Internet of Things in Industries: A Survey

Article *in* IEEE Transactions on Industrial Informatics · November 2014

DOI: 10.1109/TII.2014.2300753

3 authors, including:

Wu He
Old Dominion University
95 PUBLICATIONS **965** CITATIONS
SEE PROFILE

Shancang Li
University of the West of England, Bristol
41 PUBLICATIONS **710** CITATIONS
SEE PROFILE

Internet of Things in Industries: A Survey

Li Da Xu, *Senior Member*, *IEEE*, Wu He, and Shancang Li

***Abstract*—Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years. In an effort to understand the development of IoT in industries, this paper reviews the current research of IoT, key enabling technologies, major IoT applications in industries, and identifies research trends and challenges. A main contribution of this review paper is that it summarizes the current state-of-the-art IoT in industries systematically.**

***Index Terms*—Big data analytics, enterprise systems, information and communications technology (ICT), industrial informatics, internet of things (IoT), near field communications, radio-frequency identification (RFID), wireless sensor networks (WSNs).**

I. Introduction

AS AN EMERGING technology, the Internet of Things (IoT) is expected to offer promising solutions to transform the operation and role of many existing industrial systems such as transportation systems and manufacturing systems. For example, when IoT is used for creating intelligent transportation systems, the transportation authority will be able to track each vehicle's existing location, monitor its movement, and predict its future location and possible road traffic. The term IoT was initially proposed to refer to uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology [1]. Later on, researchers relate IoT with more technologies such as sensors, actuators, GPS devices, and mobile devices. Today, a commonly accepted definition for IoT is

> a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'Things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network [2].

Manuscript received October 01, 2013; revised November 26, 2013 and January 04, 2014; accepted January 08, 2014. Date of publication January 16, 2014; date of current version November 04, 2014. This work was supported in part by the National Natural Science Foundation of China (NNSFC) under Grant 71132008, and in part by the U.S. National Science Foundation under Grant SES-1318470 and Grant 1044845. Paper no. TII-13-0753.

L. D. Xu is with the Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100190, China; Shanghai Jiao Tong University, Shanghai 200052, China; the University of Science and Technology of China, Hefei 230026, China; and also with Old Dominion University, Norfolk, VA 23529 USA (e-mail: lxu@odu.edu).

W. He is with Old Dominion University, Norfolk, VA 23529 USA (e-mail: whe@odu.edu).

S. Li is with the Faculty of Engineering, University of Bristol, Bristol BS8 1TH, U.K. (e-mail: shancang.li@bristol.ac.uk).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TII.2014.2300753

Specifically, the integration of sensors/actuators, RFID tags, and communication technologies serves as the foundation of IoT and explains how a variety of physical objects and devices around us can be associated to the Internet and allow these objects and devices to cooperate and communicate with one another to reach common goals [3].

There is a growing interest in using IoT technologies in various industries [4]. A number of industrial IoT projects have been conducted in areas such as agriculture, food processing industry, environmental monitoring, security surveillance, and others. Meanwhile, the number of IoT publications is quickly growing. The authors conducted an extensive literature review by examining relevant articles from five major academic databases (IEEE Xplore, Web of Knowledge, ACM digital library, INSPEC, and ScienceDirect) in order to help interested researchers understand the current status and future research opportunities regarding the use of IoT in industries. Our review focuses on both identifying the breadth and diversity of existing IoT research in the industrial areas and highlighting the challenges and opportunities for future researchers. As a result, we found a large number of journal articles and conference papers related to IoT. For example, we found 306 IoT-related journal articles published from 2009 to 2013 by searching the Web of Knowledge database alone. Fig. 1 displays the number of journal articles stored in the Web of Knowledge database by year from 2009 to 2013. Fig. 1 indicates a trend that research on IoT is becoming increasingly popular.

This paper is organized as follows. Section II presents the background and current research of IoT. Section III provides an in-depth review of service-oriented architecture (SOA) of IoT. Section IV reviews the key enabling technologies that make IoT possible. Section V describes key IoT applications in industries. Section VI discusses research challenges and future trends. Conclusion is given in Section VII.

II. Background and Current Research of IoT

IoT can be considered as a global network infrastructure composed of numerous connected devices that rely on sensory, communication, networking, and information processing technologies [5]. A foundational technology for IoT is the RFID technology, which allows microchips to transmit the identification information to a reader through wireless communication. By using RFID readers, people can identify, track, and monitor any objects attached with RFID tags automatically [6]. RFID has been widely used in logistics, pharmaceutical production, retailing, and supply chain management, since 1980s [7], [8]. Another foundational technology for IoT is the wireless sensor networks (WSNs), which mainly use interconnected intelligent sensors to sense and monitoring. Its applications include environmental monitoring, healthcare monitoring, industrial monitoring, traffic monitoring, and so on [9], [10]. The advances in both RFID and WSN significantly

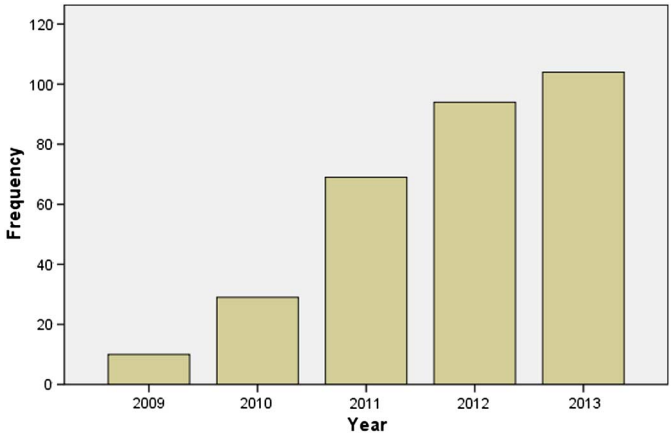


Fig. 1. Number of IoT Journal articles by year in Web of Knowledge.

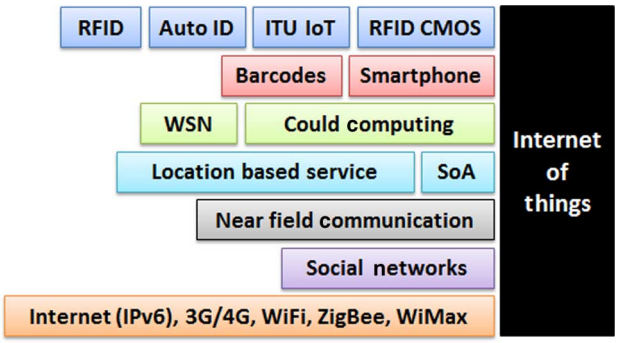


Fig. 2. Technologies associated with IoT.

contribute to the development of IoT. In addition, many other technologies and devices such as barcodes, smart phones, social networks, and cloud computing are being used to form an extensive network for supporting IoT [11]–[16] (see Fig. 2).

So far, IoT has been gaining attraction in industry such as logistics, manufacturing, retailing, and pharmaceutics. With the advances in wireless communication, smartphone, and sensor network technologies, more and more networked things or smart objects are being involved in IoT. As a result, these IoT-related technologies have also made a large impact on new information and communications technology (ICT) and enterprise systems technologies (see Fig. 3).

