A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications

Jie Lin, Wei Yu, Nan Zhang, Xinyu Yang, Hanlin Zhang, and Wei Zhao

***Abstract*—Fog/edge computing has been proposed to be integrated with Internet of Things (IoT) to enable computing services devices deployed at network edge, aiming to improve the user's experience and resilience of the services in case of failures. With the advantage of distributed architecture and close to end-users, fog/edge computing can provide faster response and greater quality of service for IoT applications. Thus, fog/edge computing-based IoT becomes future infrastructure on IoT development. To develop fog/edge computing-based IoT infrastructure, the architecture, enabling techniques, and issues related to IoT should be investigated first, and then the integration of fog/edge computing and IoT should be explored. To this end, this paper conducts a comprehensive overview of IoT with respect to system architecture, enabling technologies, security and privacy issues, and present the integration of fog/edge computing and IoT, and applications. Particularly, this paper first explores the relationship between cyber-physical systems and IoT, both of which play important roles in realizing an intelligent cyber-physical world. Then, existing architectures, enabling technologies, and security and privacy issues in IoT are presented to enhance the understanding of the state of the art IoT development. To investigate the fog/edge computing-based IoT, this paper also investigate the relationship between IoT and fog/edge computing, and discuss issues in fog/edge computing-based IoT. Finally, several applications, including the smart grid, smart transportation, and smart cities, are presented to demonstrate how fog/edge computing-based IoT to be implemented in real-world applications.**

***Index Terms*—Applications, enabling technologies, fog/edge computing, Internet of Things (IoT), security and privacy.**

I. Introduction

FOG/EDGE computing is an architecture organized by the networking edge devices or clients to provide computing services for customers or applications in the space between networking central servers and end-users [16], [147]. In fog/edge computing, the massive data generated by different kinds of Internet of Things (IoT) devices can be processed at the network edge instead of transmitting it to the centralized cloud infrastructure due to bandwidth and energy consumption concerns [103], [116]. Because fog/edge computing is organized as distributed architecture and can process data and store data in networking edge devices, which is close to end-users, fog/edge computing can provide services with faster response and greater quality, in comparison with cloud computing [147]. Thus, fog/edge computing is more suitable to be integrated with IoT to provide efficient and secure services for a large number of end-users, and fog/edge computing-based IoT can be considered as the future IoT infrastructure [16].

To design and deploy fog/edge computing-based IoT, the concept and features of IoT should be investigated first. IoT can connect ubiquitous devices and facilities with various networks to provide efficient and secure services for all applications anytime and anywhere [9], [80]. Based on the aforementioned definition, two features are required in IoT. First, IoT is the extension of the net or Internet [10], meaning that, in IoT, various networks should coexist, and the interoperability among these networks is critical for information delivery and supporting applications [7], [87]. Interconnection is a critical architecture issue in IoT [131]. Second, things connected in IoT are no longer limited to devices or objects, but can also be information, human behaviors, etc. [119], [123]. Thus, IoT should include mechanisms that handle the connection of objects in a broader manner.

There have been a number of research efforts devoted to developing IoT prototypical systems [131], [136]. Nonetheless, most of the systems that focus on specific applications are implemented within extranet or intranet, and have no interaction with each other. Based on the features of IoT that interconnection is a critical architecture issue, strictly speaking, these systems or applications are not "IoT," but the "Net of Things," or can even be considered as "Net of Devices," and the interactions between these extranets and intranets were missed [123], [131]. Thus, IoT should cover all things in large-scale networks, in which various networks should coexist, and are able to interact with each other via various gateways and middlewares, supported by the complex control plane [87]. One vision is that a generalized network infrastructure that integrates various networks should be designed,

Manuscript received September 27, 2016; revised February 13, 2017; accepted February 28, 2017. Date of publication March 15, 2017; date of current version October 9, 2017. This work was supported in part by the National Science Foundation (NSF) under Grant CNS 1350145 and in part by the USM Wilson H. Elkins Professorship fund. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the agencies. *(Corresponding author: Wei Yu.)*

J. Lin and X. Yang are with the Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an 710049, China (e-mail: jielin@xjtu.edu.cn; yxyphd@mail.xjtu.edu.cn).

W. Yu is with the Department of Computer and Information Sciences, Towson University, Towson, MD 21252 USA (e-mail: wyu@towson.edu).

N. Zhang is with Department of Computer Science, George Washington University, Washington, DC 20052 USA (e-mail: nzhang10@gwu.edu).

H. Zhang is with the Department of Computer Science and Technology, Qingdao University, Qingao 266061, China (e-mail: hanlin@qdu.edu.cn).

W. Zhao is with the Department of Computer and Information Science, University of Macau, Macau, China (e-mail: weizhao@umac.mo).

Digital Object Identifier 10.1109/JIOT.2017.2683200

and all IoT-based systems or applications can provide their services by efficiently sharing network resources and information across the generalized network infrastructure. For example, in smart cities [14], [155], if a generalized network infrastructure can be implemented and is able to cover all regions in a city, applications (smart grid, smart transportation, smart healthcare, etc.) can share their individual network infrastructures to enable data collection and information delivery. In this vision, everything that is interconnected in the network can be realized because all applications can interact with each other easily and share the resources effectively. The implementation of generalized network infrastructure can reduce the cost of network deployment as well [155].

To have a generalized network infrastructure, the development of IoT with respect to architectures, enabling technologies, and possible challenges should be studied first. In recent years, several published survey papers reviewed the IoT technologies from different aspects. For example, the survey work done by Atzori *et al.* [10] presented the enabling communication technologies and different visions of IoT, which can help those who want to approach this field have a primary understanding of IoT. The survey work done by Al-Fuqaha *et al.* [7] presented the enabling technologies, protocols, and possible applications of IoT, in which the horizontal overview of IoT was provided and the key IoT challenges were presented to point out the future directions. There have been also a number of research efforts devoted to security and privacy issues in IoT. For instance, the survey work done by Andrea *et al.* [8] presented the security vulnerabilities and challenges in IoT from the view of applications, networks, and physical systems, and considered the security and privacy issues in technologies associated with physical systems, networking, software, and encryption. The survey work done by Sha *et al.* [115] presented challenges issues and opportunities in IoT. In addition to the aforementioned survey papers, Botta *et al.* [18] considered the integration of cloud computing and IoT. Also, Wu and Zhao [131] proposed a novel IoT infrastructure, namely WInternet, which can be designed and realized by current Internet technologies, and meets various requirements of IoT. Although a number of efforts have been conducted, most existing surveys have only focused on specific aspects of IoT. This calls for a comprehensive survey of IoT to help newcomers have a general understanding of the complex discipline of this emergent research area.

To full the gap, this paper first reviews the existing efforts on IoT and then present the integration of fog/edge computing and IoT and related issues. In particular, this paper conduct a comprehensive overview of IoT with respect to architectures, enabling technologies, security and privacy issues, and present the foundation of fog/edge computing-based IoT and applications. Meanwhile, possible open issues and challenges in IoT are presented as well. Particularly, the relation between cyber-physical systems (CPSs) and IoT is explored first. Notice that both CPS and IoT emphasize the interactions between the cyber world and the physical world, and are easily confused with one another. In addition, the difference between CPS and IoT has not been clearly distinguished before. The detailed relation between CPS and IoT can help newcomers to understand the concept and features of IoT. Then, to provide a better understanding of the state of the art in IoT development, the architectures, enabling technologies, and challenges in IoT are clearly presented. We consider IoT as multilayer architectures, divided into the perception layer, networking layer, service layer, and application layer. Based on the multilayer architecture, enabling technologies and open issues in each layer are then presented. After that, security vulnerabilities and challenges are discussed, and the security issues with respect to confidentiality, integrity, availability, as well as privacy issues in IoT are discussed. In addition, the integration of IoT and fog/edge computing and related issues are presented to enable the design and deployment of fog/edge computing-based IoT. Finally, several applications (smart grid, smart transportation, and smart cities) are presented to illustrate how fog/edge computing-based IoT are to be implemented in real-world IoT-based systems.

This paper is organized as follows. We introduce relation between CPS and IoT in Section II. We present the architectures of IoT in Section III. We present the enabling technologies and challenges of IoT in Section IV. We present the security and privacy issues of IoT in Section V. The integration of IoT and fog/edge computing is presented in Section VI. Finally, we conclude this paper in Section VIII.

II. CPSs AND IoT

In this section, the relation between CPS and IoT is clarified. In the following, we first give the overview of CPS and then discuss the key differences between CPS and IoT.

A. Overview of CPS

Generally speaking, CPS is referred to as the system that can efficiently integrate both cyber and physical components through the integration of the modern computing and communication technologies [5], [130], aiming to changing the method of interaction among the human, cyber and physical worlds. CPS emphasizes the interactions between cyber and physical components and has a goal of making the monitoring and control of physical components secure, efficient, and intelligent by leveraging cyber components [23].

In CPS, "cyber" means using the modern sensing, computing, and communication technologies to effectively monitor and control the physical components, while "physical" means the physical components in real world, and "system" reflects the complexity and diversity. Based on the clarification, we can see that a CPS consists of multiple heterogeneous distributed subsystems [50]. Similar to the development of IoT, CPS has been developed in numerous areas [50], [72], [73], including smart grid, smart transportation, etc.

As shown in [23], the CPS is the integration of physical components, sensors, actuators, communication networks, and control centers, in which sensors are deployed to measure and monitor the status of physical components, actuators are deployed to ensure the desirable operations on physical components, and communication networks are used to deliver measured data and feedback comments among sensors, actuators, and control centers. The control centers are

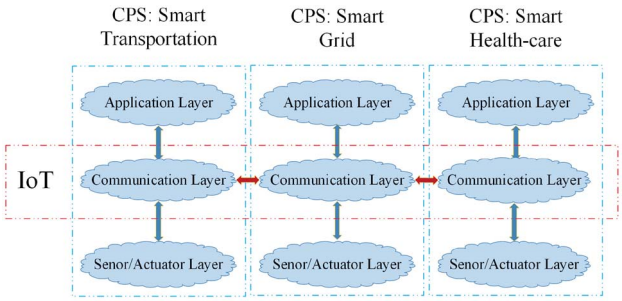

Fig. 1. Integration of IoT and CPS.

used to analyze measured data and sent feedback commands to actuators, ensuring the system operate in desired states [23], [143].

B. Difference Between CPS and IoT

Based on the overview of CPS, we know that both CPS and IoT aim to achieve the interaction between cyber world and physical world [99]. Particularly, CPS and IoT can measure the state information of physical components via smart sensor devices without human's input. Meanwhile, in both CPS and IoT, the measured state information can be transmitted and shared through wired or wireless communication networks. After the analysis of measured state information, both CPS and IoT can provide secure, efficient, and intelligent services to applications. The existing efforts on CPS applications and IoT applications have been expanded to similar areas (smart grid, smart transportation, smart city, etc.).

Because of the similarities between CPS and IoT, it is an urgent need to clarify the difference between CPS and IoT so that newcomers may enter this complex discipline easily. Nonetheless, few existing efforts clearly identify the difference between CPS and IoT, and several efforts have even considered the CPS and IoT to be the same concept. Thus, to fulfil this gap, the difference of CPS and IoT is clarified below.

As mentioned above, the essence of CPS is the system and the main objective of CPS is to measure the state information of physical devices and ensure the secure, efficient, and intelligent operation on physical devices. In CPS, the sensor/actuator layer, communication layer, and application (control) layer are present. The sensor/actuator layer is used to collect real-time data and execute commands, communication layer is used to deliver data to upper layer and commands to lower layer, and application (control) layer is used to analyze data and make decisions. Fig. 1 illustrates the three layers in CPS. From this figure, we can see that CPS is a vertical architecture.

In contrast, IoT is a networking infrastructure to connect a massive number of devices and to monitor and control devices by using modern technologies in cyber space. Thus, the key of IoT is "interconnection." The main objective of IoT is to interconnect various networks so that the data collection, resource sharing, analysis, and management can be carried out across heterogeneous networks. By doing so, reliable, efficient, and secure services can be provided. Thus, IoT is a horizontal architecture, which should integrate communication layers of all CPS applications to achieve interconnection, as shown in Fig. 1. Notice that, the interconnection of various networks is not only limited to physical connections. Control plane (interfaces, middleware, protocols, etc.) should be designed to ensure that data can be efficiently delivered across different kinds of networks and shared. For instance, in a smart city, networks of smart weather forecasting, smart transportation, and smart grid should be interconnected and interact with each other. Data from smart transportation and smart weather forecasting should be processed and extracted and used by the smart grid to determine the states and brightness of street-lamps to ensure efficient use of energy resources, as well as traffic safety at night.

Actually, control plane in IoT is more complex than that in Internet and has been ignored by most if not all. Recently, some efforts have been focused on the control plane in IoT. For example, Wu and Zhao [131] proposed an IoT architecture, namely WInternet, which focuses on interconnecting various Net of Things into a large-scale global network. In WInternet, the internal architecture of nodes was innovated with embedded computing capability to ensure that critical applications can interaction with physical space. Also, protocols (netlet computation and pipe communication protocol) were designed to meet requirements of IoT applications.

