Inf Syst Front (2015) 17:243–259
DOI 10.1007/s10796-014-9492-7

The internet of things: a survey

Shancang Li · Li Da Xu · Shanshan Zhao

Published online: 26 April 2014

Abstract In recent year, the Internet of Things (IoT) has drawn significant research attention. IoT is considered as a part of the Internet of the future and will comprise billions of intelligent communicating 'things'. The future of the Internet will consist of heterogeneously connected devices that will further extend the borders of the world with physical entities and virtual components. The Internet of Things (IoT) will empower the connected things with new capabilities. In this survey, the definitions, architecture, fundamental technologies, and applications of IoT are systematically reviewed. Firstly, various definitions of IoT are introduced; secondly, emerging techniques for the implementation of IoT are discussed; thirdly, some open issues related to the IoT applications are explored; finally, the major challenges which need addressing by the research community and corresponding potential solutions are investigated.

Keywords Literature Review · IoT · Internet of Things · RFID · Wireless Sensors Network · Service Oriented Architecture

S. Li
Faculty of Engineering, University of Bristol, Clifton BS8 1UB, UK
e-mail: shancang.li@bristol.ac.uk

L. D. Xu (✉)
Department of Information Technology and Decision Science, Old Dominion University, Norfolk, VA 23529, USA
e-mail: lxu@odu.edu

S. Zhao
School of Computing, University of the West of Scotland,
Paisley PA1 2BE, UK
e-mail: sszhao.uk@gmail.com

1 Introduction

Pretz has indicated that the Internet of things (IoT) is a things-connected network, where things are wirelessly connected via smart sensors (Pretz 2013); IoT is able to interact without human intervention. Some preliminary IoT applications have been already developed in healthcare, transportation, and automotive industries (He et al. 2014; Joshi and Kim 2013; Pretz 2013). Currently, IoT technologies are at their infant stages; however, many new developments have occurred in the integration of objects with sensors in the cloud-based Internet (Hepp et al. 2007; Joshi and Kim 2013; Pretz 2013). The development of IoT involves many issues such as infrastructure, communications, interfaces, protocols, and standards. We are motivated to summarize the research progress achieved so far in the development, standardization, and security assurance of IoT enabling technologies, and to identify critical research topics and future research directions of IoT.

The rest of the paper is organized as follows: Section 1 mainly provides an overview of the definitions, current research, standards, and future research of IoT. In Section 2, the current research on IoT system architecture is discussed. In Section 3, the enabling technologies of IoT are investigated. In Section 4, the applications of IoT are reviewed. Finally, some emerging research issues are identified and the future research directions are discussed.

1.1 The concept of IoT

Kevin Ashton firstly proposed the concept of IoT in 1999, and he referred the IoT as uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology. However, the exact definition of IoT is still in the forming process that is subject to the perspectives taken (Hepp et al. 2007; Joshi and Kim 2013; Pretz 2013). IoT was generally defined as "dynamic global network infrastructure with self-configuring capabilities based on standards and interoperable communication protocols; physical and virtual ‘things’ in an IoT have identities and attributes and are capable of using intelligent interfaces and being integrated as an information network” (IERC 2013; Kirtsis 2011; Li et al. 2012a, b). Basically, the IoT can be treated as a superset of connecting devices that are uniquely identifiable by existing near field communication (NFC) techniques (ETSI 2013). The words “Internet” and “Things” mean an inter-connected world-wide network based on sensory, communication, networking, and information processing technologies, which might be the new version of information and communications technology (ICT) (Kranenburg 2013; Marry 2013). Despite the argument on the definition of IoT, it has been discussed widely and corresponding technologies have been rapidly developed by various institutions (Guo et al. 2012; Hepp et al. 2007; ITU 2013; Li et al. 2013b; Pretz 2013); in particular, intelligent sensing and wireless communication techniques have become part of the IoT and new challenges and research horizons have emerged (Hunter et al. 2012; Wilamowski 2010). The International Telecommunication Union (ITU) discussed the enabling technologies, potential markets, and emerging challenges and the implications of the IoT (Frenken et al. 2008; ITU 2013). The evolvement of IoT can be illustrated by several phases as shown in Fig. 1. The IoT is initiated by the use of RFID technology, which is increasingly used in logistics, pharmaceutical production, retail, and diverse industries (Fielding and Taylor 2002; Guinard et al. 2010; Guinard et al. 2009; Xu 2011b).