In order to provide high-quality services to end users, IoT's technical standards need to be designed to define the specification for information exchange, processing, and communications between things. The success of IoT depends on standardization, which provides interoperability, compatibility, reliability, and effective operations on a global scale [17]. Many countries and organizations are interested in the development of IoT standards because it can bring tremendous economic benefits in the future. Currently, numerous organizations such as International Telecommunication Union, International Electro-technical Commission, International Organization for Standardization, IEEE, European Committee for Electro-technical Standardization, China Electronics Standardization Institute, and American National Standards Institute are working on the development of various IoT standards [18], [19]. As so many organizations are involved in the development of IoT standards, a strong coordination

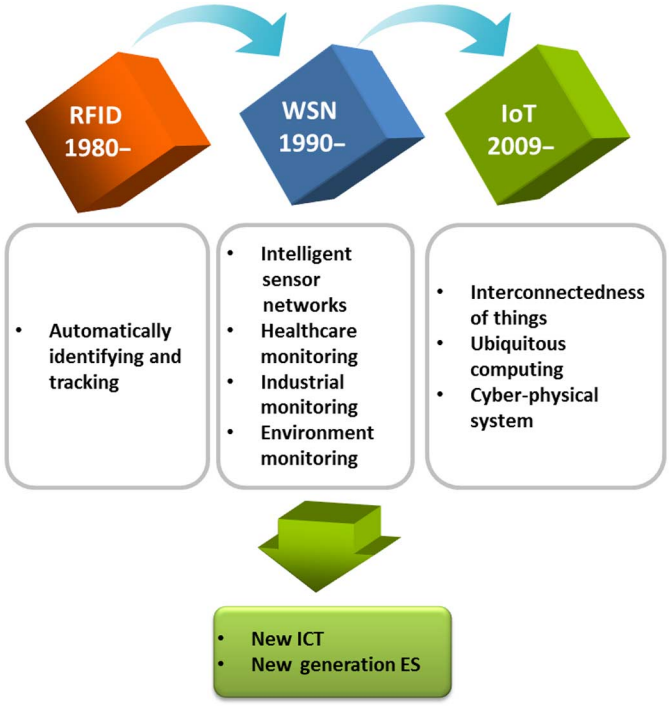


Fig. 3. IoT-related technology and their impact on new ICT and enterprise systems.

between different standardization organizations is necessary to coordinate and govern the relationships between international standards organizations and national/regional standards organizations [20]. By establishing widely accepted standards, developers and users can implement IoT applications and services that would be deployed and used on a large scale, while saving the development and maintenance cost in the long run. The standardization of the technologies in IoT will also accelerate the wide spread of IoT technology and innovations.

So far, many countries have significantly invested on IoT initiatives. The U.K. government has launched a £5 m project to develop IoT. In Europe Union, the IoT European Research Cluster (IERC) FP7 (http://www.rfid-in-action.eu/cerp/) has proposed a number of IoT projects and created an international IoT forum to develop a joint strategic and technical vision for the use of IoT in Europe [21], [22]. China takes IoT seriously and plans to invest $800 million in the IoT industry by 2015. China aims to take a leading role in setting international standards for IoT technologies [23]. In the U.S., IBM and ITIF (The Information Technology and Innovation Foundation) reported, in 2009, that IoT can be an effective way to improve traditional physical and information technology infrastructure, and will have a greater positive impact on productivity and innovation. Japan launched u-Japan and i-Japan strategies, respectively, in 2008 and 2009, in order to use IoT to support daily lives [24].

III. SOA for IoT

IoT aims to connect different things over the networks. As a key technology in integrating heterogeneous systems or devices, SOA can be applied to support IoT. SOA has been successfully used in research areas such as cloud computing, WSNs, and

TABLE I
A FOUR-LAYERED ARCHITECTURE FOR IOT

Layers	Description
Sensing layer	This layer is integrated with existing hardware (RFID, sensors, actuators, etc.) to sense/control the physical world and acquire data
Networking layer	This layer provides basic networking support and data transfer over wireless or wired network
Service layer	This layer creates and manages services. It provides services to satisfy user needs
Interface layer	This layer provides interaction methods to users and other applications

TABLE II
DESIGN CONSIDERATIONS FOR INDUSTRIAL IOT APPLICATIONS (ADAPTED FROM [48])

Design goals	Description
Energy	How long can an IoT device operate with limited power supply?
Latency	How much time is need for message propagation and processing?
Throughput	What is the maximum amount of data that can be transported through the network?
Scalability	How many devices are supported?
Topology	Who must communicate with whom?
Security and safety	How secure and safe is the application?

vehicular network [25]–[32]. Quite a few ideas have been proposed to create multi-layer SOA architectures for IoT based on the selected technology, business needs, and technical requirements. For example, the International Telecommunication Union recommends that IoT architecture consists of five different layers: sensing, accessing, networking, middleware, and application layers. Jia *et al.* [6] and Domingo [33] propose to divide the IoT system architecture into three major layers: perception layer, network layer, and service layer (or application layer). Atzori *et al.* [19] developed a three-layered architectural model for IoT which consists of the application layer, the network layer, and the sensing layer. Liu *et al.* [34] designed an IoT application infrastructure that contains physical layer, transport layer, middleware layer, and applications layer. From the perspective of functionalities, a four-layered SOA of IoT is shown in Table I. Table II shows design considerations for industrial IoT applications. Fig. 4 shows an SOA, where the four layers interact to each other.

The architectural design of IoT is concerned with architecture styles, networking and communication, smart objects, Web services and applications, business models and corresponding process, cooperative data processing, security, etc. From the technology perspective, the design of an IoT architecture needs to consider extensibility, scalability, modularity, and interoperability among heterogeneous devices. As things might move or need real-time interaction with their environment, an adaptive architecture is needed to help devices dynamically interact with other things. The decentralized and heterogeneous nature of IoT requires that the architecture provides IoT efficient event-driven capability. Thus, SOA is considered a good approach to achieve interoperability between heterogeneous devices in a multitude of way [19], [20], [32].

A. Sensing Layer

IoT can be considered as a world-wide physical inner-connected network, in which things can be connected and controlled remotely. As more and more devices are equipped with RFID or intelligent sensors, connecting things becomes much easier [35]. In the sensing layer, the wireless smart systems with tags or sensors are now able to automatically sense and exchange information among different devices. These technology advances significantly improve the capability of IoT to sense and identify things or environment. In some industry sectors, intelligent service deployment schemes and a universal unique identifier (UUID) are assigned to each service or device that may be needed. A device with UUID can be easily identified and retrieved. Thus, UUIDs are critical for successful services deployment in a huge network like IoT [35], [36].

B. Networking Layer

The role of networking layer is to connect all things together and allow things to share the information with other connected things. In addition, the networking layer is capable of aggregating information from existing IT infrastructures (e.g., business systems, transportation systems, power grids, healthcare systems, ICT systems, etc.). In SOA-IoT, services provided by things are typically deployed in a heterogeneous network and all related things are brought into the service Internet [19], [37]. This process might involve QoS management and control according to the requirements of users/applications. On the other hand, it is essential for a dynamically changing network to automatically discover and map things in a network. Things need to be automatically assigned with roles to deploy, manage, and schedule the behaviours of things and be able to switch to any other roles at any time as needed. These capabilities enable devices to be able to collaboratively perform tasks. To design the networking layer in IoT, designers need to address issues such as network management technologies for heterogonous networks (such as fixed, wireless, mobile, etc.), energy efficiency in networks, QoS requirements, service discovery and retrieval, data and signal processing, security, and privacy [38].