To summarize, the basic difference between CPS and IoT is that, CPS is considered as a system, while IoT is considered as "Internet." The common requirements for both CPS and IoT are real-time, reliable, and secure data transmission. The distinct requirements for CPS and IoT are listed as follows: for CPS, effective, reliable, accurate, real-time control is primary goal, while for IoT, resource sharing and management, data sharing and management, interface among different nets, massive-scale data and big data collection and storage, data mining, data aggregation and information extraction, and high quality of network quality of service (QoS) are important services.

In fact, one of the most representative applications that integrate CPS and IoT is smart cities, in which several CPS applications operate simultaneously, including smart gird, smart transportation, smart healthcare, etc. As shown in Fig. 1, the communication layers of all applications are interconnected as a unified network to provide service for smart cities.

III. ARCHITECTURE

In this section, we show several existing architectures for IoT.

A. Three-Layer Architecture

Typically, the architecture of IoT is divided into three basic layers [83]: 1) application layer; 2) network layer; and 3) perception layer, which are further described below.

1) Perception Layer: It is also known as the sensor layer, is implemented as the bottom layer in IoT architecture [11]. The perception layer interacts with physical devices and components through smart devices (RFID, sensors, actuators, etc.). Its main objectives are to connect things into IoT network, and to measure, collect, and process the state information associated with these things via deployed smart devices, transmitting the processed information into upper layer via layer interfaces.

2) Network Layer: It is also known as the transmission layer, is implemented as the middle layer in IoT architecture [68]. The network layer is used to receive the processed information provided by perception layer and determine the routes to transmit the data and information to the IoT hub, devices, and applications via integrated networks. The network layer is the most important layer in IoT architecture, because various devices (hub, switching, gateway, cloud computing perform, etc.), and various communication technologies (Bluetooth, Wi-Fi, long-term evolution, etc.) are integrated in this layer. The network layer should transmit data to or from different things or applications, through interfaces or gateways among heterogeneous networks, and using various communication technologies and protocols.

3) Application Layer: It is also known as the business layer, is implemented as the top layer in IoT architecture [7]. The application layer receives the data transmitted from network layer and uses the data to provide required services or operations. For instance, the application layer can provide the storage service to backup received data into a database, or provide the analysis service to evaluate the received data for predicting the future state of physical devices. A number of applications exist in this layer, each having different requirements. Examples include smart grid, smart transportation, smart cities, etc. [124], [132].

The three-layer architecture is basic for IoT and has been designed and realized in a number of systems [132]. Yet, despite the simplicity of the multilayer architecture of IoT, functions and operations in the network and application layers are diverse and complex. For example, the network layer not only needs to determine routes and transmit data, but also provide data services (data aggregation, computing, etc.). The application layer not only needs to provide services to customers and devices, it must also provide data services (data mining, data analytics, etc.). Thus, to establish a generic and flexible multilayer architecture for IoT, a service layer should be developed between network layer and application layer to provide the data services in IoT. Based on this concept, service-oriented architectures (SoAs) have recently been developed to support IoT [7], [136].

B. SoA-Based Architecture

Generally speaking, SoA is a component-based model, which can be designed to connect different functional units (also known as services) of an application via interfaces and protocols [10], [86], [135]. SoA can focus on designing the workflow of coordinated services, and enable the reuse of software and hardware components, improving the feasibility of SoA for use in designing IoT architecture [10], [136]. Thus, SoA can be easily integrated into IoT architecture, in which data services provided by the network layer and the application layer in the traditional three-layer architecture can be extracted and form a new layer, namely the service layer (also known as the interface layer or middleware layer). Thus, in an SoA-based IoT architecture, four layers exist and interact with each other [122], these being the perception layer, network layer, service layer, and application layer. It is worth noting that, in some existing efforts, the service layer is divided into two sublayers, namely service composition sublayer and service management sublayer. In addition, the business layer is extracted from the application layer and works as the upper layer of the application layer to provide complex service requests.

In the four-layer SoA-based IoT architecture, the perception layer is performed as the bottom layer of the architecture, and used to measure, collect, and extract the data associated with physical devices [52]. The network layer is used to determine routes and provide data transmission support via integrated heterogeneous networks [10], [47]. The service layer is located between network layer and application layer, providing services to support the application layer [10]. The service layer consists of service discovery, service composition, service management, and service interfaces. Here, service discovery is used to discover desired service requests, service composition is used to interact with the connected objects, and divide or integrate services to meet service requests in an efficient way, service management is used to manage and determine the trust mechanisms to meet service requests, and service interfaces are used to support interactions among all provided services. The application layer is used to support the service requests by users. The application layer can support a number of applications, including smart grid, smart transportation, smart cities, etc.

IV. Enabling Technologies and Challenges in Different Layers

Based on the architectures mentioned above, IoT can be realized with several enabling technologies. In this section, the four-layer SoA-based IoT architecture is taken as an example to present the relevant enabling technologies and challenges in each layer.

A. Perception Layer

In the perception layer, the main function is to identify and track objects. To achieve this function, the following technologies can be implemented.

1) RFID: Generally speaking, RFID, as a noncontact communication technology, is used to identify and track objects without contact. It support data exchange via radio signals over a short distance [8], [162]. The RFID-based system consists of RFID tag, RFID reader, and antenna [62]. RFID tag can be a microchip attached to an antenna. Each RFID tag is attached in an object and has its unique identification number. An RFID reader can identify an object and obtain the corresponding information by querying to the attached RFID tag through appropriate signals [64]. An antenna is used to transmit signals between RFID tag and RFID reader. In comparison with other technologies, RFID has the following benefits [51], [123] (fast scanning, durability, reusability, large storage, noncontact reading, security, small size, low cost, etc.). Because of these benefits, RFID can be useful in the perception layer of IoT to identify and track objects and exchange information.

2) Wireless Sensor Networks: Wireless sensor network (WSN) can play a very important role in IoT [34], [66], [85], [94], [133], [150]. WSN can monitor and track the status of devices, and transmit the status data to the control center or sink nodes via multiple hops [6], [69]. Thus, WSN can be considered as the further bridge between the real world and the cyber world [130]. In comparison with other technologies, WSN has a number of benefits, including scalability, dynamic reconfiguration, reliability, small size, low cost, and low energy consumption. All these benefits help WSN to be integrated in various areas with diverse requirements.

Notice that both RFID and WSN can be used for data acquisition in IoT, and the difference is that RFID is mainly used for object identification, while WSN is mainly used for the perception of real-world physical parameters associated with the surrounding environment [123].

3) Others: Barcode, also denoted 1-D code, stores the information in several black lines and white spacings. These lines and spacings have different widths, organized in a linear or 1-D direction, and are arranged with special encoding rules [49]. The information included in the barcode can be read by a machine that scans the barcode with an infrared beam [93].

A 2-D code records the information by using black and white pixels laid out on the plane, in which black pixel represents a binary of "1" and white pixel represents a binary of "0" [49]. With special encoding rules, the black and white pixels can store a significant amount of information. In comparison with barcode, 2-D code has the benefit of high information content, high reliability, high robustness, etc. [123].

In addition, RFID sensor network (RSN) is an integration of RFID system and sensor network. In an RSN, sensor network can cooperate with RFID system to identify and track the status of objects [138]. In an RSN, small RFID-based sensing devices and RFID reader are implemented, where the RFID reader works as a sink node to generate data and provides power for network operations.

B. Network Layer

The network layer is used to determine routing, and provide data transmission support through integrated heterogeneous networks. In the following, some protocols that can enable the reliable and secure communication in IoT are presented.

1) IEEE 802.15.4: IEEE 802.15.4 is a protocol designed for the physical layer and the MAC layer in wireless personal area networks (WPANs) [7], [37]. The goal of IEEE 802.15.4 is to focus on low-rate WPANs, providing the low rate connections of all things in a personal area with low energy consumption, low rate transmission, and low cost [4]. IEEE 802.15.4 protocol stack is based on open system interconnection model, in which each layer only implements parts of transmission functions, and lower layers can provide service to upper layers. IEEE 802.15.4 can support bands of 868/915M and 2.4 GHz, and the data transmission rate on these bands can achieve 20, 40, and 250 Kb/s, respectively, [7]. IEEE 802.15.4 is a basis for many wireless communication technologies and protocols, such as ZigBee [63], WirelessHART [59], etc.

2) 6LoWPAN: Low-power WPANs (LoWPANs) are organized by a large number of low-cost devices connected via wireless communications [123]. In comparison with other types of networks, LoWPAN has a number of advantages (small packet sizes, low power, low bandwidth, etc.) [123]. As an enhancement, 6LoWPAN protocol was designed by combining IPv6 and LoWPAN. In 6LoWPAN, IPv6 packets can be transmitted over IEEE 802.15.4 networks [98]. Because of the low cost and low energy consumption, 6LoWPAN is suitable to IoT, in which a large number of low cost devices are included. 6LoWPAN have several advantages, including a great connectivity and compatibility with legacy architectures, low-energy consumption, ad-hoc self-organization, etc.

3) ZigBee: ZigBee is a wireless network technology, designed for short-term communication with low-energy consumption [99]. In ZigBee protocol, five layers are included: the physical layer, the MAC layer, the transmission layer, the network layer, and the application layer [123]. The advantages of ZigBee networks include low energy consumption, low cost, low data rate, low complexity, reliability, and security. ZigBee network can support multiple topologies, including star, tree, and mesh topologies [13].

4) Z-Wave: *Z*-wave is a short-term wireless communication technology with the advantages of low cost, low energy consumption, and great reliability [99]. The main objective of *Z*-wave is to provide reliable transmission between a control unit and one or more end-devices, and *Z*-wave is suitable for the network with low bandwidth. Notice that no more than 232 nodes (slaves) can be included in a *Z*-wave network, and all nodes (slaves) would be controlled by the controller and have routing capability [99], [123]. *Z*-wave network supports the dynamic routing technology, and each slave stores a route list in its memory, which is updated by the controller [41].

Although both of ZigBee and *Z*-wave support the short-range wireless communication with low cost and low energy consumption, there are some differences between them. The main difference between ZigBee and *Z*-wave is the frequency band operated in by the physical layer. In ZigBee, the frequency band of the physical layer is normally 2.4 GHz, while the frequency band in *Z*-wave is less than 1 GHz (908.42 $\sim$ 868.42 MHz) [123]. The ZigBee network can support end-devices (slaves) up to 65 000, while the *Z*-wave network can only support 232 end-devices (slaves) [123]. In comparison with ZigBee architecture, *Z*-wave is simple in implementation.

5) Message Queue Telemetry Transport: Using the publish/subscribe technique, message queue telemetry transport (MQTT) is a messaging protocol, which is used to collect measured data on remote sensors and transmit the data to servers [7]. MQTT is a simple and lightweight protocol, and supports the network with low bandwidth and high latency. MQTT can be implemented in various platforms to connect things in IoT into the Internet, and thus MQTT can be used as a messaging protocol between sensors/actuators and servers, making MQTT play an important role in IoT.

6) Constrained Application Protocol: Constrained application protocol (CoAP) is a messaging protocol based on representational state transfer (REST) architecture [7], [17], [38]. Because most of devices in IoT are resources constrained

(i.e., small storage and low computing capability), HTTP cannot be used in IoT, due to its complexity. To overcome the issue, CoAP was proposed to modify some HTTP functions to meet the requirements for IoT. Generally speaking, CoAP is the application layer protocol in the 6LoWPAN protocol stack, and aims to enable resources constrained devices to achieve RESTful interactions. The group communication and push notification are supported by CoAP, but broadcasting is not. Resource observation, block-wise resource transport, resource discovery, interaction with HTTP, and security are all the important features provided by CoAP [7], [38].

7) Extensible Messaging and Presence Protocol: Extensible messaging and presence protocol (XMPP) is an instant messaging protocol based on XML streaming protocols [7], [111]. XMPP inherits features of XML protocol, so that XMPP has great scalability, addressing, and security capabilities, and can be used for multiparty chatting, voice and video streaming, and tele-presence. In XMPP, the following three roles are included: 1) client; 2) server; and 3) gateway, as well as bidirectional communication is supported between two parties of these three roles. Particularly, the server can achieve the functionality of link management and message routing, the gateway is used to support the stable communication among heterogeneous systems, and the client can be connected to the server based on TCP/IP protocol and transmit context based on XML streaming protocol. Thus, XMPP can be used in IoT to support the object to object communication with XML-based text messages.

8) Data Distribution Service: Data distribution service (DDS) is a publish/subscribe protocol for supporting high performance device-to-device communication [7], [44]. DDS was developed by object-manage-group [44] and is a data centric protocol, in which multicasting can be supported to achieve great QoS and high reliability. The broker-less publish/subscribe architecture makes DDS suitable to real-time constrained IoT and device-to-device communications [7]. In addition, DDS can achieve great scalability.