The emerging wirelessly sensory technologies have significantly extended the sensory capabilities of devices and therefore the original concept of IoT hence is extending to ambient intelligence and autonomous control. To date, a number of technologies are involved in IoT, such as wireless sensor networks (WSNs), barcodes, intelligent sensing, RFID, NFC, low energy wireless communications, cloud computing, and so on (Jiang et al. 2014; Kataev et al. 2013; Li et al. 2013a; Ren et al. 2012; Tao et al. 2014a, b; Wang et al. 2014). Evolutions of these technologies bring new technologies to IoT (Deng et al. 2010; Kranenburg and Anzelmo 2011; Li et al. 2012a, b; Malatras et al. 2008; Miorandi et al. 2012; Pautasso and Wilde 2009; Peris-Lopez et al. 2006; Vermesan 2013; Wang 2012). The IoT describes the next generation of Internet, where the physical things could be accessed and identified through the Internet.

Depending on various technologies for the implementation, the definition of the IoT varies. However, the fundamental of IoT implies that objects in an IoT can be identified uniquely in the virtual representations. Within an IoT, all things are able to exchange data and if needed, process data according to predefined schemes.

1.2 Current research

In the last decade, the RFID-based identification has been widely used in logistics, retail, and pharmaceutics. Since 2010 (Kranenburg and Anzelmo 2011; Malatras et al. 2008; Miorandi et al. 2012), with the advances in intelligent sensors, low energy wireless communication, and sensor network technologies, a large number of ‘things’ can be networked as an IoT (Li and Liu 2012; Welbourne et al. 2009). To provide better services to end-users or applications, the technical standards should be designed for IoT in terms of the specifications of data exchange, processing, and communications within the network. The success of IoT depends on the standardization, which provides interoperability, compatibility, reliability, and effectiveness of the operations on a global scale. Objects in an IoT must be able to communicate and exchange data with each other autonomously (Juels 2006; Mitrokotsa et al. 2013). When millions even billions of things can be integrated seamlessly and effective, IoT can be applied widely in numerous

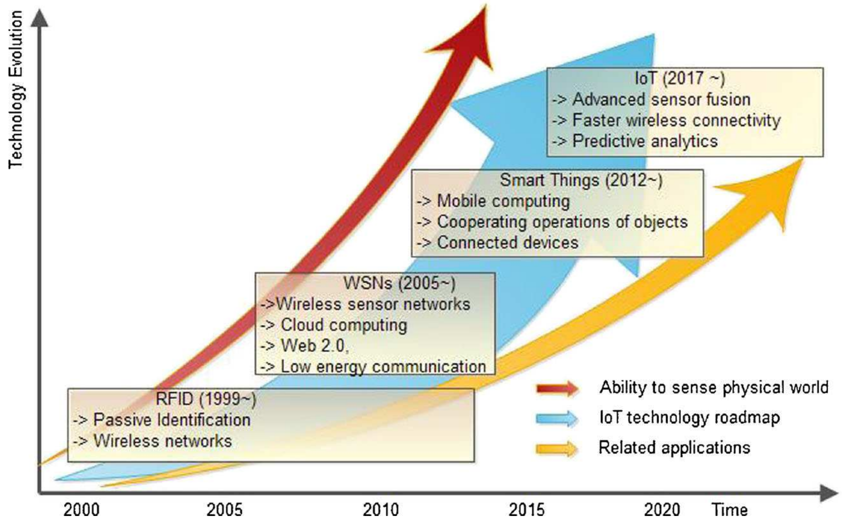


Fig. 1 Evolution of the IoT

areas (EPCglobal 2013; Joshi and Kim 2013; Li 2013; Mutti and Floerkemeier 2008).