C. Service Layer

Service layer relies on the middleware technology that provides functionalities to seamlessly integrate services and applications in IoT. The middleware technology provides the IoT with a cost-efficient platform, where the hardware and software platforms can be reused. A main activity in the service layer involves the service specifications for middleware, which are being developed by various organizations. A well-designed service layer will be able to identify common application requirements

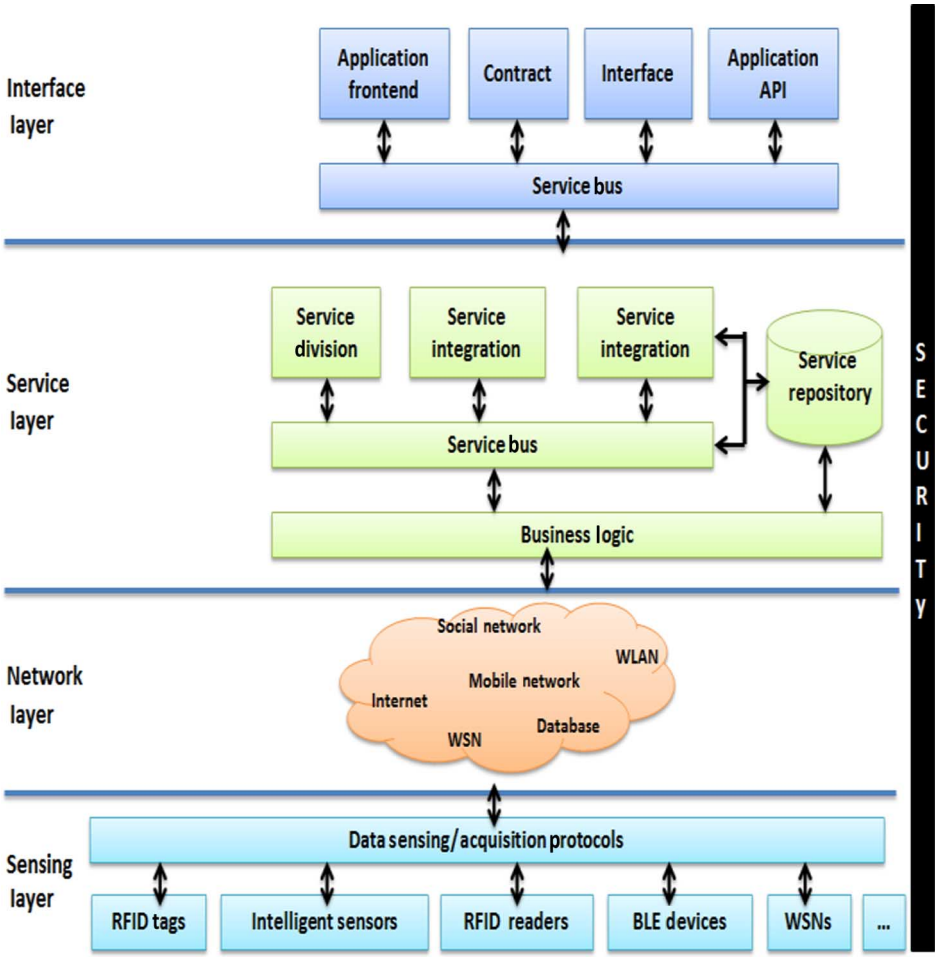


Fig. 4. SOA for IoT.

and provide APIs and protocols to support required services, applications, and user needs. This layer also processes all service-oriented issues, including information exchange and storage, data management, search engines, and communication [19], [20], [38]. This layer includes the following components.

1) Service discovery: finding objects that can offer the needed services and information in an efficient way [19].
2) Service composition: enabling the interaction and communication among connected things. The discovery phase leverage the relationships among different things to discover the desired service, and the service composition component is to schedule or re-create more suitable services in order to acquire the most reliable services to meet the request [19], [20].
3) Trustworthiness management: aiming at determining trust and reputation mechanisms that can evaluate and use the information provided by other services to create a trustworthy system [19], [37], [38].
4) Service APIs: supporting the interactions between services required in IoT [24], [38].

D. Interface Layer

In IoT, a large number of devices involved are made by different manufacturers/vendors and they do not always follow the same standards/protocols. As a result of the heterogeneity, there are many interaction problems with information exchange, communication between things, and cooperative event processing among different things. Furthermore, the constant increase of things participating in an IoT makes it harder to dynamically connect, communicate, disconnect, and operate. There is also a necessity for an interface layer to simplify the management and interconnection of things. An interface profile (IFP) can be seen as a subset of service standards that support interaction with applications deployed on the network. A good interface profile is related to the implementation of Universal Plug and Play (UPnP), which defines a protocol for facilitating interaction with services provided by various things [38], [39]. The interface profiles are used to describe the specifications between applications and services. The services on the service layer run directly on limited network infrastructures in order to effectively find new services for an application, as they connect to the network. Recently, a SOCRADES integration architecture (SIA) has been proposed to effectively interact between applications and services [38], [40]. Traditionally, the service layer provides universal API for applications. However, the recent research results on SOA-IoT reported [41] that service provisioning process (SPP) can also effectively provide interaction between applications and services. The SPP first performs a "types query" that sends a request for services with a generic WSDL format, and then uses a

"candidate search" mechanism to find potential services. Based on the "Application context" and "QoS information," all service instances are ranked and a "On-Demand service provisioning" mechanism will be used to identify a service instance that matches the application's requirements. In the end, a "Process Evaluation" is used to evaluate the process [41], [42].

IV. Key Enabling Technologies

A. Identification and Tracking Technologies

The identification and tracking technologies involved in IoT include RFID systems, barcode, and intelligent sensors. A simple RFID system is composed of an RFID reader and an RFID tag. Because of its ability to identify, trace, and track devices and physical objects, the RFID system is increasingly being used in industries, such as logistics, supply chain management, and healthcare service monitoring [6], [43]. Other benefits of the RFID system include providing precise real-time information about the involved devices, reducing labor cost, simplifying business process, increasing the accuracy of inventory information, and improving business efficiency. So far, the RFID system has been successfully used by numerous manufacturers, distributors, and retailers in many industries [7], [8].

Recent development of the RFID technology focuses on the following aspects [6], [7], [8], [43]: 1) active RFID systems with spread-spectrum transmission; and 2) technology of managing RFID applications [7], [8].

There is still a plenty of room for the growth of the RFID-based applications [44]. To further promote the RFID technology, RFID can be integrated with WSNs to better track and trace things in real time. In particular, the emerging wireless intelligent sensor technologies, such as electromagnetic sensors, biosensors, off-board sensors, sensor tags, independent tag, and sensor devices further facilitate implementation and deployment of industrial services and applications. By integrating data acquired by intelligent sensors with RFID data, more powerful IoT applications that are suitable for the industrial environments can be created.

B. Communication Technologies in IoT

IoT can contain many electronic devices, mobile devices, and industrial equipment. Different things have different communication, networking, data processing, data storage capacities, and transmission power. For instance, many smart phones now have powerful communication, networking, data processing, and data storage capacities. Compared to smart phones, heart rate monitor watches only have limited communication and computation capabilities. All these things can be connected by networking and communication technologies.