9) Advanced Message Queuing Protocol: Advanced message queuing protocol (AMQP) is an open standard message queuing protocol used to provide message service (queuing, routing, security, reliability, etc.) in the application layer [7], [40]. AMQP focuses on the message-oriented environments and can be considered as a message-oriented middleware protocol. Using AMQP, clients can achieve stable communication with message middlewares, even if these clients and middlewares are produced by different programming languages. In addition, AMQP implements various kinds of message exchange architectures, including store and forward, publish and subscribe, message distribution, message queuing, context-based routing, and point-to-point routing [113].

10) Others: In addition to the transmission protocols, communication protocols, and messaging protocols, other protocols can play important roles in IoT as well. For example, multicast DNS (mDNS) can support the name resolution in IoT applications [7], [55]. DNS service discovery can be used by clients to discover desired services in a special network via mDNS [7], [30]. Routing protocol for low power and lossy networks is a link-independent routing protocol, which can be deployed at resource-constrained nodes to determine routes over low power and lossy links [7], [128], [151]. Although these protocols can be integrated into IoT, enhanced protocols with more security, reliability, and interoperability capabilities are required to advance the development of IoT.

C. Service Layer

As described above, the service layer is located between the network layer and the application layer, and provides efficient and secure services to objects or applications. In the service layer, the following enabling technologies should be included to ensure that the service can be provided efficiently: interface technology, service management technology, middleware technology, and resource management and sharing technology.

1) Interface: The interface technology must be designed in the service layer to ensure the efficient and secure information exchange for communications among devices and applications. In addition, the interface should efficiently manage the interconnected devices, including device connection, device disconnection, device communication, and device operation [136].

To support applications in IoT, an interface profile (IFP) can be considered as a service standard, which can be used to facilitate the interactions among services provided by various devices or applications. To achieve an efficient IFP, universal plug and play should be implemented [36], [45], [136]. As the development of IoT, a number of efforts on the interface have been performed. For instance, SOCRADES integration architecture can be used to provide effective interactions between applications and services [45], [107]. As the development of SoA-IoT, service provisioning process has the functionality of providing interactions with applications and services [136], [166]. Although a number of interface technologies have been developed for IoT, implementing more effective, secure, and scalable interface technologies with low cost remains a great challenge in future research to support IoT.

2) Service Management: Service management can effectively discover the devices and applications, and schedule efficient and reliable services to meet requests. A service can be considered as a behavior, including collection, exchanging, and storage of data, or an association of these behaviors to achieve a special objective [10], [86]. In IoT, some requirements can be met by only one service, while other requirements have to be met by the integration of multiple services. Thus, the service can be divided into two categories in IoT: 1) primary service and 2) secondary service [136]. The primary service, also known as the basic service, can expose the primary functionalities at devices or applications. In contrast, the secondary service can achieve the auxiliary functionalities based on the primary service or other secondary service.

To hide the implementation detail of services and make these services be compatibly implemented in heterogeneous devices and applications, SoA has been used to integrate services. Through this, the reliability and consistence of services can be provided [78], [136]. For example, OSGi platform

established by a dynamic SoA architecture is an effective modular platform to deploy services. To deploy an SoA-based service, the service composition platforms should be developed first, and then the functionalities and communication capabilities of devices should be abstracted. Finally, a common set of services should be provisioned [10], [136]. In SoA-based service, each service offered by a device or application can be considered as a standard service, which can be effectively and easily used in various heterogeneous devices and applications without any change. In this way, requirements in SoA-based IoT can be satisfied more quick and efficient [136].

3) Middleware: Middleware is a software or service programming that can provide an abstraction interposed between IoT technologies and applications [46], [153]. In middleware, the details of different technologies are hidden, and the standard interfaces are provided to enable developers to focus on the development of applications without considering the compatibility between applications and infrastructures [10]. Thus, by using middleware, devices and applications with different interfaces can exchange information and share resources with each other.

Middleware has the following benefits [10]: 1) middleware can support various applications; 2) middleware can run on various operating systems and platforms; 3) middleware can support the distributed computing and the interaction of services among heterogeneous networks, devices, and applications; 4) middleware can support standard protocols; and 5) middleware can provide standard interfaces, providing portability and standard protocols to enable interoperability, and making middleware play an important role in standardization [25]. Middleware can also provide a stable high-level interface for applications. With stable interfaces, applications can work independently on hardware and operating system. This feature makes middleware suitable for IoT, because a large number of heterogeneous devices and networks are integrated, and these devices and networks would be changed or updated often.

A number of research efforts on middleware have been developed, and can be divided into five categories [25], [102], including: 1) message-oriented middleware; 2) semantic Web-based middleware; 3) location-based service and surveillance middleware; 4) communication middleware; and 5) pervasive middleware. Particularly, message-oriented middleware can provide the reliable information exchange among various platforms, and communication protocols (e.g., AMQP, DDS, MQTT, and XMPP) [7], [25]. Semantic Web-based middleware can provide the interactions and interoperability among various sensor networks. Examples of this category includes the SoA-based middleware [118], task computing-based middleware [43], etc. Location-based service and surveillance middleware integrates the locations of devices and other information to provide integrated value services [109]. Communication middleware can provide reliable communications among heterogeneous devices and applications. In communication middleware, RFID-based middleware (Fosstrak [2], etc.), sensor network-based middleware (TinyREST [81], etc.) and the supervisory control and data acquisition are typical examples. Pervasive middleware is designed for the pervasive computing environment, and provides services on multiple and heterogeneous platforms [92].

To integrate middleware into IoT, the following challenges need to be addressed [25].

1) *Interoperability challenge* is to connect heterogeneous devices in communication and information exchange.
2) *Scalability challenge* is to be effectively operated in either small-scale environment or large-scale environment that could involve a massive number of objects.
3) *Abstraction provision challenge* is to provide abstractions at various levels.
4) *Spontaneous interaction challenge* is to provide the reliable service for spontaneous events.
5) *Infixed infrastructure challenge* is to provide reliable services without requesting a fixed infrastructure.
6) *Multiplicity challenge* is to support simultaneously communication among devices and to select or schedule the most suitable services for devices from a massive set of services.

The middleware for IoT should achieve trust, security, and privacy.

4) Resource Management and Sharing: Various heterogeneous networks are integrated to provide data delivery for all applications in IoT (smart transportation, smart grid, etc.). To reduce the cost, some applications can share part of the network resources to increase its utilization. In this case, ensuring that information requested by various applications is delivered on time is a challenging issue in IoT. Existing resource sharing mechanisms primarily focus on the spectrum sharing, which is used to efficiently coordinate multiple networks in the same frequency to maximize the utilization of network resources [77], [126], [164]. The spectrum sharing can be divided into three dimensions, including time, frequency, and space. While most of the existing schemes were developed for machine-to-machine or device-to-device communications, IoT focuses on thing-to-thing networks, in which "thing" not only refers to devices or machines, but also refers to human behaviors, and other objects. Thus, designing an effective resource sharing scheme across heterogeneous networks that is suitable for IoT environment is a significant challenge for future development.

In addition, raw data in IoT are collected by smart devices (RFID, sensors, etc.), and most of these smart devices are resource-constrained and cannot harvest energy from environment. Thus, an energy saving scheme should be considered in resource management [108]. There have been a number of efforts on energy conservation and energy management in sensor networks, including schemes to enhance the life of sensors via harvesting energy from distributed energy resources [21], schemes to reduce the energy of sensors via duty-cycle scheme [97], energy-based routing protocols to balance the energy consumption and to increase the life of the sensor network [150], [151], etc. Although these efforts can work well on energy saving and management, a scheme that is suitable for IoT network infrastructures comprised of heterogeneous networks is an unresolved challenge for future research as well.

V. Security and Privacy

In this section, the security features of IoT are presented first. Then, the security and privacy issues, and possible solutions are discussed in detail.

A. Security Features of IoT

1) Confidentiality: Confidentiality can ensure that the data is only available to authorized users throughout the process, and cannot be eavesdropped or interfered by nonauthorized users. In IoT, confidentiality is an important security principle, because a large number of measurement devices (RFID, sensors, etc.) can integrated in IoT. Thus, it is critical to ensure that the data collected by a measurement device will not reveal secure information to its neighboring devices. To achieve great confidentiality, enhanced techniques, including secure key management mechanisms, and others should be developed and used [22].

2) Integrity: Integrity can ensure that the data cannot be tampered by intended or un-intended interference during the data delivery in communication networks, ultimately providing the accurate data for authorized users. Integrity is important for IoT, because if IoT applications receive forged data or tampered data, erroneous operation status can be estimated and wrong feedback commands can be made, which could further disrupt the operation of IoT applications. To achieve acceptable integrity, enhanced secure data integrity mechanisms (false data filtering schemes, etc.) should be developed and applied [143].

3) Availability: Availability can ensure that the data and devices are available for authorized users and services whenever the data and devices are requested. In IoT, services are commonly requested in real-time fashion, and services cannot be scheduled and provided if the requested data cannot be delivered in a timely manner. Thus, availability is also an important security principle. One of the most serious threats to availability is the denial-of-service (DoS) attack, and enhanced techniques (secure and efficient routing protocols, etc.) should be studied and applied to ensure availability in IoT [82].

4) Identification and Authentication: Identification can ensure that nonauthorized devices or applications cannot be connected to IoT, and authentication can ensure that the data delivered in networks are legitimate, and the devices or applications that request the data are legitimate as well. In IoT, identifying and authenticating each data and object is difficult, because a large number of diverse objects comprise an IoT. Thus, designing efficient mechanisms to deal with the authentication of objects or things is critical in IoT [32].

5) Privacy: Privacy can ensure that the data can only be controlled by the corresponding user, and that no other user can access or process the data. Unlike confidentiality, which aims to encrypt the data without being eavesdropped and interfered by nonauthorized users, privacy ensures that the user can only have some specific controls based on received data and cannot infer other valuable information from the received data [20], [106], [144], [159]. Privacy is considered as one of important security principles due to a large number of devices, services, and people sharing the same communication network in IoT.

6) Trust: Trust can ensure the aforementioned security and privacy objectives to be achieved during the interactions among different objects, different IoT layers, and different applications. The objectives of trust in IoT can be divided as trust between each IoT layer, trust between devices, and trust between devices and applications [8]. With trust, security, and privacy can be enforced. Trust management systems should be designed to implement these trust objectives in IoT.

B. Security

In this section, security challenges in each layer of IoT architecture are presented in detail. In SoA-based IoT, the service layer is established via extracting the functionality of data services in the network layer and the application layer. Thus, security challenges in the service layer can be attributed to challenges in the network and the application layers. In the following, only security challenges in the perception layer, the network layer, and the application layer are presented.

1) Perception Layer: As the main purpose of the perception layer in IoT is to collect data, the security challenges in this layer focus on forging collected data and destroying perception devices, which are presented below.

a) Node capture attacks: In a node capture attack, the adversary can capture and control the node or device in IoT via physically replacing the entire node, or tampering with the hardware of the node or device [162]. If a node is compromised by the node capture attack, the important information (group communication key, radio key, matching key, etc.) can be exposed to the adversary. The adversary can also copy the important information associated with the captured node to a malicious node, and then fake the malicious node as an authorized node to connect to the IoT network or system. This attack is denoted as the node replication attack. A node capture attack can incur a serious impact on the network. To defend against the node capture attack, effective schemes to monitor and detect malicious nodes need to be studied [15].

b) Malicious code injection attacks: In addition to the node capture attack, the adversary can control a node or a device in IoT by injecting malicious code into the memory of the node or device, which is denoted as the malicious code injection attack [142]. The injected malicious code not only can perform specific functions, but can also grant the adversary access into the IoT system, and even gain the full control of the IoT system. To defend against the malicious code injection attack, effective code authentication schemes need to be designed and integrated into IoT [114], [142].

c) False data injection attacks: With the captured node or device in IoT, the adversary can inject false data in place of normal data measured by the captured node or device, and transmit the false data to IoT applications [143]. After receiving the false data, IoT applications can return erroneous feedback commands or provide wrong services, which further affects the effectiveness of IoT applications and networks. To defend against such a malicious attack, techniques (false data filtering schemes, etc.), which can efficiently detect and

drop the false data before the data is received by the IoT applications, need to be designed [71], [72].

d) Replay attacks (or freshness attacks): In IoT, the adversary can use a malicious node or device to transmit to the destination host with legitimate identification information, which has been received by the destination host, in order to make the malicious node or device obtain the trust of IoT [89], [162]. Replay attack is commonly launched in authentication process to destroy the validity of certification. To mitigate the replay attack, techniques (secure time stamp schemes, etc.) should be designed and developed in IoT [31].

e) Cryptanalysis attacks and side channel attacks: A cryptanalysis attack can use the obtained ciphertext or plaintext to infer the encryption key being used in the encryption algorithm [157]. Nonetheless, the efficiency of cryptanalysis attack is low. To improve the efficiency, new attacks, namely the side channel attacks, can be introduced by the adversary. For example, in the side channel attack investigated in IoT [137], the adversary could deploy some techniques on the encryption devices in IoT to obtain the encryption key, which is used in IoT for encrypting data and decrypting data. One of the typical side channel attacks is the timing attack, in which the adversary can obtain the encryption key by analyzing the time information required to execute the encryption algorithm. To mitigate the side channel attack, efficient and secure encryption algorithms and key management schemes need to be developed in IoT [22].

f) Eavesdropping and interference: Because most of devices in IoT will communicate via wireless networks, vulnerability lies in the fact that information delivered in wireless links can be eavesdropped by nonauthorized users [42], [163]. To deal with eavesdropping, secure encryption algorithms and key management schemes are required. The adversary can also send noise data or signal to interfere with the information delivered in wireless links. To ensure the accuracy and timely delivery of data, effective secure noise filtering schemes are required to filter the noise data and restore original data [90].

g) Sleep deprivation attacks: In IoT, most devices or nodes have low power ability. To extend the life cycle of the devices and nodes, devices or nodes are programmed to follow a sleep routine to reduce the power consumption [8], [112]. Nonetheless, the sleep deprivation attack can break the programmed sleep routines and keep device or nodes awake all the time until they are shut down. To extend the life cycle of these devices and nodes, the energy harvest scheme can be one possible solution, in which devices and nodes can harvest energy from the external environment (solar, etc. [21]). In addition, other techniques, like secured duty-cycle mechanism to mitigate the sleep deprivation attack, need to be studied in IoT.