Both developed and developing countries have recognized the importance and potential of IoT and proposed their national strategies in exploring IoT enabling technologies. For example, the UK government has launched a £5 m project on IoT technology and innovation (Fleisch 2013; Klair et al. 2010). In European Union (EU), the IoT European Research Cluster (IERC) (http://www.rfid-in-action.eu/cerp/) sponsored a number of cooperative projects on the fundamental research related to IoT. In these projects, the applications and end-users provide the specific requirements to drive the theoretical studies. For example, the project of Internet of Things Architecture (IoT-A) was to develop the reference model and architecture of IoT to meet the specific needs in the applications. Meanwhile, the European Telecommunications Standards Institute (ETSI) is responsible to make the policies related to IoT (Floerkemeier et al. 2007; Gama et al. 2012; Welbourne et al. 2009). Japan proposed "u-Japan x ICT" and "i-Japan strategies" in 2008 and 2009; these projects aimed at deploying IoT in all areas of daily lives. In the United States, the Information Technology & Innovation Foundation (ITIF) indicated that new information and communication technologies (ICT) can be an effective way to improve traditional and information technology infrastructure, and will have a greater positive impact on productivity and innovation. The focused sectors of ICT developments in US are energy, broadband technologies, rural utilities services, and health information technologies (He and Xu 2014; Xu 2011a). South Korea conducted RFID/USN and "New IT Strategy" program to advance the IoT infrastructure development. In China, the government officially launched the "Sensing China" project in June 2010; the objective of the project was to develop the technologies so that any objects in an environment have identity tags, which are able to broadcast information and such information can be accessed through the Internet. People could be tracked within the IoT and any condition variables can be monitored, so that the performances of the networked systems can be optimized to reduce wastes and costs.

1.3 Standards

It is argued that the lack of standards may decrease the competitiveness of IoT products (Broll et al. 2009; Dada and Thiesse 2008; Floerkemeier et al. 2007; Gama et al. 2012; Ilic et al. 2009; Karpischek et al. 2009; Li et al. 2014a, b). In the past decade, a number of technical standards have been developed by various organizations; these standards are playing more and more important role to the success of IoT. In particular, the standards for middleware and interfaces are extremely important. The research efforts include: (1) designing policies and distributed architecture; (2) ensuring the privacy and protecting users; (3) realizing the trustiness, acceptability, and security of networks; (4) developing standards; (5) exploring new enabling technologies such as micro-electronic-mechanical system (MEMS) devices and ubiquitous localization (Karpischek et al. 2009; Li et al. 2014a, b).

Standards on IoT have attracted a great deal of attention in many countries. Internationally (Broll et al. 2009; Dada and Thiesse 2008; Floerkemeier et al. 2007; Gama et al. 2012; Ilic et al. 2009; Karpischek et al. 2009; Li et al. 2014a, b), the ITU, Electronic Product Code global (EPCglobal), International Electro-technical Commission (IEC), International Organization for Standardization (ISO), and IEEE have provided a set of standards to identify, capture, and share data using RFID technologies. Regionally, the European Telecommunications Standards Institute (ETSI) and European Committee for Electro-technical Standardization (CEN/CENELEC) have released a set of standards on the fundamental technologies in IoT, such as RFID, WSN, etc. The American National Standards Institute (ANSI) in US is working on the management standards of IoT. The study on IoT in US has become a national research priority; IoT is expected to be applied in military, logistics, industrial automation, retail industry, airports, public-transit hubs, and hospitals. In Japan, the "uID" was developed as an infrastructure to connect fundamental researches with applied research and development (Li et al. 2014a, b). The China Communications Standards Association and the China Electronics Standardization Institute (CESI) are working on the standards of semi-passive RFID and ultra high frequency (UHF) band RFID. 973 Projects have been developed in China on the standardization and fundamental techniques of IoT (Guinard et al. 2010). Table 1 summarizes the standards involved in IoT.

IoT standardization takes efficiency and availability of specifications into account (Marry 2013; Vilamovska et al. 2012). While many organizations are working on the primary standards for IoT, a global collaboration between standards bodies is necessary to deal with the lack of consistency among standards bodies and the standards; the World Standards Cooperation (WSC) should be able to manage the relationships between the international standards bodies and regional standards bodies.

Besides, it is worth to emphasize the importance of standards for the technological development of IoT. On one hand, standards help the developers and users to determine the best technical protocols for dynamic applications and services in IoT. On the other hand, the standardization of the technologies in IoT is important and urgent which can and will accelerate the spread of IoT technology. Figure 2 summarizes the enabling technologies for IoT.