IoT involves a number of heterogeneous networks such as WSNs, wireless mesh networks, WLAN, etc. These networks help things in IoT exchange information. A gateway has the ability to facilitate the communication or interaction of various devices over the Internet. The gateway can also leverage its network knowledge by executing optimization algorithms locally. Therefore, a gateway can be used to handle many complex aspects involved in communication on the network [44].

Different things may have varying QoS requirements such as performance, energy efficiency, and security. For example, many devices rely on batteries and thus reducing energy consumption for these devices is a top concern. In contrast, devices with power supply connection often do not set energy saving as a top priority. IoT would also greatly benefit by leveraging existing Internet protocols such as IPv6, as this would make it possible to directly address any number of things needed through the Internet [3], [19], [20]. Main communication protocols and standards include RFID (e.g., ISO 18000 6c EPC class 1 Gen2), NFC, IEEE 802.11 (WLAN), IEEE 802.15.4 (ZigBee), IEEE 802.15.1 (Bluetooth), Multihop Wireless Sensor/Mesh Networks, IETF Low power Wireless Personal Area Networks (6LoWPAN), Machine to Machine (M2M), and traditional IP technologies such as IP, IPv6, etc.

C. Networks Involved in IoT

There are quite a few cross-layer protocols for wireless networks such as Wireless Sensor and Actuator Networks (WSANs) or Ad Hoc Networks (AHNs) [37]. However, they must be revised before they can be applied to the IoT. The reason is that because things in IoT often have diverse communication and computation capabilities, and varying QoS requirements. In contrast, nodes in WSNs typically have similar requirements for hardware and network communication. In addition, the IoT network uses the Internet to support information exchange and data communication. In contrast, WSNs and AHNs do not have to involve the Internet for communication.

D. Service Management in IoT

Service management in IoT refers to the implementation and management of quality IoT services that meet the needs of users or applications. The SOA can be used to encapsulate services by hiding the implementation details of services such as protocols used [45]. This makes it possible to decouple between components in a system and therefore hide the heterogeneity from end users. An SOA-IoT allows applications to use heterogeneous objects as compatible services [11]. On the other hand, the dynamic nature of IoT applications requires IoT to provide reliable and consistent services. An effective SOA can minimize the impact caused by device moves or battery failure. A good example is the OSGi platform [46] that applies a dynamic SOA architecture to enable the deployment of smart services. As an effective modular platform for service deployment, OSGi has been employed in diverse contexts (e.g., mobile apps, plug-in, application servers, etc.). In IoT, the service composition based on OSGi platform can be implemented by Apache Felix iPoJo [47].

A service is a collection of data and associated behaviors to accomplish a particular function or feature of a device or portions of a device. Services can be provisioned in various ways. A service may reference other primary or secondary services and/or a set of characteristics that make up the service. The services can be categorized into two types: primary service and secondary service. The former denotes services that expose the primary functionalities at an IoT node, which can be seen as the basic service component and can be included by another service. A secondary service can provide auxiliary functionalities to the

primary service or other secondary services. A service may consist of one or more characteristics, which defines service data structures, permission, descriptors, and other attributes of a service [32], [38].

In a service-oriented IoT, services can be created and deployed according to the following steps [3], [19], [20]: 1) developing services composition platforms; 2) abstracting the device' functionalities and communication capabilities; and 3) provision of a common set of services. Services identity management involves context management and object classification. IoT also makes it possible to build a mirror for each real object in the IoT. IoT also has a service-oriented and context aware architecture, where every virtual and physical object can communicate with one another. The service-oriented IoT allows each component to offer its functionalities as standard services, which might significantly increase the efficiency of both devices and networks involved in IoT.

V. Key IoT Applications in Industries

IoT applications are still in its early stage [19], [20], [32]. However, the use of IoT is rapidly evolving and growing. Quite a few IoT applications are being developed and/or deployed in various industries including environmental monitoring, healthcare service, inventory and production management, food supply chain (FSC), transportation, workplace and home support, security, and surveillance. Atzori *et al.* [19] and Miorandi *et al.* [20] provide a general introduction to IoT applications in various domains. Different from their discussions, our discussion specifically focuses on industrial IoT applications. The design of industrial IoT applications needs to consider multiple goals.

Depending on the intended industrial application, designers may have to make a tradeoff among these goals to achieve a balance of cost and benefits [48]. Below are some IoT applications in industries.

1) *Using IoT in the healthcare service industry* [49]. IoT provides new opportunities to improve healthcare [33]. Powered by IoT's ubiquitous identification, sensing, and communication capacities, all objects in the healthcare systems (people, equipment, medicine, etc.) can be tracked and monitored constantly [50]. Enabled by its global connectivity, all the healthcare-related information (logistics, diagnosis, therapy, recovery, medication, management, finance, and even daily activity) can be collected, managed, and shared efficiently. For example, a patient's heart rate can be collected by sensors from time to time and then sent to the doctor's office. By using the personal computing devices (laptop, mobile phone, tablet, etc.) and mobile internet access (WiFi, 3G, LTE, etc.), the IoT-based healthcare services can be mobile and personalized [51]. The wide spread of mobile internet service has expedited the development of the IoT-powered in-home healthcare (IHH) services [49]. Security and privacy concerns are two major challenges.
2) *Using IoT in FSC* [52]. Today's FSC is extremely distributed and complex. It has large geographical and temporal scale, complex operation processes, and large number of stakeholders. The complexity has caused many issues in the quality management, operational efficiency, and public food safety. IoT technologies offer promising potentials to address the traceability, visibility, and controllability challenges. It can cover the FSC in the so-called farm-to-plate manner, from precise agriculture, to food production, processing, storage, distribution, and consuming. Safer, more efficient, and sustainable FSCs are expectable in the future. A typical IoT solution for FSC (the so-called Food-IoT) comprises three parts: a) the field devices such as WSN nodes, RFID readers/tags, user interface terminals, etc.; b) the backbone system such as databases, servers, and many kinds of terminals connected by distributed computer networks, etc.; and c) the communication infrastructures such as WLAN, cellular, satellite, power line, Ethernet, etc. As the IoT system offers ubiquitous networking capacity, all of these elements can be distributed throughout the entire FSC. Furthermore, it also offers effective sensing functionalities to track and monitor the process of food production. The vast amount of raw data can be further mined and analyzed to improve the business process and support decision making. Big data analytics can be used to respond to the challenge of analyzing the tremendous amount of data collected from FSC.
3) *Using IoT for safer mining production*. Mine safety is a big concern for many countries due to the working condition in the underground mines. To prevent and reduce accidents in the mining, there is a need to use IoT technologies to sense mine disaster signals in order to make early warning, disaster forecasting, and safety improvement of underground production possible [53]. By using RFID, WiFi, and other wireless communications technology and devices to enable effective communication between surface and underground, mining companies can track the location of underground miners and analyze critical safety data collected from sensors to enhance safety measures. Another useful application is to use chemical and biological sensors for the early disease detection and diagnosis of underground miners, as they work in a hazardous environment. These chemical and biological sensors can be used to acquire biological information from human body and organs and to detect hazardous dust, harmful gases, and other environmental hazards that will cause accidents. A challenge is that wireless devices need power and could potentially detonate gas in the mine. More research is needed regarding safety characteristics of IoT devices used in the mining production.
4) *Using IoT in transportation and logistics*. IoT will play an increasingly important role in transportation and logistics industries [19]. As more and more physical objects are equipped with bar codes, RFID tags or sensors, transportation and logistics companies can conduct real-time monitoring of the move of physical objects from an origin to a destination across the entire supply chain including manufacturing, shipping, distribution, and so on [54]. Furthermore, IoT is expected to offer promising solutions to transform transportation systems and automobile services [55]. As vehicles have increasingly powerful sensing, networking, communication, and data processing