2) Network Layer: As the main purpose of the network layer in IoT is to transmit collected data, the security challenges in this layer focus on the impact of the availability of network resources. Also, most devices in IoT are connected into IoT networks via wireless communication links. Thus, most security challenges in this layer are related to wireless networks in IoT.

a) DoS attacks: DoS attacks can consume all of the available resources in IoT by attacking network protocols or bombarding the IoT network with massive traffic, rendering the services of IoT systems unavailable [83]. The DoS attack is considered to be one of the most common attacks, and represents an attack category, which can result in the services of IoT systems being unavailable. Thus, DoS attacks can be generated by attack schemes, including Ping of Death, TearDrop, UDP flood, SYN flood, Land Attack, etc. To defend against DoS attacks, attacking schemes need to be carefully investigated first, and then the efficient defensive schemes to mitigate attacks need be developed to secure IoT systems [82].

b) Spoofing attacks: The purpose of spoofing attacks is for the adversary to gain full access to the IoT system, and send malicious data into the system [8]. In IoT, examples of spoofing attacks include IP spoofing [91], RFID spoofing [88], etc. In an IP spoofing attack, the adversary can spoof and record the valid IP address of other authorized devices in the IoT, and then access the IoT system to send malicious data with the obtained valid IP address, making malicious data appear to be valid. In an RFID spoofing attack, the adversary can spoof and record the information of a valid RFID tag, and then send malicious data with this valid tag ID to the IoT system. Secure trust management, identification and authentication can be possible solutions to defend against the spoofing attack [28], [32].

c) Sinkhole attacks: In a sinkhole attack, a compromised device or node claims exceptional capabilities of power, computation, and communication, such that more neighboring devices or nodes will select the compromised device or node as the forwarding node in data routing process because of the appealing capabilities [117]. By doing this, the compromised device or node can increase the amount of data obtained before its delivered in the IoT system. Notice that a sinkhole attack not only can break the confidentiality of delivered data, but also can be a fundamental step to launch additional attacks (DoS attack, etc.). To defend against the sinkhole attack, techniques such as secure multiple routing protocols need to be studied and applied [57].

d) Wormhole attacks: Wormhole attack can be launched by two cooperative malicious devices or nodes in IoT, in which the two malicious devices in different locations can exchange routing information with private links to achieve a false one-hop transmission between them, even if they are located far away from each other [67]. In a wormhole attack, because the forwarding hops are reduced, more data will be delivered through these two malicious devices or nodes. With access to more delivered data, the wormhole attack can lead to the similar damage as sinkhole attack. To defend against wormhole attack, there are some possible defensive techniques. One technique is to modify the routing protocols to enhance the security in the route selection process [26], while other techniques involve deploying secure hardware (GPS, directed antenna, etc.).

e) Man in the middle attack: In a man in the middle attack, a malicious device controlled by the adversary can be virtually located between two communicating devices in IoT [96]. By stealing the identify information of the

two normal devices, the malicious device can be a middle device to store and forward all data, which is communicated between these two normal devices, while the two normal devices cannot detect the existence of the malicious device, and instead believe that they directly communicate with each other. The man in the middle attack can violate the confidentiality, integrity, and privacy of restricted data in IoT through monitoring, eavesdropping, tampering, and controlling the communication between the two normal devices. Unlike malicious node capture attacks that need to physically tamper with the hardware of devices, the man in middle attack can be launched by only relying on the communication protocols used in IoT networks. Secure communication protocols and key management schemes, which can ensure the identify and key information of normal devices not be leaked to the adversary, can be efficient defense techniques to protect against the attack [22], [82].

f) Routing information attacks: Routing information attacks focus on the routing protocols in IoT systems, in which the routing information can be manipulated and resent by the adversary to create route loops in the data transmission of the network, leading to the extension of source paths and the increase of end-to-end delay in IoT networks [8]. To defend against the routing information attack, secure routing protocols and trust management to establish secure links among devices in IoT and ensure the identifying information and IP addresses not to be leaked to the adversary are possible techniques to be used.

g) Sybil attacks: In a sybil attack, a malicious device, namely a sybil device, can claim several legitimate identities and impersonate them in IoT systems [8], [95], [158]. Because a sybil device has several legitimate identities, false data sent by the sybil device can be easily accepted by their benign neighboring devices. Also, routes that select sybil devices as forwarding nodes may consider that several different intersected paths are determined, but, in fact only one path is determined and all transmitted data needs to go through the sybil device, in which jamming and DoS can be used. To defend against sybil attacks, secure identification and authentication mechanisms need to be developed for IoT systems [32].

h) Unauthorized access: RFID is an important enabling technology in IoT. Nonetheless, as a large number of RFID-based devices are integrated in IoT, and most of the RFID tags lack proper authentication mechanisms, RFID tags can be accessed and the information stored in tags can be obtained, modified, and deleted by the adversary [8], [60]. Thus, authorization access and authentication mechanisms for RFID-based devices in IoT is a challenge in need of further development [56].

3) Application Layer: The main purpose of the application layer is to support services requested by users. Thus, challenges in the application layer focus on the software attacks. Here, several possible challenges in the application layer of IoT are presented below.

a) Phishing attack: In phishing attacks, the adversary can obtain the confidential data of users, such as identification and passwords, by spoofing the authentication credentials of users via the infected e-mails and phishing websites [8], [54]. Secure authorization access, and identification and authentication can mitigate phishing attacks [8]. Nonetheless, the most efficient way is for users themselves to always be vigilant while surfing online. This becomes an issue as most of devices in IoT are machines, which may lack of such intelligence.

b) Malicious virus/worm: A malicious virus/worm is another challenges to IoT applications [8], [127], [154]. The adversary can infect the IoT applications with malicious self-propagation attacks (worms, Trojan Horse, etc.), and then obtain or tamper with confidential data. Reliable firewall, virus detection, and other defensive mechanisms need to be deployed to combat malicious virus/worm attacks in IoT applications [110].

c) Malicious scripts: Malicious scripts represent the scripts that are added to software, modified in software, and deleted from software with the purpose of harming the system functions of IoT [8]. Because all IoT applications are connected to the Internet, the adversary can easily fool the customers in running malicious scripts (java attack applets, active-x scripts, etc.) when requesting services through the Internet. Malicious scripts can pose the leakage of confidential data and even a complete system shut down. To defend against malicious scripts, effective script detection techniques, including honeypot techniques, static code detection, and dynamic action detection, need to be deployed in IoT systems.

C. Privacy

In general, all of the massive data collected and used in IoT should go through the following three steps: 1) data collection; 2) data aggregation [129]; and 3) data mining and analytics [125], [165]. Particularly, data collection is enacted to sense and collect the status data of objects in IoT, data aggregation integrates an amount of related data into a comprehensive information, and data mining and analytics extract the potential value of integrated comprehensive information for special applications in IoT [125]. Although data collection, data aggregation, and data mining and analytics can provide a number of services to our daily lives, the privacy issues of the data in these steps are raised in IoT as well. Privacy, as a new challenge in IoT, can lead to property loss, and even compromise human safety [106], [144]. For example, in the smart grid, if the adversary obtains the private data of the energy consumption of customers, he or she can infer the time when users are in the home or out of home, and conduct theft or other damage to users with a probability. Thus, privacy-preserving mechanisms need to be developed to ensure private data not to be leaked to the adversary in IoT.

Based on different data processing steps, privacy-preserving mechanisms can be divided into three categories: 1) privacy preservation in data collection [65]; 2) privacy preservation in data aggregation; and 3) privacy preservation in data mining and analytics [20], [134]. As the privacy in data collection, data mining, and data analytics can be greatly preserved by various techniques (encryption, key management, etc.), a majority of the existing efforts on privacy preservation in IoT focus on data privacy in data aggregation.

In data aggregation, the relevant data could be processed in several different locations, and thus it is difficult to achieve privacy preservation through traditional encryption mechanisms. Thus, several privacy-preserving mechanisms have been developed that focused on data aggregation, and can be divided into the following categories: 1) anonymity-based privacy preservation [104]; 2) encryption-based privacy preservation [39]; and 3) perturbation-based privacy preservation [48], [100], [101]. Particularly, in anonymity-based privacy preservation, several related anonymity techniques (K-anonymity, L-diversity, T-closeness, etc.) were used in the data aggregation process to preserve the privacy of identification information [105]. In addition, traffic analysis techniques could affect anonymous communication systems [75], [76], [148]. In encryption-based privacy preservation, several encryption techniques (homomorphic encryption, commitment mechanism, secret sharing, zero-knowledge proof, etc.) were used in the data aggregation to ensure data not to be eavesdropped by adversaries [39]. Nonetheless, existing encryption techniques can only achieve the confidentiality on data transmission and may not work well on privacy preservation. In perturbation-based privacy preservation, perturbation-based techniques (data customization, data sharing, random noise injection, etc.) were used in data aggregation to perturb raw data, achieving privacy preservation [48], however, the utilization of data could hinder the application of this technique in the IoT.

Due to the great performance by directly operating on raw data, perturbation-based privacy preserving schemes are highly popular techniques used in IoT. Nonetheless, most of perturbation-based privacy preserving achieves great performance via reducing the utility of the data. With low utility, data may not, or may only partially, support services requested by IoT applications. Thus, the design of privacy preserving schemes with great data utility remains great challenges on data privacy preservation in IoT for future research.

VI. Integration of IoT and Fog/Edge Computing

In this section, we present how to integrate IoT with fog/edge computing.

A. Overview

The information generated by the things requires big data to collect and process all of the information that is produced and gathered, and turn it into something that is useful. Big data requires the support of IoT because of the challenges of massive sensing and actuating data supported by IoT (smart grid, smart transportation, etc.). In addition, the data collected in IoT applications are generally unstructured data, and need further analysis to extract useful information. The IoT and big data can work well with each other. One real-world example is United Parcel Service (UPS), which is one of the largest shipping companies in the world [79]. UPS deploys sensors to collect data (which is the IoT application) and conduct the big-data analysis to reduce cost and improve delivery efficiency. The sensors are deployed on the delivery vehicles and collect the tracking the information (mileage, speed, fuel cost, etc.).

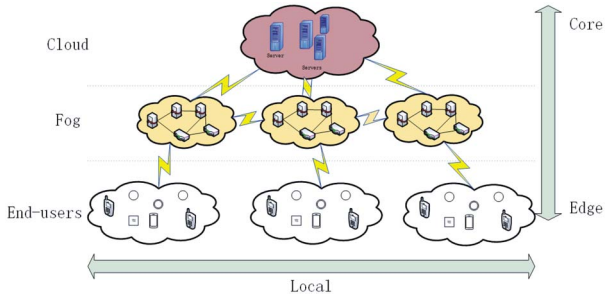

Fig. 2. Fog/edge computing.

As IoT is becoming the next technology revolution, it will affect big data in aspects of data storage, data processing, and analytics. In IoT, continuous streams of data will affect the data storage capacity in various organizations. Additional data centers will be needed to deal with the load of data collected from IoT applications. One possible solution is to move the data to the cloud by leveraging the platform as a service. When an organization selects a technology for performing big data processing and analytics, the nature of the IoT data needs to be considered. Hadoop and Hive can be used to handle big data. Nonetheless, for data collected by IoT application, NoSQL document databases (the Apache CouchDB, etc.) may be suitable [33]. This is because the NoSQL document databases can provide high throughput and low latency. In addition, Apache Kafka is one IoT tool for intermediate message brokering It can be used for the real-time stream processing. The security of big data will also be affected by IoT [156].

B. Fog/Edge Computing-Based IoT

Cloud computing is now a mature technology used to provide computing services or data storage over the Internet, and most of the big IT companies (Amazon, IBM, Google, etc.) are hosting cloud services. Cloud computing provides the benefits of flexibility, efficiency, and ability to store and use data. Nonetheless, when cloud computing is used in IoT, new challenges will appear. In many IoT/CPS applications, data from a massive number of things and objects spanning a large geographical area need to be stored, processed, and analyzed efficiently. To fulfill the gap, fog/edge computing is able to extend cloud computing to be closer to the things it supports [120]. Instead of doing all the computation in the center of the cloud, fog/edge computing can provide computing and storage service to devices (nodes) at the edge of the network.

