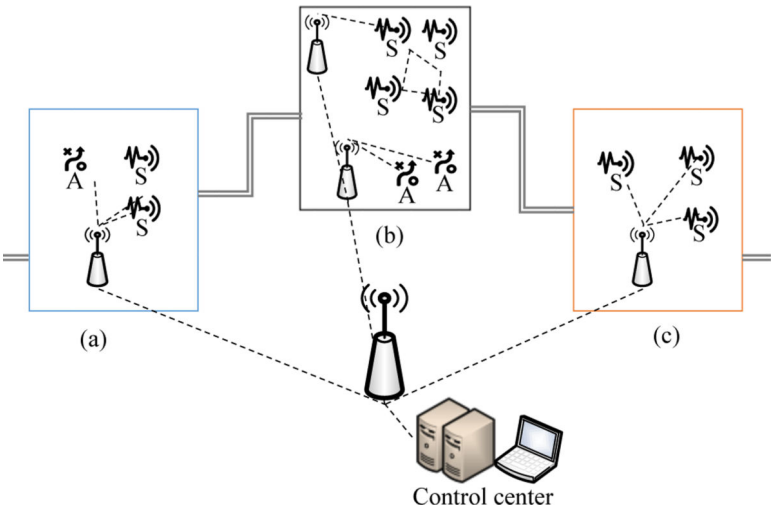

Fig. 12:

Network Deployment Scenarios: (a) multiple sensors are deployed to sense information and guide the actions of one actuator, (b) multiple sensors and actuators are deployed in the manufacturing area to perform complex sensing and actuating and tasks, (c) only multiple sensors are deployed to collect information about the complex manufacturing area

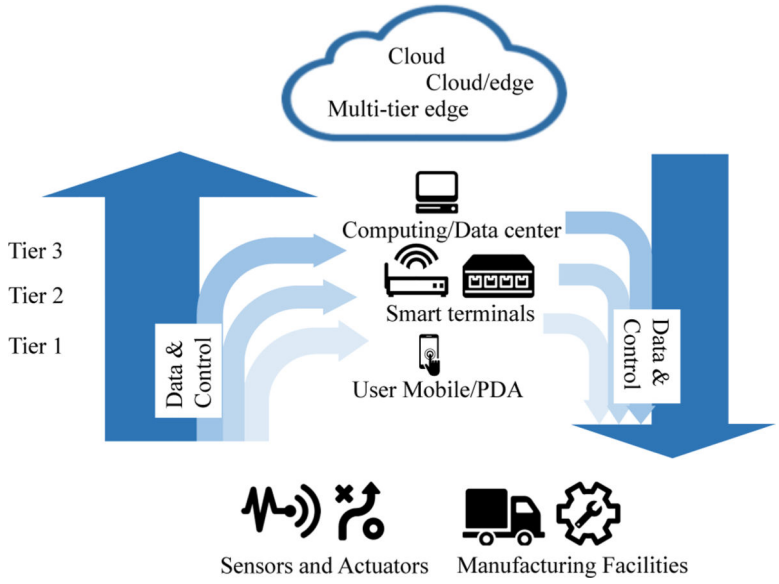

Fig. 13:
Hierarchical Computing Architecture

TABLE I:

Acronym and Description

Acronym	Description
AES	Advanced Encryption Standard
AP	Access Point
BS	Base Station
CAR	Conflict Aware Routing
CCM	Concentric Computing Model
CPS	Cyber-Physical System
CN	Core Network
CNN	Convolutional Neural Network
DCS	Distributed Control System
D2D	Device-to-Device
DoS	Denial-of-Service
FA	Factory Automation
FG	Functional Group
HIL	Hardware-In-the-Loop
HMI	Human Machine Interface
I-CPS	Industrial Cyber-Physical System
I-IoT	Industrial Internet of Things
IIRA	Industrial Internet Reference Architecture
IoT	Internet of Things
LoRaWAN	Low-Power Wide Area Network
LTE	Long-Term Evolution
LTE-A	Long-Term Evolution Advanced
Massive MIMO	Massive Multiple-Input and Multiple-Output
M2M	Machine-to-Machine
NB-IoT	Narrow Band Internet of Things
NFV	Network Function Virtualization
NV	Network Virtualization
PA	Process Automation
PER	Packet Error Rate
PID	Proportional-Integral-Derivative
PLC	Programmable Logic Controller
PSA	Power System Automation
PSA	Path Selection Algorithm
QoS	Quality of Service
RAN	Radio Access Network
RFID	Radio-Frequency Identification
RL	Reinforcement Learning
RNN	Recurrent Neural Network
RTU	Remote Terminal Unit

Acronym	Description
SCADA	Supervisory Control And Data Acquisition
SDI	Software-Defined Infrastructure
SL	Supervised Learning
SDN	Software Defined Networking
TSCH	Time Scheduled Channel Hopping
UDN	Ultra-Dense Network
UL	Uplink
USL	Unsupervised Learning
WSAN	Wireless Sensor and Actuator Network

TABLE II:

Characteristics of Industrial Applications [31]

Application Type	Number of Nodes	Cycle Time	Reliability
PA	10^1	100ms	Medium
FA	10^3	1ms	High