capabilities, IoT technologies can be used to enhance these capabilities and share under-utilized resources among vehicles in the parking space or on the road. For example, IoT technologies make it possible to track each vehicle' existing location, monitor its movement, and predict its future location. Recently, an intelligent informatics system (iDrive system) developed by BMW used various sensors and tags to monitor the environment such as tracking the vehicle location and the road condition to provide driving directions [56]. Zhang *et al.* [57] designed an intelligent monitoring system to monitor temperature/humidity inside refrigerator trucks by using RFID tags, sensors, and wireless communication technology. In the near future, we will see the development of an automotive autopilot that can automatically detect pedestrians or other vehicles and take evasive steering to avoid collisions as needed [58]. Security and privacy protection are important for the widespread use of IoT in transportation and logistics, since many vehicle drivers are worried about information leak and privacy invasion. Reasonable efforts in technology, law, and regulation are needed to prevent unauthorized access to or disclosure of the privacy data.

5) *Using IoT in firefighting*. IoT has been used in the firefighting safety field to detect potential fire and provide early warning for possible fire disasters. In China, RFID tags and/or bar codes are being attached to firefighting products to develop nationwide firefighting product information databases and management systems. By leveraging RFID tags, mobile RFID readers, intelligent video cameras, sensor networks, and wireless communication networks, the firefighting authority or related organizations could perform automatic diagnosis to realize real-time environmental monitoring, early fire warning and emergency rescue as needed. Researchers in China are also using IoT technologies to construct fire automatic alarming systems in order to raise the nation's firefighting management and emergency management to a new level [59]. Recently, Ji and Qi [60] illustrate an infrastructure of IoT applications used for emergency management in China. Their IoT application infrastructure contains sensing layer, transmission layer, supporting layer, platform layer, and application layer. Their IoT infrastructure has been designed to integrate both local-based and sector-specific emergency systems. Establishing standards for implementing Fire IoT is a pressing challenge now.

VI. Research Challenges and Future Trends

It is broadly accepted that the IoT technologies and applications are still in their infancy [32]. There are still many research challenges for industrial use such as technology, standardization, security, and privacy [19], [20]. Future efforts are needed to address these challenges and examine the characteristics of different industries to ensure a good fit of IoT devices in the industrial environments. A sufficient understanding of industrial characteristics and requirements on factors such as cost, security, privacy, and risk is required before IoT will be widely accepted and deployed in industries.

A. Technical Challenges

Although a lot of research efforts have been made on IoT technologies, there are still technical challenges.

1) Design an SOA for IoT is a big challenge, in which service-based things might suffer from performance and cost limitations. In addition, scalability issues often arise as more and more physical objects are connected to the network. When the number of things is large, scalability is problematic at different levels including data transfer and networking, data processing and management, and service provisioning [20].
2) From the viewpoint of network, the IoT is a very complicated heterogeneous network, which includes the connection between various types of networks through various communication technologies. Currently, there is lack of widely accepted common platform that hides the heterogeneity of underlining networks/communication technologies and provides a transparent naming service to various applications [20]. Large amounts of data transmission across the network at the same time can also cause frequent delay, conflict, and communication issues. It is a challenging task to develop networking technologies and standards that can allow data gathered by a large number of devices to move efficiently within IoT networks. Managing connected things in terms of facilitating the collaboration between different entities and the administering devices addressing, identification, and optimization at the architectural and protocol levels is a research challenge [17].
3) From the viewpoint of service, a lack of a commonly accepted service description language makes the service development and integration of resources of physical objects into value-added services difficult. The developed services could be incompatible with different communication and implementation environments [19], [22]. In addition, powerful service discovery methods and object naming services need to be developed to spread the IoT technology [19], [20].
4) As IoT is often developed based on a traditional ICT environment and it is affected by everything connected to the network, it requires a lot of work to integrate IoT with existing IT systems or legacy systems into a unified information infrastructure. Furthermore, with the huge number of things connected to the Internet, a massive amount of real-time data flow will be automatically produced by connected things [61]. The data may not have much meaningful value unless people find an effective way to analyze and understand it [62]. Analyzing or mining massive amounts of data generated from both IoT applications and existing IT systems to derive valuable information requires strong big data analytics skills, which could be challenging for many end users. In addition, integrating IoT devices with external resources such as existing software systems and Web services requires the development of various middleware solutions, since applications vary a lot by industries. Building practical applications in which heterogeneous IoT-related data are combined with traditional data can be a challenging task for a variety of industries.

B. Standardization

The rapid growth of IoT makes the standardization difficult. However, standardization plays an import role for the further development and spread of IoT. Standardization in IoT aims to lower the entry barriers for the new service providers and users, to improve the interoperability of different applications/systems and to allow products or services to better perform at a higher level. A careful standardization process and a lot of coordination efforts are needed to ensure devices and applications from different countries to be able to exchange information [20]. Various standards used in IoT (e.g., security standards, communication standards, and identification standards) might be the key enablers for the spread of IoT technologies and need to be designed to embrace emerging technologies. Specific issues in IoT standardization include interoperability issue, radio access level issues, semantic interoperability, and security and privacy issues [63]–[65]. In addition, industry-specific guidelines or standards for implementing IoT in industrial environments are also recommended for easier integration of various services.

C. Information Security and Privacy Protection

The acceptance and widespread of new IoT technologies and services will largely rely on the information security and data privacy protection, which are two difficult issues in IoT because of its deployment, mobility, and complexity [66]. Many existing technologies are available for consumer use, but are not suitable for industrial applications that have strict safety and security requirements. To secure the information, existing encryption technology borrowed from the WSNs or other networks need to be carefully reviewed, when they are used to build IoT. As IoT allows many daily things to be tracked, monitored, and connected, and a lot of personal and private information can be collected automatically [19]. Protecting privacy in the IoT environment becomes more serious than the traditional ICT environment because the number of attack vectors on IoT entities is apparently much larger [67], [68], [69]. For example, a health monitor will collect patient's information, such as heart rate and blood sugar level and then send the information directly to the doctor's office over the network. When the information is transferred over the network, patient's data could be stolen or compromised. Another example is that bio-sensor used in the food industry can be used to monitor temperature and bacterial composition of food stored in the refrigerator. When some food becomes deteriorated, data can be sent back to the food company through the network. However, such data should be kept strictly confidential in order to protect the reputation of a food company [20]. It should be noticed that some issues, such as the definition of privacy and legal interpretation are still vague and are not clearly defined in IoT. Although the existing network security technologies provide a basis for privacy and security in IoT, more work still needs to be done. A reliable security protection mechanism for IoT needs to be researched from the following aspects: 1) the definition of security and privacy from the viewpoint of social, legal, and culture; 2) trust and reputation mechanism; 3) communication security such as end-to-end encryption; 4) privacy of communication and user data; and 5) security on services and applications.