A fog/edge computing node can be any network device with the capability of storage, computing, and network connectivity (routers, switches, video surveillance cameras, servers, etc.), as shown in Fig. 2. These devices can be deployed at any place with a network connection, and collect the data from IoT devices associated with IoT applications. Different types of IoT data can be directed to the proper place for further analysis based on performance requirements. The high priority data that needs to be addressed immediately can be processed on fog/edge computing nodes, which are the closest to the IoT devices that generate the data. The low priority data, which is

not delay-sensitive, can be directed to some aggregation nodes for further processing and analysis.

In addition to the benefits that fog/edge computing can contribute, there are some challenges to integrate fog/edge computing with IoT. One possible challenge is how to efficiently manage fog/edge computing infrastructure and allocate available resources to IoT devices. At each time, a large number of services can be requested by IoT devices, and each fog/edge service node only has limited computing and storage capability. In this case, all fog/edge nodes should be optimally managed and allocated for IoT devices (or a set of IoT devices in a cluster) to provide requested services efficiently. Another challenge is how to efficiently manage fog/edge computing resources. While the previous challenge focuses on the interface between fog/edge nodes and IoT services, this challenge focuses on the resource management among fog/edge nodes.

When fog/edge nodes are allocated to provide services, different requirements need to be considered, including service availability, energy consumption, and even revenue. Thus, how to optically map the fog/edge service nodes to IoT devices to meet requirements of IoT applications remains a compelling issue. In addition, security and privacy issues (authentication, access control, intrusion detection, trust management, etc.) in fog/edge computing infrastructures that integrate with IoT remain also challenging [27], [29], [35], [152]. The security and privacy issues can be mitigated by countermeasure technologies mentioned in Section V, and thus the challenges in resource allocation are discussed below. The challenges on resources allocation in fog/edge computing-based IoT can be divided as resources allocation between end-devices and fog/edge node and resources allocation among fog/edge nodes.

1) Resource Allocation Between End-Devices and Fog/Edge Node: Because computing and storing resources are limited in a fog/edge node, it is difficult to totally satisfy all services requested by end-users simultaneously. To address this issue, each end-users may have a satisfaction function to assess the allocated resources to provide its requested service. The satisfaction function can be represented by

$$S(r) = \begin{cases} \log(r+1), & 0 \leqslant r < r_{\min} \\ \log(r_{\max}+1), & r \geqslant r_{\min} \end{cases} \tag{1}$$

where S is the satisfaction function, r is the allocated resources, and $r_{\max}$ is the maximum resource, which is required to provide the requested service.

With this satisfaction function, the main objective of fog/edge node is to maximize the overall satisfaction of all end-users, which can be represented as

$$\textbf{Objective}.\ \max\{S_{\text{overall}}\} \tag{2}$$

$$\textbf{S.t.} \quad \begin{cases} S_{\text{overall}} = \sum_{i=1}^{n}\{p_i \cdot S_i(r_i)\} \\ r_1 + r_2 + \cdots + r_n \leqslant R \\ p_1 + p_2 + \cdots + p_n = 1 \\ r_1, r_2, \ldots, r_n \geqslant 0 \end{cases} \tag{3}$$

where S_{overall} is the overall satisfaction of all end-users, R is the resource that a fog/edge node has, r_i is the resource allocated for end-users i, and p_i is the priority level for end-user i. Based on (2) and (3), a fog/edge node can allocate its resources to all end-device while achieving maximum overall satisfaction.

In a fog/edge computing-based IoT, a number of fog/edge nodes are connected, if a fog/edge node does not have enough resources to provide the requested services from nearby end-users while its neighboring nodes have spare resources, the fog/edge node can move some local data to its neighboring nodes to be processed and stored data. By doing this, services for its local end-users can be provided. This is related to the resource allocation among fog/edge nodes, which will be described below.

2) Resource Allocation Among Fog/Edge Nodes: As the distributed architecture of fog/edge computing-based IoT, all fog/edge nodes can be connected with each other via the network connections and share their computing and storing resources to provide service for end-users. In this scenario, if a fog/edge node does not have enough resource to provide local requested services, the fog/edge node can move some requested services with low priority level to be processed in its neighboring fog/edge nodes, which have spare resources. The spare resources of a fog/edge node can be represented as

$$R^f_{\text{spare}} = R^f - \sum_{i=1}^{n} r_i^{\max} \tag{4}$$

where, R^f is the resource that fog/edge node f has, and $r_i^{\max}$ is the maximum resource needed by end-user i. Thus, if R^f_{spare} is less than "0," fog/edge node f does have enough resource and needs assist from neighboring nodes, and the fog/edge node can be denoted as resource-poor node. Otherwise, fog/edge node f has spare resource to help other fog/edge nodes, and the node can be denoted as resource-rich node in the fog/edge computing infrastructure.

In the resource allocation among fog/edge nodes, a resource-poor fog/edge node may not care about which resource-node helps it to provide computing services, and a resource-rich node does not care about data from which that it processes. The only one all fog/edge nodes care about is to achieve the minimum cost (minimum delay, etc.) in the overall fog/edge computing infrastructure. By taking the objective of the minimum delay as an example, we have

$$\textbf{Objective}.\ \min\left(\text{Cost}_{\text{all}} = \frac{1}{2} \cdot \sum_{L_{fg} \in L} \left(\left|R^{fg}_{\text{spare}}\right| \cdot \text{Cost}_{fg}\right)\right)$$

$$\textbf{S.t.} \quad \begin{cases} \forall f \in N_S, & \sum_{i \in N_f} R^{fi}_{\text{spare}} \leq R^f_{\text{spare}} \\ \forall g \in N_g, & \sum_{j \in N_g} R^{jg}_{\text{spare}} = R^g_{\text{spare}} \\ \forall L_{fg} \in L, & R^{fg}_{\text{spare}} = -R^{gf}_{\text{spare}} \\ \forall L_{fg} \in L, & \left|R^{fg}_{\text{spare}}\right| \leq \text{Constraints}_{fg} \end{cases} \tag{5}$$

where Cost_{all} is the total cost, Cost_{fg} is the cost of delivering data on link L_{fg} between fog/edge node f and g, N_f is the set of neighboring nodes of fog/edge node f, R^{jg}_{spare} is the data

moved from fog/edge node j to node g, and Constraints_{jg} is the constraints of link L_{fg} (bandwidth, etc.). Based on this formalization, resource allocation among fog/edge nodes with the minimum cost in fog/edge computing infrastructure can be realized.

VII. Applications

In the following, several applications, including the smart grid, smart transportation, and smart cities, are presented to demonstrate how fog/edge computing-based IoT to be implemented in real-world applications.

A. Smart Grid

In integrating IoT and CPS, the smart grid has been developed to replace traditional power grid to provide reliable and efficient energy service to consumers [1]. In the smart gird, distributed energy generators are introduced to improve the utilization of distributed energy resources and electric vehicles are introduced to improve the capability of energy storage and reduce emission of CO_2, and smart meters and bidirectional communication networks are introduced to achieve the interactions between customers and utility providers. With these techniques, the smart grid can achieve great reliability, efficiency, safety, and interactivity [71], [72].

By integrating with IoT, a large number of smart meters can be deployed in houses and buildings connected in smart grid communication networks [74]. Smart meters can monitor energy generation, storage, and consumption, and can interact with utility providers to report energy demand information of customers and receive real-time electricity pricing for customers [71], [160]. With the aid of fog/edge computing infrastructure, the large amount of data collected from smart meters can be stored and processed so that the effective operations of the smart grid can be supported. With the interaction information, utility providers can optimize the energy dispatch of the grid, and customers can optimize their energy consumption, resulting in the improvement of resource utilization and the reduction of cost.

Lastly, because a large number of smart meters are deployed in the smart grid, and communicate with each other via wireless communication links and processed in fog/edge computing infrastructure, adversaries can easily capture these smart meters, nodes in fog/edge computing infrastructure, and obtain or modify the data collected [72], [142]. The confidentiality and privacy of energy consumption information can be available to adversaries. With the modified data, utility providers may incorrectly estimate the energy supply and demand of the gird, and can feedback erroneous energy dispatch decisions, leading to imbalance on energy supply and demand in the grid and even posing large-scale outages [72]. In addition, key function components in the smart grid can be disrupted. Examples include state estimation [139], [141], energy routing [70], [72], energy price [71], [145], [161], optimal power flow [140], etc. Thus, efficient security mechanisms that can preserve data privacy and integrity in the data collection and transmission processes need to be developed for the smart grid [146], [149].

B. Smart Transportation

Smart transportation, also known as intelligent transportation systems, is another typical IoT-CPS-based application, in which intelligent transportation management, control system, communication networks, and computing techniques are integrated to make transportation systems reliable, efficient, and secure [73]. In the smart transportation system, a large number of smart vehicles are included and connected with each other through wireless networks [58], [61]. Smart vehicles can efficiently perceive and share traffic data and schedule drivers' travels with great efficiency, reliability, and safety. In the recent past, smart vehicles (Google's Self-Driving car, etc.) have been designed and tested. Those smart vehicles can detect objects around them and safely manage speed during traveling without the operation of drivers [3].

In the smart transportation system, each smart vehicle is deployed with a number of electronic control units (ECUs) to monitor and control subsystems in the vehicles. These ECUs are organized as an internal network to share the collected data within the vehicle [121]. In addition, each smart vehicle is deployed with communication interfaces to connect to the outside network. With these communication interfaces, vehicles can carry out vehicle-to-vehicle communication and vehicle-to-infrastructure communication [58]. In this way, all vehicles can be connected into the smart transportation system, namely the vehicular network, and exchange and share massive data of current traffic status, and ultimately offer the most efficient and secure travels to customers. The massive collected data can be further stored and processed in the fog/edge computing infrastructure, enabling efficient service to drivers and system operators.

Because all the traffic status data are shared by vehicular networks, the adversary may intrude into the system and control ECUs in vehicles by launching malicious attacks against vehicle networks and fog/edge computing nodes in the fog/edge computing-based IoT infrastructure, sharing misleading traffic status data with other vehicles via communication interfaces deployed in the compromised vehicle [12], [140]. In this case, the confidentiality, integrity, and privacy of traffic status data can be compromised by the adversary, and serious damage to the transportation system can be caused (the increase number of congested roads, increase time spent to complete travels, etc.). Thus, in order to deploy an efficient and secure smart transportation system, techniques that can support services in the aforementioned eight main categories and related security issues need be carefully investigated in future research.

C. Smart Cities

Smart cities can be considered a complex IoT paradigm, which aims to manage public affairs via introducing information and communication technology (ICT) solutions [155]. Smart cities can use public resources in more efficient ways, resulting in the improvement of the QoSs provided to users and the reduction of operational costs to public administrators [53], [155]. For instance, one practical implementation of smart cities, namely *Padova Smart City*, has been realized in

the city of Padova in Italy, which can select open data and ICT solutions for public administrators as early as possible to achieve the best use of public resources [19], [24].

Smart cities, as a complex CPS/IoT application, may consist of several subapplications or services [84], [155], including the smart gird, smart transportation, the structural health of buildings, waste management, environmental monitoring, smart health, smart lighting, etc. All these subapplications, or services, should be supported by a unified communication network infrastructure, or communication networks designed for these subapplications or services should be interconnected to establish a large-scale interconnected heterogenous network for IoT/CPS applications, with the aim of achieving the best use of public resources in cities. To enable effective smart cities, all enabling technologies discussed in Section IV and security and privacy issues discussed in Section V should be carefully investigated and integrated. In addition, the fog/edge computing-based IoT can enable efficient subapplications and services in smart cities.

VIII. Conclusion

In this paper, a comprehensive review of IoT has been presented, including architectures, enabling technologies, and security and privacy issues, as well as the integration of fog/edge computing and IoT to support diverse applications. Particularly, the relationship and difference between IoT and CPS has been clarified at the outset. Possible architectures for IoT have been discussed, including the traditional three-layer architecture and the SoA-based four-layer architecture. Based on the SoA-based IoT architecture, enabling technologies in layers (perception layer, network layer, and service layer) have been detailed, respectively. In addition, to secure IoT, potential security and privacy issues that could affect the effectiveness of IoT, and their potential solutions, have been presented. To investigate the fog/edge computing-based IoT, the relationship between IoT and fog/edge computing and related issues have been discussed. Furthermore, several applications, including the smart grid, smart transportation, and smart cities, are presented to show how fog/edge computing-based IoT to be implemented in real-world applications. The main purpose of this survey is to provide a clear, comprehensive, and deep understanding of IoT and its integration with fog/edge computing, outlining the breadth of topics that IoT entails, and highlighting areas that remain unresolved, in an effort to further promote the development of IoT.

References

[1] *NIST & The Smart Grid*. Accessed on Sep. 21, 2016. [Online]. Available: http://www.nist.gov/smartgrid/nistandsmartgrid.cfm

[2] *Fosstrak: Open Source RFID Software Platform*. [Online]. Available: https://fosstrak.github.io/

[3] *Google Self-Driving Car*. [Online]. Available: http://www.google.com/selfdrivingcar/how/

[4] *IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture*, IEEE Standard 802-2001, pp. 1–48, Feb. 2002.