1.4 Research trend of IoT

The IoT emphasises on the interactions among the networked things. The emerging technologies such as sensing, ubiquitous

Table 1 A summary of Standards in IoT (Broll et al. 2009; Dada and Thiesse 2008; Floerkemeier et al. 2007; Gama et al. 2012; Ilic et al. 2009; Karpischek et al. 2009; Li et al. 2014a, b)

Technologies	Standards
Communication	IEEE 802.15.4(ZigBee)
	IEEE 802.11 (WLAN)
	IEEE 802.15.1(Bluetooth, Low energy Bluetooth)
	IEEE 802.15.6 (Wireless Body Area Networks)
	IEEE 1888
	IPv6
	3G/4G
	UWB
RFID	RFID tag ISO 11784
	RFID air interface Protocol: ISO 11785
	RFID payment system and contactless smart card: ISO 14443/15693
	Mobile RFID: , ISO/IEC 18092 ISO/IEC 29143
	ISO 18000-1 – Generic Parameters for the Air Interface for Globally Accepted Frequencies
	ISO 18000-2 – for frequencies below 135 kHz
	ISO 18000-3 – for 13.56 MHz
	ISO 18000-4 – for 2.45 GHz
	ISO 18000-6 – for 860 to 960 MHz
	ISO 18000-7 – for 433 MHz
Data content and encoding	EPC Global Electronic Product Code, or EPCTM
	EPC Global Physical Mark Up Language
	EPC Global Object Naming Service (ONS)
Electronic product code	Auto-ID: Global Trade Identification Number (GTIN), Serial Shipping Container Code (SSCC), and the Global Location Number (GLN).
Sensor	ISO/IEC JTC1 SC31 and ISO/IEC
	JTC1 WG7
	Sensor Interfaces: IEEE 1451.x, IEC SC 17B, EPC global, ISO TC 211, ISO TC 205
Network Management	ZigBee Alliance, IETF SNMP WG, ITU-T SG 2,
	ITU-T SG 16, IEEE 1588
Middle	ISO TC 205, ITU-T SG 16
QoS	ITU-T, IETF

computing, cloud computing, and wireless sensing, making an IoT capable of configuring machine-to-machine (M2M) networks, sensors networks, and ultimately, ubiquitous networks. Currently, researchers are studying the techniques for the interactions between human and environment, human and machine, as well as ubiquitous computing. In the long term, the trend of IoT is the fusion of sensing and Internet; all of the networked things should be flexible, smart, and autonomous enough to provide required services. IoT will provide our daily lives with desired connectivity and intelligence (Pretz 2013).

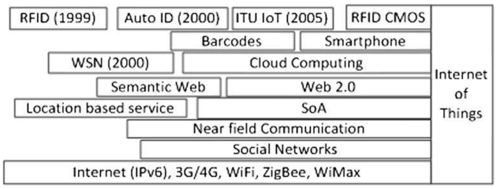


Fig. 2 Enabling Technologies for IoT

2 Service-oriented architecture

A critical requirement of an IoT is that the things in the network must be inter-connected. IoT system architecture must guarantee the operations of IoT, which bridges the gap between the physical and the virtual worlds. Design of IoT architecture involves many factors such as networking, communication, business models and processes, and security (Ulmer et al. 2013; van Looy et al. 2014). In designing the architecture of IoT, the extensibility, scalability, and interoperability among heterogeneous devices and their business models should be taken into consideration. Due to the fact that things may move geographically and need to interact with others in real-time mode, IoT architecture should be adaptive to make devices interact with other things dynamically and support unambiguous communication of events. In addition, IoT should possess the decentralized and heterogeneous nature.

In IoT, service-oriented architecture (SoA) might be imperative for the service providers and users (Ciganek et al. 2014; Hachani et al. 2013). SoA ensures the interoperability among the heterogeneous devices in multiple ways (Panetto and Cecil 2013; Jardim-Goncalves et al. 2013; Wang and Xu 2012). Figure 3 provides a generic SoA, which consists of four layers with distinguished functionalities as below:

- *Sensing layer* is integrated with available hardware objects to sense the statuses of things;
- *Network layer* is the infrastructure to support over wireless or wired connections among things;
- *Service layer* is to create and manage services required by users or applications;
- *Interfaces layer* consists of the interaction methods with users or applications.

The SoA treats a complex system as a set of well-defined simple objects or subsystems (Xu 2011a). Those objects or subsystems can be reused and maintained individually; therefore, the software and hardware components in an IoT can be reused and upgraded efficiently. Due to these advantages, SoA has been widely applied as a mainstream architecture for wireless sensors networks (Alcaraz and Lopez 2010; Roman et al. 2011; Roman and Lopez 2009). When SoA is applied in IoT, it is designed to provide the extensibility, scalability, modularity, and interoperability among heterogeneous things; in addition, the functionalities and capabilities are abstracted into a common set of services (Xiao et al. 2014). Figure 3 provides an example of SoA proposed for IoT (Roman and Lopez 2009), and the details of its components are discussed below.