D. Research Trends

The development of IoT infrastructures will likely follow an incremental approach and expand from existing identification techniques, such as RFID. International cooperation efforts and a system-level perspective are needed to address the above IoT-related challenges [20], [70]–[73]. In addition to conducting research to address the above challenges, we also identify a few other research trends.

1) Integrating Social Networking With IoT Solutions: There is a strong interest to use social networking to enhance the communications among different IoT things. A new paradigm, named Social Internet of Things (SIoT), was recently proposed by Atzori *et al.* [42]. There is a trend for the move from IoT to a new vision named Web of Things that allows IoT objects to become active actors and peers on the Web [74]–[77].

2) Developing Green IoT Technologies: As IoT involves billions of connected sensors communicating through the wireless network, the power consumption of sensors is a big concern and limitation for the widespread of IoT. Saving energy should become a critical design goal for IoT devices, such as wireless sensors [78]. There is a need to develop energy-efficient techniques or approaches that can reduce the consumed power by sensors [79].

3) Developing Context-Aware IoT Middleware Solutions: When billions of sensors are connected to the Internet, it is not feasible for people to process all the data collected by those sensors. Context-awareness computing techniques, such as IoT middleware are proposed to better understand sensor data and help decide what data needs to be processed [61]. Currently, most IoT middleware solutions do not have context-awareness capabilities. The European Union has identified context awareness as an important IoT research area and specified a time frame (2015–2020) for context-aware IoT computing research and development [21].

4) Employing Artificial Intelligence Techniques to Create Intelligent Things or Smart Objects: Arsénio *et al.* [80] propose to create Internet of Intelligent Things by bringing artificial intelligence into things and communication networks. Future IoT systems should have characteristics including "self-configuration, self-optimization, self-protection, and self-healing" [81], [82]. Smart objects will become more intelligent [83] and context-aware with larger memory, processing, and reasoning capabilities in the future.

5) Combining IoT and Cloud Computing: Clouds provide a good way for things to get connected and allow us to access different things on the Internet. Further research will focus on implementing new models or platforms that provide "sensing as a service" on the cloud [84]–[86].

VII. Conclusion

As a complex cyber-physical system, IoT integrates various devices equipped with sensing, identification, processing, communication, and networking capabilities. In particular, sensors and actuators are getting increasingly powerful, less expensive and smaller, which makes their use ubiquitous. Industries have

strong interest in deploying IoT devices to develop industrial applications such as automated monitoring, control, management, and maintenance. Due to the rapid advances in technology and industrial infrastructure, IoT is expected to be widely applied to industries. For example, the food industry is integrating WSN and RFID to build automated systems for tracking, monitoring, and tracing food quality along the food supply chain in order to improve food quality.

This paper reviews the recent researches on IoT from the industrial perspective. We firstly introduce the background and SOA models of IoT and then discuss the fundamental technologies that might be used in IoT. Next, we introduce some key industrial applications of IoT. Afterward, we analyzed the research challenges and future trends associated with IoT. Different from other IoT survey papers, a main contribution of this review paper is that it focuses on industrial IoT applications and highlights the challenges and possible research opportunities for future industrial researchers.

References

[1] K. Ashton. (2009, Jun.). Internet of things. *RFID J.* [Online]. Available: http://www.rfidjournal.com/articles/view?4986

[2] R. van Kranenburg, *The Internet of Things: A Critique of Ambient Technology and the All-Seeing Network of RFID.* Amsterdam, The Netherlands: Institute of Network Cultures, 2007.

[3] R. van Kranenburg, E. Anzelmo, A. Bassi, D. Caprio, S. Dodson, and M. Ratto, "The internet of things," in *Proc. 1st Berlin Symp. Internet Soc.,* Berlin, Germany, 2011, pp. 25–27.

[4] Y. Li, M. Hou, H. Liu, and Y. Liu, "Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things," *Inf. Technol. Manage.*, vol. 13, no. 4, pp. 205–216, 2012.

[5] L. Tan and N. Wang, "Future internet: The internet of things," in *Proc. 3rd Int. Conf. Adv. Comput. Theory Eng.* (ICACTE), Chengdu, China, Aug. 20–22, 2010, pp. V5-376–V5-380.

[6] X. Jia, O. Feng, T. Fan, and Q. Lei, "RFID technology and its applications in internet of things (IoT)," in *Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw.* (CECNet), Yichang, China, Apr. 21–23, 2012, pp. 1282–1285.

[7] C. Sun, "Application of RFID technology for logistics on internet of things," *AASRI Procedia*, vol. 1, pp. 106–111, 2012.

[8] E. W. T. Ngai, K. K. Moon, F. J. Riggins, and C. Y. Yi, "RFID research: An academic literature review (1995–2005) and future research directions," *Int. J. Prod. Econ.*, vol. 112, no. 2, pp. 510–520, 2008.

[9] S. Li, L. Xu, and X. Wang, "Compressed sensing signal and data acquisition in wireless sensor networks and internet of things," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2177–2186, Nov. 2013.

[10] W. He and L. Xu, "Integration of distributed enterprise applications: A survey," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 35–42, Feb. 2014.

[11] D. Uckelmann, M. Harrison, and F. Michahelles, "An architectural approach towards the future internet of things," in *Architecting the Internet of Things*. D. Uckelmann, M. Harrison, and F. Michahelles, Eds., New York, NY, USA: Springer, 2011, pp 1–24.

[12] S. Li, L. Xu, X. Wang, and J. Wang, "Integration of hybrid wireless networks in cloud services oriented enterprise information systems," *Enterp. Inf. Syst.*, vol. 6, no. 2, pp. 165–187, 2012.

[13] L. Wang, L. Xu, Z. Bi, and Y. Xu, "Data filtering for RFID and WSN integration," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 408–418, Feb. 2014.

[14] L. Ren, L. Zhang, F. Tao, X. Zhang, Y. Luo, and Y. Zhang, "A methodology towards virtualization-based high performance simulation platform supporting multidisciplinary design of complex products," *Enterp. Inf. Syst.*, vol. 6, no. 3, pp. 267–290, 2012.

[15] F. Tao, Y. Laili, L. Xu, and L. Zhang, "FC-PACO-RM: A parallel method for service composition optimal-selection in cloud manufacturing system," *IEEE Trans. Ind. Informat.*, vol. 9, no. 4, pp. 2023–2033, Nov. 2013.

[16] Q. Li, Z. Wang, W. Li, J. Li, C. Wang, and R. Du, "Applications integration in a hybrid cloud computing environment: Modelling and platform," *Enterp. Inf. Syst.*, vol. 7, no. 3, pp. 237–271, 2013.

[17] D. Bandyopadhyay and J. Sen, "Internet of things: Applications and challenges in technology and standardization," *Wireless Pers. Commun.*, vol. 58, no. 1, pp. 49–69, 2011.

[18] ITU NGN-GSI Rapporteur Group, *Requirements for Support of USN Applications and Services in NGN Environment,* Geneva, Switzerland: International Telecommunication Union (ITU), 2010.