[5] S. H. Ahmed, G. Kim, and D. Kim, "Cyber physical system: Architecture, applications and research challenges," in *Proc. IFIP Wireless Days (WD)*, Valencia, Spain, Nov. 2013, pp. 1–5.

[6] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

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

[8] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, "Internet of Things: Security vulnerabilities and challenges," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Larnaca, Cyprus, Jul. 2015, pp. 180–187.

[9] A. P. Athreya and P. Tague, "Network self-organization in the Internet of Things," in *Proc. IEEE Int. Conf. Sens. Commun. Netw. (SECON)*, Jun. 2013, pp. 25–33.

[10] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.

[11] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social Internet of Things (SIoT)—When social networks meet the Internet of Things: Concept, architecture and network characterization," *Comput. Netw.*, vol. 56, no. 16, pp. 3594–3608, Nov. 2012.

[12] S. Azadegan, W. Yu, H. Liu, A. Sistani, and S. Acharya, "Novel anti-forensics approaches for smart phones," in *Proc. 45th Hawaii Int. Conf. Syst. Sci. (HICSS)*, 2012, pp. 5424–5431.

[13] P. Baronti *et al.*, "Wireless sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards," *Comput. Commun.*, vol. 30, no. 7, pp. 1655–1695, May 2007.

[14] J. Bélissent, "Getting clever about smart cities: New opportunities require new business models," Forrester Res., Cambridge, MA, USA, Tech. Rep., Nov. 2010. [Online]. Available: https://www.forrester.com/report/Getting+Clever+About+Smart+Cities+New+Opportunities+Require+New+Business+Models/-/E-RES56701?aid=AST127312

[15] M. V. Bharathi, R. C. Tanguturi, C. Jayakumar, and K. Selvamani, "Node capture attack in wireless sensor network: A survey," in *Proc. IEEE Int. Conf. Comput. Intell. Comput. Res. (ICCIC)*, Coimbatore, India, Dec. 2012, pp. 1–3.

[16] F. Bonomi, R. A. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," in *Proc. 1st Edition MCC Workshop Mobile Cloud Comput.*, Helsinki, Finland, Aug. 2012, pp. 13–16.

[17] C. Bormann, A. P. Castellani, and Z. Shelby, "CoAP: An application protocol for billions of tiny Internet nodes," *IEEE Internet Comput.*, vol. 16, no. 2, pp. 62–67, Mar./Apr. 2012.

[18] A. Botta, W. de Donato, V. Persico, and A. Pescapé, "On the integration of cloud computing and Internet of Things," in *Proc. Int. Conf. Future Internet Things Cloud (FiCloud)*, Barcelona, Spain, Aug. 2014, pp. 23–30.

[19] N. Bressan *et al.*, "The deployment of a smart monitoring system using wireless sensor and actuator networks," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm)*, Gaithersburg, MD, USA, Oct. 2010, pp. 49–54.

[20] Z. Cai, Z. He, X. Guan, and Y. Li, "Collective data-sanitization for preventing sensitive information inference attacks in social networks," *IEEE Trans. Depend. Secure Comput.*, to be published, doi: 10.1109/TDSC.2016.2613521.

[21] A. Cammarano, C. Petrioli, and D. Spenza, "Pro-energy: A novel energy prediction model for solar and wind energy-harvesting wireless sensor networks," in *Proc. IEEE 9th Int. Conf. Mobile Ad-Hoc Sensor Syst. (MASS)*, Las Vegas, NV, USA, Oct. 2012, pp. 75–83.

[22] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-organized public-key management for mobile ad hoc networks," *IEEE Trans. Mobile Comput.*, vol. 2, no. 1, pp. 52–64, Jan./Mar. 2003.

[23] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. Workshops*, Beijing, China, Jun. 2008, pp. 495–500.

[24] P. Casari *et al.*, "The 'wireless sensor networks for city-wide ambient intelligence (WISE-WAI)' project," *Sensors*, vol. 9, no. 6, pp. 4056–4082, May 2009.

[25] M. A. Chaqfeh and N. Mohamed, "Challenges in middleware solutions for the Internet of Things," in *Proc. Int. Conf. Collaboration Technol. Syst. (CTS)*, Denver, CO, USA, May 2012, pp. 21–26.

[26] U. K. Chaurasia and V. Singh, "MAODV: Modified wormhole detection AODV protocol," in *Proc. 6th Int. Conf. Contemp. Comput. (IC3)*, Noida, India, Aug. 2013, pp. 239–243.

[27] F. Chen, T. Xiang, X. Fu, and W. Yu, "User differentiated verifiable file search on the cloud," *IEEE Trans. Services Comput.*, to be published, doi: 10.1109/TSC.2016.2589245.

[28] I.-R. Chen, J. Guo, and F. Bao, "Trust management for service composition in SOA-based IoT systems," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, Istanbul, Turkey, Apr. 2014, pp. 3444–3449.

[29] Z. Chen *et al.*, "A cloud computing based network monitoring and threat detection system for critical infrastructures," *Big Data Res.*, vol. 3, pp. 10–23, Apr. 2016.

[30] S. Cheshire, "DNS-based service discovery," INTERNET-DRAFT draft-cheshire-dnsext-dns-sd-04.txt, 2011.

[31] C.-H. Cho, K.-H. Do, J.-W. Kim, and M.-S. Jun, "Design of RFID mutual authentication protocol using time stamp," in *Proc. 4th Int. Conf. Comput. Sci. Convergence Inf. Technol. (ICCIT)*, Seoul, South Korea, Nov. 2009, pp. 1047–1051.

[32] M.-C. Chuang and J.-F. Lee, "TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks," *IEEE Syst. J.*, vol. 8, no. 3, pp. 749–758, Sep. 2014.

[33] C. Doukas and F. Antonelli, "COMPOSE: Building smart & context-aware mobile applications utilizing IoT technologies," in *Proc. 5th IEEE Glob. Inf. Infrastruct. Netw. Symp.*, Trento, Italy, Oct. 2013, pp. 1–6.

[34] X. Du, Y. Xiao, M. Guizani, and H.-H. Chen, "An effective key management scheme for heterogeneous sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 24–34, 2007.

[35] X. Fu, Z. Ling, W. Yu, and J. Luo, "Cyber crime scene investigations (C2SI) through cloud computing," in *Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst. Workshops (ICDCSW)*, Genoa, Italy, 2010, pp. 26–31.

[36] K. Gama, L. Touseau, and D. Donsez, "Combining heterogeneous service technologies for building an Internet of Things middleware," *Comput. Commun.*, vol. 35, no. 4, pp. 405–417, Feb. 2012.

[37] G. Gan, Z. Lu, and J. Jiang, "Internet of Things security analysis," in *Proc. Int. Conf. Internet Technol. Appl. (iTAP)*, Wuhan, China, Aug. 2011, pp. 1–4.

[38] W. Gao, J. Nguyen, W. Yu, C. Lu, and D. Ku, "Assessing performance of constrained application protocol (CoAP) in MANET using emulation," in *Proc. ACM Int. Conf. Rel. Convergent Syst. (RACS)*, Odense, Denmark, 2016, pp. 103–108.

[39] J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation for reverse multicast traffic in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, vol. 5. Seoul, South Korea, May 2005, pp. 3044–3049.

[40] R. Godfrey, D. Ingham, and R. Schloming, OASIS Advanced Message Queuing Protocol (AMQP) Version 1.0; OASIS Standard," Oct. 2012.

[41] C. Gomez and J. Paradells, "Wireless home automation networks: A survey of architectures and technologies," *IEEE Commun. Mag.*, vol. 48, no. 6, pp. 92–101, Jun. 2010.

[42] G. Gomez, F. J. Lopez-Martinez, D. Morales-Jimenez, and M. R. McKay, "On the equivalence between interference and eavesdropping in wireless communications," *IEEE Trans. Veh. Technol.*, vol. 64, no. 12, pp. 5935–5940, Dec. 2015.

[43] A. Gómez-Goiri and D. López-de Ipiña, "A triple space-based semantic distributed middleware for Internet of Things," in *Proc. Int. Conf. Web Eng.*, Vienna, Austria, Jul. 2010, pp. 447–458.

[44] *Data Distribution Service (DDS)*, *Version 1.2*, Object Manag. Group, Nov. 2016.

[45] D. Guinard, V. Trifa, S. Karnouskos, P. Spiess, and D. Savio, "Interacting with the SOA-based Internet of Things: Discovery, query, selection, and on-demand provisioning of Web services," *IEEE Trans. Services Comput.*, vol. 3, no. 3, pp. 223–235, Jul./Sep. 2010.

[46] S. Hadim and N. Mohamed, "Middleware: Middleware challenges and approaches for wireless sensor networks," *IEEE Distrib. Syst. Online*, vol. 7, no. 3, p. 1, Mar. 2006.

[47] C. Han, J. M. Jornet, E. Fadel, and I. F. Akyildiz, "A cross-layer communication module for the Internet of Things," *Comput. Netw.*, vol. 57, no. 3, pp. 622–633, Feb. 2013.

[48] W. He, X. Liu, H. Nguyen, K. Nahrstedt, and T. Abdelzaher, "PDA: Privacy-preserving data aggregation in wireless sensor networks," in *Proc. 26th IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Anchorage, AK, USA, May 2007, pp. 2045–2053.

[49] X. He, "The two-dimensional bar code application in book management," in *Proc. Int. Conf. Web Inf. Syst. Min. (WISM)*, vol. 1. Sanya, China, Oct. 2010, pp. 409–411.

[50] R. G. Helps and S. J. Pack, "Cyber-physical system concepts for IT students," in *Proc. 14th Annu. ACM SIGITE Conf. Inf. Technol. Educ. (SIGITE)*, Orlando, FL, USA, Oct. 2013, pp. 7–12.

[51] D. Ćika, M. Draganić, and Z. Šipuš, "Active wireless sensor with radio frequency identification chip," in *Proc. 35th Int. Conv.*, Opatija, Croatia, May 2012, pp. 727–732.

[52] E. Ilie-Zudor, Z. Kemény, F. van Blommestein, L. Monostori, and A. van der Meulen, "Survey paper: A survey of applications and requirements of unique identification systems and RFID techniques," *Comput. Ind. Eng.*, vol. 62, no. 3, pp. 227–252, Apr. 2011.

[53] A. Laya, V.-I. Bratu, and J. Markendahl, "Who is investing in machine-to-machine communications?" in *Proc. 24th Eur. Regional Conf. Int. Telecommun. Soc.*, Florence, Italy, Oct. 2013, pp. 1–21.

[54] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Commun. ACM*, vol. 50, no. 10, pp. 94–100, Oct. 2007.

[55] A. J. Jara, P. Martinez-Julia, and A. Skarmeta, "Light-weight multicast DNS and DNS-SD (lmDNS-SD): IPv6-based resource and service discovery for the Web of Things," in *Proc. 6th Int. Conf. Innov. Mobile Internet Services Ubiquitous Comput. (IMIS)*, Palermo, Italy, Jul. 2012, pp. 731–738.

[56] B.-Z. Jing *et al.*, "RFID access authorization by face recognition," in *Proc. Int. Conf. Mach. Learn. Cybern.*, vol. 1. Jul. 2009, pp. 302–307.

[57] G. Kalnoor and J. Agarkhed, "QoS based multipath routing for intrusion detection of sinkhole attack in wireless sensor networks," in *Proc. Int. Conf. Circuit Power Comput. Technol. (ICCPCT)*, Mar. 2016, pp. 1–6.

[58] M. Khanjary and S. M. Hashemi, "Route guidance systems: Review and classification," in *Proc. 6th Euro Amer. Conf. Telematics Inf. Syst. (EATIS)*, Valencia, Spain, May 2012, pp. 1–7.

[59] A. N. Kim, F. Hekland, S. Petersen, and P. Doyle, "When HART goes wireless: Understanding and implementing the wirelessHART standard," in *Proc. IEEE Int. Conf. Emerg. Technol. Factory Autom.*, Hamburg, Germany, Sep. 2008, pp. 899–907.

[60] D. S. Kim, T.-H. Shin, and J. S. Park, "Access control and authorization for security of RFID multi-domain using SAML and XACML," in *Proc. Int. Conf. Comput. Intell. Security*, vol. 2. Nov. 2006, pp. 1587–1590.

[61] R. Kim, H. Lim, and B. Krishnamachari, "Prefetching-based data dissemination in vehicular cloud systems," *IEEE Trans. Veh. Technol.*, vol. 65, no. 1, pp. 292–306, Jan. 2015.

[62] D. M. K. Finkenzeller, *RFID Handbook: Fundamentals and Applications in Contactless Smart Cards, Radio Frequency Identification and Near-Field Communication*, 3rd ed. Chichester, U.K.: Wiley, Aug. 2010.

[63] W. Kluge *et al.*, "A fully integrated 2.4-GHz IEEE 802.15.4-compliant transceiver for ZigBee^{TM} trade applications," *IEEE J. Solid-State Circuits*, vol. 41, no. 12, pp. 2767–2775, Dec. 2006.