2.1 Sensing layer

IoT is expected to be a world-wide physical inner-connected network, in which things are connected seamlessly and can be controlled remotely. In the sensing layer, the smart systems on tags or sensors are able to automatically sense the environment and exchange data among devices.

In the past few years, advanced sensing and communication technologies made things with RFID or sensors more versatile and accessible, which extends the capability of IoT significantly in sense that things can be uniquely identified and the surrounding environments can be monitored for various purposes and applications. Every object in IoT holds a digital identity and can be easily tracked in the digital domain. The technique of assigned unique identity to an object is called a universal unique identifier (UUID). In particular, UUID is critical to successful services deployment in a huge network like IoT. The identifiers might refer to names and addresses.

In determining the sensing layer of an IoT, the following aspects should be taken into consideration:

- *Cost, size, resource, and energy consumption*. The things might be equipped with sensing devices such as RFID tags, sensor node. Due to a large number of sensors in complex system applications, intelligent devices should be designed to minimize required resources as well as costs.
- *Deployment*. The sensing things (RFID tags, sensors, etc.) can be deployed one-time, or incrementally, or randomly depending on the requirements of applications.
- *Heterogeneity*. A variety of things with different properties can make the IoT very heterogeneous.
- *Communication*. Sensors must be communicable to make things accessible and retrievable.
- *Network*. The things are organized as multi-hop, mesh or ad hoc networks.

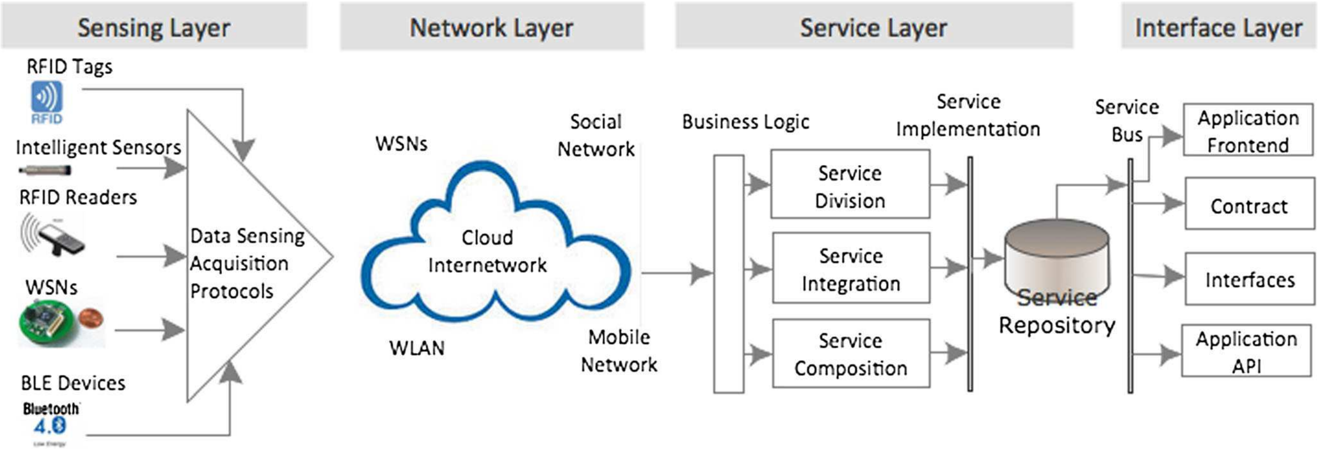


Fig. 3 Service-oriented architecture for IoT

As the scale of IoT increases, a large number of hardware and software components can be involved; therefore, IoT should also possess the following features:

- *Energy efficiency.* Sensors should be active all the time to acquire real-time data. This brings the challenge to supply power to sensors; high energy efficiency allows sensors to work a longer period time without the discontinuity of service.
- *Protocols*. Different things existing in IoT provide multiple functions of systems. IoT must support the coexistence of different communications such as WLAN, ZigBee, and Bluetooth.

From the perspective of hardware design, the main issues of hardware design are wireless identifiable systems, ultra-low cost tags, and smart/mobile sensors (Fig. 4).