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

[20] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Netw.*, vol. 10, no. 7, pp. 1497–1516, 2012.

[21] O. Vermesan, P. Friess, and P. Guillemin. (2009). Internet of things strategic research roadmap. *The Cluster of European Research Projects* [Online]. Available: http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf, accessed on Oct. 1, 2013.

[22] H. Sundmaeker, P. Guillemin, and P. Friess, *Vision and Challenges for Realizing the Internet of Things.* Brussels, Belgium: European Commission, 2010.

[23] K. Voigt. (2012). *China Looks to Lead the Internet of Things* [Online]. Available: http://www.cnn.com/2012/11/28/business/china-internet-of-things/, accessed on Oct. 1, 2013.

[24] H. Zhang and L. Zhu, "Internet of things: Key technology, architecture and challenging problems," in *Proc. 2011 IEEE Int. Conf. Comput. Sci. Autom. Eng.* (CSAE), Shanghai, China, Jun. 10–12, pp. 507–512.

[25] S. Wang, L. Li, K. Wang, and J. Jones, "E-business system integration: A systems perspective," *Inf. Technol. Manage.*, vol. 13, no. 4, pp. 233–249, 2012.

[26] F. Tao, H. Guo, L. Zhang, and Y. Cheng, "Modelling of combinable relationship-based composition service network and the theoretical proof of its scale-free characteristics," *Enterp. Inf. Syst.*, vol. 6, no. 4, pp. 373–404, 2012.

[27] L. Xu, W. Viriyasitavat, P. Ruchikachorn, and A. Martin, "Using propositional logic for requirements verification of service workflow," *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 639–646, Aug. 2012.

[28] D. Paulraj, S. Swamynathan, and M. Madhaiyan, "Process model-based atomic service discovery and composition of composite semantic web services using web ontology language for services," *Enterp. Inf. Syst.*, vol. 6, no. 4, pp. 445–471, 2012.

[29] H. Panetto and J. Cecil, "Information systems for enterprise integration, interoperability and networking: Theory and applications," *Enterp. Inf. Syst.*, vol. 7, no. 1, pp. 1–6, 2013.

[30] W. Viriyasitavat, L. Xu, and A. Martin, "SWSpec, service workflow requirements specification language: The formal requirements specification in service workflow environments," *IEEE Trans. Ind. Informat.*, vol. 8, no. 3, pp. 631–638, Aug. 2012.

[31] S. Hachani, L. Gzara, and H. Verjus, "A service-oriented approach for flexible process support within enterprises: An application on PLM systems," *Enterp. Inf. Syst.*, vol. 7, no. 1, pp. 79–99, 2013.

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

[33] M. C. Domingo, "An overview of the internet of things for people with disabilities," *J. Netw. Comput. Appl.*, vol. 35, no. 2, pp. 584–596, 2012.

[34] C. H. Liu, B. Yang, and T. Liu, "Efficient naming, addressing and profile services in Internet-of-Things sensory environments," *Ad Hoc Netw.*, to be published.

[35] Y. Wu, Q. Z. Sheng, and S. Zeadally, "RFID: Opportunities and challenges," in *Next-Generation Wireless Technologies*, N. Chilamkurti, Ed. New York, NY, USA: Springer, 2013, ch. 7, pp. 105–129.

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

[37] 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, 2013.

[38] 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. Serv. Comput.*, vol. 3, no. 3, pp. 223–235, Jul./Sep. 2010.

[39] 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, 2012.