[64] S. Lahiri, *RFID Sourcebook*. Upper Saddle River, NJ, USA: IBM Press, 2005.

[65] N. D. Lane *et al.*, "A survey of mobile phone sensing," *IEEE Commun. Mag.*, vol. 48, no. 9, pp. 140–150, Sep. 2010.

[66] T. N. Le, W. Yu, X. Bai, and D. Xuan, "A dynamic geographic hash table for data-centric storage in sensor networks," in *Proc. IEEE Int. Conf. Comput. Netw. Commun. (WCNC)*, Las Vegas, NV, USA, 2007, pp. 2168–2174.

[67] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Trans. Autom. Control*, vol. 59, no. 12, pp. 3224–3237, Dec. 2014.

[68] M. Leo, F. Battisti, M. Carli, and A. Neri, "A federated architecture approach for Internet of Things security," in *Proc. Euro Med Telco Conf. (EMTC)*, Naples, Italy, Nov. 2014, pp. 1–5.

[69] J. Lin, X. Yang, W. Yu, and X. Fu, "Towards effective en-route filtering against injected false data in wireless sensor networks," in *Proc. IEEE Glob. Telecommun. Conf. (GLOBECOM)*, Houston, TX, USA, Dec. 2011, pp. 1–5.

[70] J. Lin *et al.*, "On distributed energy routing protocols in the smart grid," in *Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing* (Studies in Computational Intelligence), vol. 492, R. Lee, Ed. Heidelberg, Germany: Springer, 2013.

[71] J. Lin, W. Yu, and X. Yang, "Towards multistep electricity prices in smart grid electricity markets," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 1, pp. 286–302, Jan. 2016.

[72] J. Lin, W. Yu, X. Yang, G. Xu, and W. Zhao, "On false data injection attacks against distributed energy routing in smart grid," in *Proc. IEEE/ACM 3rd Int. Conf. Cyber-Phys. Syst. (ICCPS)*, Beijing, China, Apr. 2012, pp. 183–192.

[73] J. Lin *et al.*, "A novel dynamic en-route decision real-time route guidance scheme in intelligent transportation systems," in *Proc. IEEE 35th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Columbus, OH, USA, Jun. 2015, pp. 61–72.

[74] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in smart grids," in *Proc. 2nd IEEE PES Int. Conf. Exhibit. Innov. Smart Grid Technol. (ISGT Europe)*, Manchester, U.K., Dec. 2011, pp. 1–8.

[75] Z. Ling *et al.*, "A new cell counter based attack against tor," in *Proc. 16th ACM Conf. Comput. Commun. Security (CCS)*, Chicago, IL, USA, 2009, pp. 578–589.

[76] Z. Ling *et al.*, "A new cell-counting-based attack against tor," *IEEE/ACM Trans. Netw.*, vol. 20, no. 4, pp. 1245–1261, Aug. 2012.

[77] H. Liu, S. Hua, X. Zhuo, D. Chen, and X. Cheng, "Cooperative spectrum sharing of multiple primary users and multiple secondary users," *Digit. Commun. Netw.*, vol. 2, no. 4, pp. 191–195, 2016.

[78] Y. Liu and G. Zhou, "Key technologies and applications of Internet of Things," in *Proc. 5th Int. Conf. Intell. Comput. Technol. Autom. (ICICTA)*, Zhangjiajie, China, Jan. 2012, pp. 197–200.

[79] S. Lohr, "The age of big data," *New York Times*, Feb. 2012.

[80] P. López, D. Fernández, A. J. Jara, and A. F. Skarmeta, "Survey of Internet of Things technologies for clinical environments," in *Proc. 27th Int. Conf. Adv. Inf. Netw. Appl. Workshops (WAINA)*, Barcelona, Spain, Mar. 2013, pp. 1349–1354.

[81] T. Luckenbach, P. Gober, S. Arbanowski, A. Kotsopoulos, and K. Kim, "Tinyrest-a protocol for integrating sensor networks into the Internet," in *Proc. Real-World Wireless Sensor Netw. (REALWSN)*, Jun. 2005, pp. 101–105.

[82] S. U. Maheswari, N. S. Usha, E. A. M. Anita, and K. R. Devi, "A novel robust routing protocol RAEED to avoid DoS attacks in WSN," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Chennai, India, Feb. 2016, pp. 1–5.

[83] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of Things (IoT) security: Current status, challenges and prospective measures," in *Proc. 10th Int. Conf. Internet Technol. Secured Trans. (ICITST)*, London, U.K., Dec. 2015, pp. 336–341.

[84] S. Mallapuram, N. Ngwum, F. Yuan, C. Lu, and W. Yu, "Smart city: The state of the art, datasets, and evaluation platforms," in *Proc. 16th IEEE/ACIS Int. Conf. Comput. Inf. Sci. (ICIS)*, 2017.

[85] L. D. Mello and L. T. Kubota, "Review of the use of biosensors as analytical tools in the food and drink industries," *Food Chem.*, vol. 77, no. 2, pp. 237–256, 2002.

[86] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012.

[87] M. H. Miraz, M. Ali, P. S. Excell, and R. Picking, "A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of Nano Things (IoNT)," in *Proc. Internet Technol. Appl. (ITA)*, Wrexham, U.K., Sep. 2015, pp. 219–224.

[88] A. Mitrokotsa, M. R. Rieback, and A. S. Tanenbaum, "Classifying RFID attacks and defenses," *Inf. Syst. Front.*, vol. 12, no. 5, pp. 491–505, Nov. 2010.

[89] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Proc. 47th Annu. Allerton Conf. Commun. Control Comput.*, Monticello, IL, USA, Sep./Oct. 2009, pp. 911–918.

[90] J. R. Mohammed, "A new simple adaptive noise cancellation scheme based on ALE and NLMS filter," in *Proc. 5th Annu. Conf. Commun. Netw. Services Res. (CNSR)*, Fredericton, NB, Canada, May 2007, pp. 245–254.

[91] A. Mukaddam, I. Elhajj, A. Kayssi, and A. Chehab, "IP spoofing detection using modified hop count," in *Proc. IEEE 28th Int. Conf. Adv. Inf. Netw. Appl.*, Victoria, BC, Canada, May 2014, pp. 512–516.

[92] A. Mukherjee, D. Saha, and C. Biswas, "Present scenarios and future challenges in pervasive middleware," in *Proc. 1st Int. Conf. Commun. Syst. Software Middleware*, New Delhi, India, Jan. 2006, pp. 1–5.

[93] R. Muniz, L. Junco, and A. Otero, "A robust software barcode reader using the Hough transform," in *Proc. Int. Conf. Inf. Intell. Syst.*, Bethesda, MD, USA, Oct. 1999, pp. 313–319.

[94] J. Nakamura, *Image Sensors and Signal Processing for Digital Still Cameras* (Opt. Sci. Eng.). Boca Raton, FL, USA: CRC Press, Aug. 2005.

[95] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd IEEE Int. Symp. Inf. Process. Sensor Netw.*, Berkeley, CA, USA, Apr. 2004, pp. 259–268.

[96] R. P. Padhy, M. R. Patra, and S. C. Satapathy, "Cloud computing: Security issues and research challenges," *Int. J. Comput. Sci. Inf. Technol. Security*, vol. 1, no. 2, pp. 136–146, Dec. 2011.

[97] M. R. Palattella *et al.*, "On optimal scheduling in duty-cycled industrial IoT applications using IEEE802.15.4e TSCH," *IEEE Sensors J.*, vol. 13, no. 10, pp. 3655–3666, Oct. 2013.

[98] M. R. Palattella *et al.*, "Standardized protocol stack for the Internet of (important) Things," *IEEE Commun. Surveys Tuts.*, vol. 15, no. 3, pp. 1389–1406, 3rd Quart., 2013.

[99] H. B. Pandya and T. A. Champaneria, "Internet of Things: Survey and case studies," in *Proc. Int. Conf. Elect. Electron. Signals Commun. Optim. (EESCO)*, Visakhapatnam, India, Jan. 2015, pp. 1–6.

[100] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "CAP: A context-aware privacy protection system for location-based services," in *Proc. IEEE Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Montreal, QC, Canada, 2009, pp. 49–57.

[101] A. Pingley, W. Yu, N. Zhang, X. Fu, and W. Zhao, "A context-aware scheme for privacy-preserving location-based services," *Comput. Netw.*, vol. 56, no. 11, pp. 2551–2568, 2012.

[102] R. Prodan and S. Ostermann, "A survey and taxonomy of infrastructure as a service and Web hosting cloud providers," in *Proc. 10th IEEE/ACM Int. Conf. Grid Comput.*, Banff, AB, Canada, Oct. 2009, pp. 17–25.

[103] Q. Pu *et al.*, "Low latency geo-distributed data analytic," in *Proc. ACM SIGCOMM*, London, U.K., Aug. 2015, pp. 421–434.

[104] K. P. N. Puttaswamy, R. Bhagwan, and V. N. Padmanabhan, "Anonygator: Privacy and integrity preserving data aggregation," in *Proc. ACM/IFIP/USENIX 11th Int. Conf. Middleware*, Bengaluru, India, 2010, pp. 85–106.

[105] F. Qiu, F. Wu, and G. Chen, "Privacy and quality preserving multimedia data aggregation for participatory sensing systems," *IEEE Trans. Mobile Comput.*, vol. 14, no. 6, pp. 1287–1300, Jun. 2015.

[106] X. Ren, X. Yang, J. Lin, Q. Yang, and W. Yu, "On scaling perturbation based privacy-preserving schemes in smart metering systems," in *Proc. 22nd Int. Conf. Comput. Commun. Netw. (ICCCN)*, Nassau, The Bahamas, Jul. 2013, pp. 1–7.

[107] D. Romero *et al.*, *RESTful Integration of Heterogeneous Devices in Pervasive Environments*. Heidelberg, Germany: Springer, 2010, pp. 1–14.

[108] L. Roselli *et al.*, "Review of the present technologies concurrently contributing to the implementation of the Internet of things (IoT) paradigm: RFID, green electronics, WPT and energy harvesting," in *Proc. IEEE Topical Conf. Wireless Sensors Sensor Netw. (WiSNet)*, San Diego, CA, USA, Jan. 2015, pp. 1–3.

[109] A. Roxin, C. Dumez, N. Cottin, J. Gaber, and M. Wack, "TransportML: A middleware for location-based services collaboration," in *Proc. 3rd Int. Conf. New Technol. Mobility Security*, Cairo, Egypt, Dec. 2009, pp. 1–6.

[110] A. K. Sahoo, A. Das, and M. Tiwary, "Firewall engine based on graphics processing unit," in *Proc. Int. Conf. Adv. Commun. Control Comput. Technol. (ICACCCT)*, May 2014, pp. 758–763.

[111] P. Saint-Andre, "Extensible messaging and presence protocol (XMPP): Core," Internet Eng. Task Force, Fremont, CA, USA, RFC 6121, Mar. 2011.

[112] M. Sarkar and D. B. Roy, "Prevention of sleep deprivation attacks using clustering," in *Proc. 3rd Int. Conf. Electron. Comput. Technol. (ICECT)*, vol. 5. Apr. 2011, pp. 391–394.

[113] S. Schneider, *Understanding the Protocols Behind the Internet of Things*, Electron. Design, Oct. 2013. [Online]. Available: http://electronicdesign.com/iot/understanding-protocols-behind-internet-things

[114] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: Software-based attestation for embedded devices," in *Proc. IEEE Symp. Security Privacy*, Berkeley, CA, USA, May 2004, pp. 272–282.

[115] K. Sha, W. Wei, A. Yang, and W. Shi, "Security in Internet of Things: Opportunities and challenges," in *Proc. Int. Conf. Identification Inf. Knowl. Internet Things*, Oct. 2016, pp. 49–50.

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

[117] V. Soni, P. Modi, and V. Chaudhri, "Detecting sinkhole attack in wireless sensor network," *Int. J. Appl. Innov. Eng. Manag.*, vol. 2, no. 2, pp. 29–32, Feb. 2013.

[118] P. Spiess *et al.*, "Soa-based integration of the Internet of Things in enterprise services," in *Proc. IEEE Int. Conf. Web Services (ICWS)*, Los Angeles, CA, USA, Jul. 2009, pp. 968–975.

[119] J. A. Stankovic, "Research directions for the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 3–9, Feb. 2014.

[120] I. Stojmenovic and S. Wen, "The fog computing paradigm: Scenarios and security issues," in *Proc. Federated Conf. Comput. Sci. Inf. Syst. (FedCSIS)*, Warsaw, Poland, Sep. 2014, pp. 1–8.

[121] I. Studnia *et al.*, "Survey on security threats and protection mechanisms in embedded automotive networks," in *Proc. 43rd Annu. IEEE/IFIP Conf. Depend. Syst. Netw. Workshop (DSN W)*, Budapest, Hungary, Jun. 2013, pp. 1–12.

[122] H. Suo, J. Wan, C. Zou, and J. Liu, "Security in the Internet of Things: A review," in *Proc. Int. Conf. Comput. Sci. Electron. Eng. (ICCSEE)*, vol. 3. Hangzhou, China, Mar. 2012, pp. 648–651.