2.2 Network layer

The network layer in IoT, connects all things and allows them be aware of their surroundings. Via the network layer, things can share data with the connected things, which is crucial to intelligent events management and processing in IoT. Moreover, the networking layer is capable of aggregating data from existing IT infrastructures; data can then be transmitted to decision-making units for the high-level complex services. In a SoA, the services are always performed by the things, which are deployed in a heterogeneous network. Relevant things can also be integrated through the service Internet. The communication in the network might involve the Quality of Service (QoS) to guarantee reliable services for different users or applications (Li et al. 2014a; Zheng et al. 2014b).

On the other hand, it is essential for a network to automatically discover and map things in network. Things need to be assigned roles automatically to deploy, manage, and schedule the behaviours of things and be able to switch to any roles at any time as required. This enables devices to perform tasks collaboratively. In the networking layer, the following issues should be addressed:

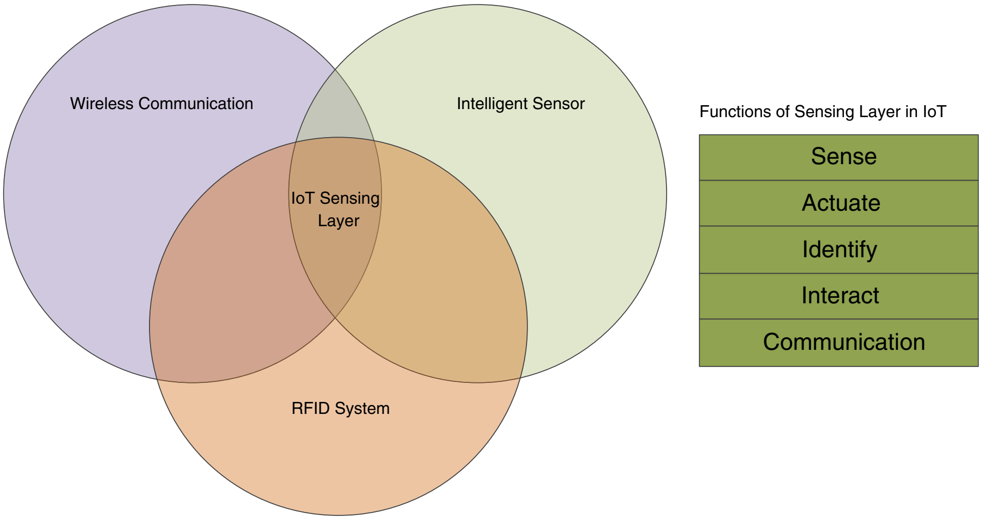
- Network management technologies including managing fixed, wireless, mobile networks
- Network energy efficiency
- Requirements of QoS
- Technologies for mining and searching
- Data and signal processing
- Security and privacy

Among these issues, information confidentiality and human privacy security are critical because of its deployment, mobility, and complexity. For information confidentiality, the existing encryption technology used in WSNs can be extended and deployed in IoT. However, it may increase the complexity of IoT. The existing network security technologies can provide a basis for privacy and security in IoT, but more work still need to be done. For example, since an IoT connects many personal things, which brings the potential risk regarding privacy.

2.3 Service layer

Service layer relies on the middleware technology, which is a key enabler of services and applications in IoT. The middleware technology provides a cost-effective platform, where the hardware and software platforms can be reused.

Fig. 4 Functions of sensing layer in IoT



The service layer involves activities required by the middle service specifications. The services in the service layer run directly on the network to effectively locate new services for an application and retrieve metadata dynamically about services. Most of specifications are undertaken by various standards developed by different organizations. However, a universally accepted service layer is important for IoT. A practical service layer consists of a minimum set of the common requirements of applications, application programming interfaces (APIs), and protocols supporting required applications and services.

All of the service-oriented activities, such as information exchanging and storage, management of data, ontologies database, search engines and communication, are performed at the service layer. The activities are conducted by the following components:

- *Service discovery* finds objects that can provide the required service and information in an effective way.
- *Service composition* enables the interaction among connected things. The discovery exploits the relationships of things to find the desired service, and the service composition schedules or re-creates more suitable service to obtain the most reliable services.
- *Trustworthiness management* aims at understanding how the information provided by other services has to be processed.
- *Service APIs* provides the interactions between services required by users.