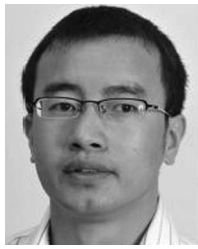
[40] D. Romero, G. Hermosillo, A. Taherkordi, R. Nzekwa, R. Rouvoy, and F. Eliassen, "RESTful integration of heterogeneous devices in pervasive environments," in *Distributed Applications and Interoperable Systems.* Berlin, Germany: Springer-Verlag, 2010, ch. 01, pp. 1–4.
[41] H. Zhou, *The Internet of Things in the Cloud: A Middleware Perspective.* Boca Raton, FL, USA: CRC Press, 2012.
[42] 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, 2012.
[43] M. K. Lim, W. Bahr, and S. Leung, "RFID in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends," *Int. J. Prod. Econ.*, vol. 145, no. 1, pp. 409–430, 2013.
[44] Q. Zhu, R. Wang, Q. Chen, Y. Liu, and W. Qin, "IoT gateway: Bridging wireless sensor networks into internet of things," in *Proc. IEEE/IFIP 8th Int. Conf. Embedded Ubiquitous Comput.* (EUC), Hong Kong, China, Dec. 11–13, 2010, pp. 347–352.
[45] Y. Liu and G. Zhou, "Key technologies and applications of internet of things," in *Proc. 2012, 5th Int. Conf. Intell. Comput. Technol. Autom.* (ICICTA), Zhangjiajie, China, pp. 187–200.
[46] H. Cervantes and R. S. Hall, "Automating service dependency management in a service-oriented component model," in *Proc. 6th Workshop Compon.-Based Softw. Eng.,* Portland, Oregon, USA, May 2003, pp. 1–5.
[47] J. I. Vazquez, A. Almeida, I. Doamo, X. Laiseca, and P. Orduña, "Flexeo: An architecture for integrating wireless sensor networks into the internet of things," in *Proc. 2008, 3rd Symp. Ubiquitous Comput. Ambient Intell.,* Salamanca, Spain, 2009, pp. 219–228.
[48] C. Flügel and V. Gehrmann, "Scientific workshop 4: Intelligent objects for the internet of things: Internet of things-application of sensor networks in logistics," *Commun. Comput. Inf. Sci.*, vol. 32, pp. 16–26, 2009.
[49] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in *Proc. 2013, 15th Int. Conf. Adv. Commun. Technol.* (ICACT), Pyeongchang, Korea, pp. 529–534.
[50] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2688–2710, 2010.
[51] I. Plaza, L. Martín, S. Martin, and C. Medrano, "Mobile applications in an aging society: Status and trends," *J. Syst. Softw.*, vol. 84, no. 11, pp. 1977–1988, 2011.
[52] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion," *Inf. Syst. Front.*, to be published.
[53] Q. Wei, S. Zhu, and C. Du, "Study on key technologies of internet of things perceiving mine," *Procedia Eng.*, vol. 26, pp. 2326–2333, 2011.
[54] B. Karakostas, "A DNS architecture for the internet of things: A case study in transport logistics," *Procedia Comput. Sci.*, vol. 19, pp. 594–601, 2013.
[55] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," *Commun. Comput. Inf. Sci.*, vol. 312, pp. 572–580, 2012.
[56] E. Qin, Y. Long, C. Zhang, and L. Huang, "Cloud computing and the internet of things: Technology innovation in automobile service," LNCS 8017, New York, NY, USA, 2013, pp. 173–180.
[57] Y. Zhang, B. Chen, and X. Lu, "Intelligent monitoring system on refrigerator trucks based on the internet of things," *Wireless Commun. Appl.*, vol. 72, pp. 201–206, 2012.
[58] C. G. Keller, T. Dang, H. Fritz, A. Joos, C. Rabe, and D. M. Gavrila, "Active pedestrian safety by automatic braking and evasive steering," *IEEE Trans. Intell. Transp. Syst.*, vol. 12, no. 4, pp. 1292–1304, Dec. 2011.
[59] Y. C. Zhang and J. Yu, "A study on the fire IOT development strategy," *Procedia Eng.*, vol. 52, pp. 314–319, 2013.
[60] Z. Ji and A. Qi, "The application of internet of things (IOT) in emergency management system in China," in *Proc. 2010 IEEE Int. Conf. Technol. Homeland Security* (HST), pp. 139–142.
[61] S. Wang, Z. Zhang, Z. Ye, X. Wang, X. Lin, and S. Chen, "Application of environmental internet of things on water quality management of urban scenic river," *Int. J. Sustain. Develop. World Ecol.*, vol. 20, no. 3, pp. 216–222, 2013.
[62] C. Perera, A. Zaslavsky, P. Christen, and D. Georgakopoulos, "Context aware computing for the internet of things: A survey," *IEEE Commun. Surveys Tuts.*, to be published.
[63] F. Wang, B. Ge, L. Zhang, Y. Chen, Y. Xin, and X. Li, "A system framework of security management in enterprise systems," *Syst. Res. Behav. Sci.*, vol. 30, no. 3, pp. 287–299, 2013.
[64] J. Li, J. Yang, Y. Zhao, and B. Liu, "A top-down approach for approximate data anonymisation," *Enterp. Inf. Syst.*, vol. 7, no. 3, pp. 272–302, 2013.
[65] Y. Xing, L. Li, Z. Bi, M. Wilamowska-Korsak, and L. Zhang, "Operations research (OR) in service industries: A comprehensive review," *Syst. Res. Behav. Sci.*, vol. 30, no. 3, pp. 300–353, 2013.
[66] J. Wan and J. Jones, "Managing IT service management implementation complexity from the perspective of the Warfield version of systems science," *Enterp. Inf. Syst.*, vol. 7, no. 4, pp. 490–522, 2013.
[67] R. Roman, P. Najera, and J. Lopez, "Securing the internet of things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.
[68] L. Li, "Technology designed to combat fakes in the global supply chain," *Bus. Horizons*, vol. 56, no. 2, pp. 167–177, 2013.
[69] S. L. Ting and W. H. Ip, "Combating the counterfeits with web portal technology," *Enterp. Inf. Syst.*, to be published.
[70] J. Clarke, R. Castro, A. Sharma, J. Lopez, and N. Suri, "Trust & security RTD in the internet of things: Opportunities for international cooperation," in *Proc. 1st Int. Conf. Security of Internet of Things,* Kollam, India, 2012, pp. 172–178.
[71] L. Xu, "Introduction: Systems science in industrial sectors," *Syst. Res. Behav. Sci.*, vol. 30, no. 3, pp. 211–213, 2013.
[72] F. Li, C. Jin, Y. Jing, M. Wilamowska-Korsak, and Z. Bi, "A rough programming model based on the greatest compatible classes and synthesis effect," *Syst. Res. Behav. Sci.*, vol. 30, no. 3, pp. 229–243, 2013.
[73] Y. Lin, X. Duan, C. Zhao, and L. Xu, *Systems Science Methodological Approaches.* Boca Raton, FL, USA: CRC Press, 2013
[74] L. Atzori, D. Carboni, and A. Iera, "Smart things in the social loop: Paradigms, technologies, and potentials," *Ad Hoc Netw.*, to be published.
[75] L. Xu, "Information architecture for supply chain quality management," in *Int. J. Prod. Res.*, vol. 49, no. 1, pp. 183–198, 2011.
[76] J. Z. Sun, "Towards the web of things: Open research issues and the BAS-AMI use case," *Lect. Notes Electr. Eng.*, vol. 144, pp. 1–8, 2012.
[77] D. Guinard, V. Trifa, F. Mattern, and E. Wilde, "From the internet of things to the web of things: Resource-oriented architecture and best practices," in *Architecting the Internet of Things.* New York, NY, USA: Springer, 2011, pp 97–129.
[78] F. Xia, "Wireless sensor technologies and applications," *Sensors*, vol. 9, no. 11, pp. 8824–8830, 2009.
[79] E. Yaacoub, A. Kadri, and A. Abu-Dayya, "Cooperative wireless sensor networks for green internet of things," in *Proc. 8th ACM Symp. QoS Security Wireless Mobile Netw.,* Paphos, Cyprus, 2012, pp. 79–80.
[80] A. Arsénio, H. Serra, R. Francisco, F. Nabais, J. Andrade, and E. Serrano, "Internet of Intelligent Things: Bringing artificial intelligence into things and communication networks," *Stud. Comput. Intell.*, vol. 495, pp. 1–37, 2014.
[81] J. O. Kephart and D. M. Chess, "The vision of autonomic computing," *IEEE Computer*, vol. 36, no. 1, pp. 41–50, Jan. 2003.
[82] G. Kortuem, F. Kawsar, D. Fitton, and V. Sundramoorthy, "Smart objects as building blocks for the internet of things," *IEEE Internet Comput.*, vol. 14, no. 1, pp. 44–51, Jan./Feb. 2010.
[83] Y. Ding, Y. Jin, L. Ren, and K. Hao, "An intelligent self-organization scheme for the internet of things," *IEEE Comput. Intell. Mag.*, vol. 8, no. 3, pp. 41–53, Aug. 2013.
[84] B. P. Rao, P. Saluia, N. Sharma, A. Mittal, and S. V. Sharma, "Cloud computing for internet of things & sensing based applications," in *Proc. 2012 6th Int. Conf. Sens. Technol.* (ICST), Kolkata, West Bangal, India, pp. 374–380.
[85] S. Fang, L. Xu, H. Pei, and Y. Liu, "An integrated approach to snowmelt flood forecasting in water resource management," *IEEE Trans. Ind. Informat.*, vol. 10, no. 1, pp. 548–558, Feb. 2014.
[86] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Gen. Comput. Syst.*, vol. 29, no. 7, pp. 1645–1660, 2013.

Li Da Xu (M'86–SM'11) received the M.S. degree in information science and engineering from the University of Science and Technology of China, Hefei, China, in 1981, and the Ph.D. degree in systems science and engineering from Portland State University, Portland, OR, USA, in 1986.

He serves as the Founding Chair of the International Federation for Information Processing (IFIP) Technical Committee on Information Systems (TC8) Working Group on Enterprise Information Systems (WG8.9) and the Founding Chair of the IEEE SMC Society Technical Committee on Enterprise Information Systems. He is the co-author of the recent book entitled *Systems Science Methodological Approaches*, published by Taylor & Francis Group.

Wu He received the B.S. degree in computer science from DongHua University, Shanghai, China, in 1998, and the Ph.D. degree in information science from the University of Missouri, Columbia, MO, USA, in 2006.

His research interests include enterprise applications, data mining, cyber security, and knowledge management.



Shancang Li (M'08) received the B.Eng. and M.Sc. degrees in mechanical engineering, and the Ph.D. degree in computer science from Xi'an Jiaotong University, Xian, China, in 2001, 2004, and 2008, respectively.

He joined the Faculty of Engineering, University of Bristol, Bristol, U.K., as a Researcher in 2013. His current research interests include wireless mesh and sensor networks, IoT, signal processing, and applications of wireless technologies.