[123] J. Tan and S. G. M. Koo, "A survey of technologies in Internet of Things," in *Proc. IEEE Int. Conf. Distrib. Comput. Sensor Syst.*, Marina Del Rey, CA, USA, May 2014, pp. 269–274.

[124] L. Tan and N. Wang, "Future Internet: The Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5. Chengdu, China, Aug. 2010, pp. V5-376–V5-380.

[125] C.-W. Tsai, C.-F. Lai, M.-C. Chiang, and L. T. Yang, "Data mining for Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 77–97, 1st Quart., 2014.

[126] S. Wang and C. Wang, "Joint optimization of spectrum and energy efficiency in cognitive radio networks," *Digit. Commun. Netw.*, vol. 1, no. 3, pp. 161–170, 2015.

[127] X. Wang, W. Yu, A. Champion, X. Fu, and D. Xuan, "Detecting worms via mining dynamic program execution," in *Proc. 3rd Int. Conf. Security Privacy Commun. Netw.*, Nice, France, 2007, pp. 412–421.

[128] T. Winter *et al.*, "RPL: Ipv6 routing protocol for low-power and lossy networks," Internet Eng. Task Force, Fremont, CA, USA, RFC 6550, Mar. 2012.

[129] D. Wu, B. Yang, and R. Wang, "Scalable privacy-preserving big data aggregation mechanism," *Digit. Commun. Netw.*, vol. 2, no. 3, pp. 122–129, 2016.

[130] F.-J. Wu, Y.-F. Kao, and Y.-C. Tseng, "Review: From wireless sensor networks towards cyber physical systems," *Pervasive Mobile Comput.*, vol. 7, no. 4, pp. 397–413, Aug. 2011.

[131] J. Wu and W. Zhao, "Design and realization of WInternet: From Net of Things to Internet of Things," *ACM Trans. Cyber Phys. Syst.*, vol. 1, no. 1, Feb. 2017, Art. no. 2.

[132] M. Wu, T.-J. Lu, F.-Y. Ling, J. Sun, and H.-Y. Du, "Research on the architecture of Internet of Things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 5. Chengdu, China, Aug. 2010, pp. V5-484–V5-487.

[133] Y. Xiao *et al.*, "A survey of key management schemes in wireless sensor networks," *J. Comput. Commun.*, vol. 30, nos. 11–12, pp. 2314–2341, 2007.

[134] L. Xu, C. Jiang, J. Wang, J. Yuan, and Y. Ren, "Information security in big data: Privacy and data mining," *IEEE Access*, vol. 2, pp. 1149–1176, Oct. 2014.

[135] L. D. Xu, "Enterprise systems: State-of-the-art and future trends," *IEEE Trans. Ind. Informat.*, vol. 7, no. 4, pp. 630–640, Nov. 2011.

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

[137] B. Yang, K. Wu, and R. Karri, "Scan based side channel attack on dedicated hardware implementations of data encryption standard," in *Proc. Int. Test Conf. (ITC)*, Charlotte, NC, USA, Oct. 2004, pp. 339–344.

[138] H. Yang and S.-H. Yang, "RFID sensor network network architectures to integrate RFID, sensor and WSN," *Meas. Control*, vol. 40, no. 2, pp. 56–59, Mar. 2007.

[139] Q. Yang, L. Chang, and W. Yu, "On false data injection attacks against Kalman filtering in power system dynamic state estimation," *Security Commun. Netw.*, vol. 9, no. 9, pp. 833–849, Jun. 2016.

[140] Q. Yang *et al.*, "On data integrity attacks against optimal power flow in power grid systems," in *Proc. Annu. IEEE Consumer Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, 2017.

[141] Q. Yang *et al.*, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[142] X. Yang *et al.*, "Towards a low-cost remote memory attestation for the smart grid," *Sensors*, vol. 15, no. 8, pp. 20799–20824, Aug. 2015.

[143] X. Yang *et al.*, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Trans. Comput.*, vol. 64, no. 1, pp. 4–18, Jan. 2015.

[144] X. Yang, X. Ren, J. Lin, and W. Yu, "On binary decomposition based privacy-preserving aggregation schemes in real-time monitoring systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 27, no. 10, pp. 2967–2983, Oct. 2016.

[145] X. Yang *et al.*, "Data integrity attacks against the distributed real-time pricing in the smart grid," in *Proc. IEEE Int. Perform. Comput. Commun. Conf. (IPCCC)*, Las Vegas, NV, USA, 2016, pp. 1–8.

[146] X. Yang, P. Zhao, X. Zhang, J. Lin, and W. Yu, "Toward a Gaussian-mixture model-based detection scheme against data integrity attacks in the smart grid," *IEEE Internet Things J.*, vol. 4, no. 1, pp. 147–161, Feb. 2017.

[147] S. Yi, C. Li, and Q. Li, "A survey of fog computing: Concepts, applications and issues," in *Proc. Workshop Mobile Big Data*, Hangzhou, China, Jun. 2015, pp. 37–42.

[148] W. Yu, X. Fu, S. Graham, D. Xuan, and W. Zhao, "DSSS-based flow marking technique for invisible traceback," in *Proc. IEEE Symp. Security Privacy (S P)*, Oakland, CA, USA, 2007, pp. 18–32.

[149] W. Yu, D. Griffith, L. Ge, S. Bhattarai, and N. Golmie, "An integrated detection system against false data injection attacks in the smart grid," *Security Commun. Netw.*, vol. 8, no. 2, pp. 91–109, 2015.

[150] W. Yu, T. N. Le, D. Xuan, and W. Zhao, "Query aggregation for providing efficient data services in sensor networks," in *Proc. IEEE Mobile Ad-Hoc Sensor Syst. (MASS)*, Fort Lauderdale, FL, USA, 2004, pp. 31–40.

[151] W. Yu and J. Lee, "Efficient energy sensitive routing protocols in mobile ad-hoc networks," in *Proc. Int. Conf. Wireless Netw.*, Las Vegas, NV, USA, 2002.

[152] W. Yu, G. Xu, Z. Chen, and P. Moulema, "Cyber crime scene investigations (C2SI) through cloud computing," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, Washington, DC, USA, 2013, pp. 26–31.

[153] W. Yu, D. Xuan, B. Graham, S. Santhanam, R. Bettati, and W. Zhao, "An integrated middleware-based solution for supporting secured dynamic-coalition applications in heterogeneous environments," in *Proc. IEEE Workshop Inf. Assurance Security*, West Point, NY, USA, 2002, pp. 259–264.

[154] W. Yu, N. Zhang, X. Fu, and W. Zhao, "Self-disciplinary worms and countermeasures: Modeling and analysis," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 10, pp. 1501–1514, Oct. 2010.

[155] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of Things for smart cities," *IEEE Internet Things J.*, vol. 1, no. 1, pp. 22–32, Feb. 2014.

[156] A. Zaslavsky, C. Perera, and D. Georgakopoulos, "Sensing as a service and big data," in *Proc. Int. Conf. Adv. Cloud Comput. (ACC)*, Charlotte, NC, USA, Jul. 2012.

[157] J. Zhang, D. Gu, Z. Guo, and L. Zhang, "Differential power cryptanalysis attacks against present implementation," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng. (ICACTE)*, vol. 6. Chengdu, China, Aug. 2010, pp. V6-61–V6-65.

[158] K. Zhang, X. Liang, R. Lu, and X. Shen, "Sybil attacks and their defenses in the Internet of Things," *IEEE Internet Things J.*, vol. 1, no. 5, pp. 372–383, Oct. 2014.

[159] L. Zhang, Z. Cai, and X. Wang, "Fakemask: A novel privacy preserving approach for smartphones," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 2, pp. 335–348, Jun. 2016.

[160] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "Towards efficient and secured real-time pricing in the smart grid," in *Proc. IEEE Glob. Commun. Conf. (GLOBECOM)*, San Diego, CA, USA, Dec. 2015, pp. 1–6.

[161] X. Zhang, X. Yang, J. Lin, G. Xu, and W. Yu, "On data integrity attacks against real-time pricing in energy-based cyber-physical systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 1, pp. 170–187, Jan. 2017.

[162] K. Zhao and L. Ge, "A survey on the Internet of Things security," in *Proc. 9th Int. Conf. Comput. Intell. Security (CIS)*, Dec. 2013, pp. 663–667.

[163] N. Zhao, F. R. Yu, M. Li, and V. C. M. Leung, "Anti-eavesdropping schemes for interference alignment (IA)-based wireless networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 8, pp. 5719–5732, Aug. 2016.

[164] K. Zheng, F. Hu, W. Wang, W. Xiang, and M. Dohler, "Radio resource allocation in LTE-advanced cellular networks with m2m communications," *IEEE Commun. Mag.*, vol. 50, no. 7, pp. 184–192, Jul. 2012.

[165] X. Zheng, Z. Cai, J. Li, and H. Gao, "Location-privacy-aware review publication mechanism for local business service systems," in *Proc. 36th Annu. IEEE Int. Conf. Comput. Commun. (INFOCOM)*, Atlanta, GA, USA, 2017, pp. 1–9.

[166] H. Zhou, *The Internet of Things in the Cloud: A Middleware Perspective*, 1st ed. Boca Raton, FL, USA: CRC Press, Oct. 2012.

Jie Lin received the B.S. and Ph.D. degrees from the Department of Computer Science and Technology, Xi'an Jiaotong University, Xi'an, China, in 2009 and 2013, respectively.

He is currently an Associate Professor with the Department of Computer Science and Technology, Xi'an Jiaotong University. His current research interests include smart grid, cyberspace security, and computer networks.

Wei Yu received the B.S. degree in electrical engineering from the Nanjing University of Technology, Nanjing, China, in 1992, the M.S. degree in electrical engineering from Tongji University, Shanghai, China, in 1995, and the Ph.D. degree in computer engineering from Texas A&M University, College Station, TX, USA, in 2008.

He was with Cisco Systems Inc., San Jose, CA, USA, for nine years. He is currently an Associate Professor with the Department of Computer and Information Sciences, Towson University, Towson, MD, USA. His current research interests include cyberspace security and privacy, computer networks, cyber-physical systems, and distributed computing.

Dr. Yu was a recipient of the 2014 NSF CAREER Award, the 2015 University System of Maryland (USM) Regents' Faculty Award for Excellence in Scholarship, Research, or Creative Activity, the USM's Wilson H. Elkins Professorship Award in 2016, and the Best Paper Awards from IEEE ICC 2008, ICC 2013, and IEEE IPCCC 2016.

Nan Zhang received the B.S. degree in computer science from Peking University, Beijing, China, in 2001, and the Ph.D. degree in computer science from Texas A&M University, College Station, TX, USA, in 2006.

He is an Associate Professor of Computer Science with the George Washington University, Washington, DC, USA. His current research interests include databases, data analytics, and information privacy/security.

Dr. Zhang was a recipient of several awards including the NSF CAREER Award in 2008, the Best Paper Award of IEEE ICC 2013 and IEEE NAS 2010, the Best Student Paper Award of ACM CIKM 2013, the Best Paper Nomination from IEEE ISI 2015, and the GW Technology Transfer Innovation Price and the First Place finish at the GW Business Plan Competition, both in 2012.

Xinyu Yang received the B.S., M.S., Ph.D. degrees, and Diploma degree in computer science and technology from Xi'an Jiaotong University, Xi'an, China, in 1995, 1997, 2001, and 2001, respectively.

He is currently a Professor with the Department of Computer Science and Technology, Xi'an Jiaotong University. His current research interests include wireless communication, mobile ad hoc networks, and network security.

Hanlin Zhang received the B.S. degree in software engineering from Qingdao University, Qingdao, China, in 2010, and the M.S. degree in applied information technology and Doctoral degree in information technology from Towson University, Towson, MD, USA, in 2011 and 2016, respectively.

He is currently an Assistant Professor with the Department of Computer Science, Qingdao University. His current research interests include information security, cloud security, mobile security, and network security.

Wei Zhao received the undergraduate program in physics degree from Shaanxi Normal University, Xi'an, China, in 1977, and the M.S. and Ph.D. degrees in computer and information sciences from the University of Massachusetts Amherst, Amherst, MA, USA, in 1983 and 1986, respectively.

He was the Dean of the School of Science, Rensselaer Polytechnic Institute, Troy, NY, USA. He is currently the Rector with the University of Macau, Macau, China. From 2005 to 2006, he was the Director for the Division of Computer and Network Systems, U.S. National Science Foundation, Arlington, TX, USA, when he was on leave from Texas A&M University, College Station, TX, USA, where he was a Senior Associate Vice President for Research and a Professor of Computer Science. He was the Founding Director of the Texas A&M Center for Information Security and Assurance, which has been recognized as a Center of Academic Excellence in Information Assurance Education by the National Security Agency. Since then, he has been a Faculty Member with Amherst College, Amherst, MA, USA, the University of Adelaide, Adelaide SA, Australia, and Texas A&M University. His current research interests include distributed computing, real-time systems, computer networks, and cyber space security.