An SOCRADES integration architecture (SIA) has been proposed that can be used to interact between applications and service layers effectively. According to Kranenburg (2013) and Vermesan (2013), the things are abstracted into the devices, which provide services at low-levels such as network discovery services, metadata exchange services, and asynchronous publish and subscribing events. A representation state transfer (REST) is defined to increase interoperability for loosely-coupled between services and distributed applications (Peris-Lopez et al. 2006). Traditionally, a service layer provides the universal API for applications, but recent research results has shown that the service provisioning process (SPP) can effectively provide the interaction between the applications and services (Hernandez-Castro et al. 2013). The SPP firstly perform a “types query”, which sends a request for services with a generic WSDL format, then “candidate search” is called to find the potential services. Based on the “Application Context” and “QoS Information”, the service instance is ranked and a “On-Demand Service Provisioning” will try to discover a service instance that matches the application’s requirements. At the end, a “Process Evaluation” is used to evaluate the process.

2.4 Interface layer

In IoT, a large number of devices are involved; those devices can be provided by different vendors and hence do not always comply with same standards. The compatibility issue among the heterogeneous things must be addressed for the interactions among things. Compatibility involves in information exchanging, communication, and events processing. There is a strong need for an effective interface mechanism to simplify the management and interconnection of things.

An interface profile (IFP) can be seen as a subset of service standards that allows a minimal interaction with the applications running on application layers. The interface profiles are used to describe the specifications between applications and services. An illustration of the interface layer is the implementation of Universal Plug and Play (UPnP), which specifies a protocol for the seamless interactions among heterogeneous things.

3 Enabling technologies

3.1 Identification and tracking technologies

The concept of IoT was coined based on the RFID-enabled identification and tracking technologies. A basic RFID system is composed of an RFID reader and an RFID tag. Due to its capability to identify, trace, and track, the RFID system has been widely applied in logistics, such as package tracking, supply chain management, healthcare applications, etc. (Krapelse 2013; Lam and Ip 2012; Li 2012; Xu 2011b). A RFID system could provide sufficient real-time information about things in IoT, which are very useful to manufacturers, distributors, and retailers. For example, RFID application in supply chain management can improve inventory management. Some identified advantages include reduced labour cost, simplified business processes, and improved efficiency.

Recently, it was reported that 3 % EU companies are using RFID (Kranenburg and Anzelmo 2011). In the RFID-based applications, 56 % for access control, 29 % for supply chain, 25 % for motorway tolls, 24 % for security control, 21 % product control, and 15 % for asset management. The next generation of RFID technology will focus on the item level RFID usage and RFID-aware management issues. Although RFID technology is successfully used in many areas, it is still evolving in developing active systems, Inkjet-printing based RFID, and management technologies (Hepp et al. 2007). Other identified problems need to be solved for using in IoT, include:

- *Collision of RFID readings*. It covers the collisions between RFID readers or RFID tags and multiple reads of the same RFID tag.

- *Signal Interferences*. Interference occurs within an RFID system or with other radio-based devices.
- *Privacy Protection*. It covers customer privacy and the confidentiality of RFID tags that can be scanned by authorized RFID scanners.
- *Standards*. Universally applicable standards are still lacking for RFIDs.
- *Integration*. The integration of RFID and smart sensors.

3.2 Integration of WSN and RFID

Many types of intelligent sensors have been developed based on physical principles of infrared, γ-ray, pressure, vibration, electromagnetic, biosensor, and X-ray. Data from those sensors in IoT can be acquired and integrated for analysis, decision-making, and storage. Examples of RFID integrated sensors are On/Off-board locating sensor, sensor tags, independent tag and sensor devices, and RFID reading systems (Pretz 2013; Miorandi et al. 2012).

The integration of sensors and RFID empowers IoT in the implementations of industrial services and the further deployment of services in extended applications. IoT integrating with RFID and WSNs makes it possible to develop IoT applications in healthcare, decision-making of complex systems, and smart systems such as smart transportation, smart city, or smart rehabilitation systems (Fan et al. 2014).

3.3 Communications

Hardware devices involve very diversified specifications in terms of communication, computation, memory, and data storage capacity, or transmission capacities. An IoT application consists of many types of devices. All types of hardware devices should be well organized through the network and be accessible via available communication. Typically, devices can be organized by gateways for the communication purpose over the Internet.

IoT can be an aggregation of heterogeneous networks, such as WSNs, wireless mesh networks, mobile networks, and WLAN (Chi et al. 2012). These networks help the things in fulfilling complex activities such as decision-makings, computation, and data exchange. In addition, the reliable communication between gateway and things is essential to make a centralized decision with respect to IoT. The gateway is capable of running the complicate optimization algorithm locally by exploiting its network knowledge. The computational complexity is shifted from things to the gateway; the global optimal route and parameter values for the gateway can be obtained. This is feasible since the size of the gateway domain is in the order of a few of tens in comparison with the sizes of things.

Hardware capabilities and the communication requirements vary from one device type to another. The things in IoT can have very different capabilities for computation, memory, power, or communication. For instance, a cellular phone or a tablet has much better communication and computation capabilities than a single-purpose electronic product such as a heart rate monitor watch. Similarly, things can have very different requirements of Quality of Service (QoS), in particular, in the aspects of delay, energy consumption, and reliability. For example, minimizing the energy use for communication/computation purposes is a major constraint for the battery powered devices without efficient energy harvesting techniques; this energy constraint is not critical for the devices with power supply connection.

IoT would also greatly benefit from the existing protocols in Internet such as IPv6 (Pretz 2013). The commonly used 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)
- Traditional IP technologies, such as IP, IPv6, etc.

The details of the communication technologies can be found in Table 2.

3.4 Networks

There exist a lot of cross-layer protocols for Wireless Networks (ETSI 2013; IERC 2013), Wireless Mesh Networks (WMNs) (Fleisch 2013) or Ad Hoc Networks (AHNs) (Marry 2013). However, they cannot be applied to the IoT due to several reasons. First, the heterogeneity of the IoT due to the fact that things have largely diversified hardware configurations, QoS requirements, functionalities, and goals. On the other hand, nodes in a WSN usually have similar hardware specifications, similar communication requirements, and the shared goal. Second, the Internet is involved in the IoT, from which it inherits a centralized and hierarchical architecture. In comparison, WSNs, WMNs and AHNs have relatively flat network architectures: nodes in these networks communicate in a multi-hop fashion and the Internet is not involved.

3.5 Service management

Service management refers to the implementation and management of the services that meet the needs of users or applications. SoA can promote the encapsulation of services. Encapsulation allows the details of services, such as the implementation and the protocols, be hidden behind the

Table 2 Communication technologies in IoT

Communication Protocols	Transmission rate	Spectrum	Transmission range
RFID	424 kbps	135 Khz	>50 cm
		13.56 MHz,	>50 cm
		866–960 MHz	>3 m
		2.4 Ghz	>1.5 m
NFC	100 kbps–10 Mbps	2.45 GHz	
ZigBee	256 kbps/20 kbps	2.4 GHz/900 MHz	10 m
Bluetooth	1 Mbps	2.4 GHz	10 m
BLE	10 kbps	2.4 GHz	10 m
UWB	50 Mbps	Wide range	30 m
WiFi	50–320 Mbps	2.4/5.8 GHz	100 m
Wi-Max	70 Mbps	2–11 GHz	50 km
UMTS/CDMA/EDGE/MBWA	2 Mbps	896 MHz	~

instances of services. SoA allows applications to use heterogonous objects as compatible services. On the other hand, the dynamic nature of IoT applications requires that IoT can provide reliable and consistent service; it can benefit from an effective service-oriented architecture to avoid failures from dislocations of device or death of battery.

3.5.1 Dynamic services composition

As reported in (Deng et al. 2010), the Open Services Gateway initiative (OSGi) platform provides a dynamic SOA architecture, which is capable of supporting smart services. The successful applications in the software industry have shown the effectiveness and modularization of OSGi in diversified areas such as mobile apps, plug-ins, and application servers. For IoT, the service composition based on the OSGi platform can be implemented by Apache Felix iPoJo.

3.5.2 Services management architecture

There is a variety of service management architecture contributing to IoT, such as the IBM's architecture with an RFID edge controller. Gama et al. (2012) proposed the service architecture based on RFID readers and sensors.

3.5.3 Recognizing and performing services

IoT is service-oriented and the mandatory subset of the future Internet – every virtual and physical object can communicate with other objects providing seamless services to other objects. Millions of devices in IoT need to be mutually interoperable. SoA makes it possible for every object to offer its functionalities as standard services. To organize the services that the real objects provide, each service can be identified uniquely by a virtual element in IoT. Figure 5 shows a real object and its virtual representation in IoT (Malatras et al. 2008).

In IoT, services can be created and deployed via the following steps (Kranenburg and Anzelmo 2011): (1) developing the services composition platforms; (2) abstracting the functionalities and communication capabilities of device; (3) providing a common set of services. Services identify the management, which involves the context management and object classification. IoT creates a mirror image for each real object in such a way to make re-creation of synchronization available.

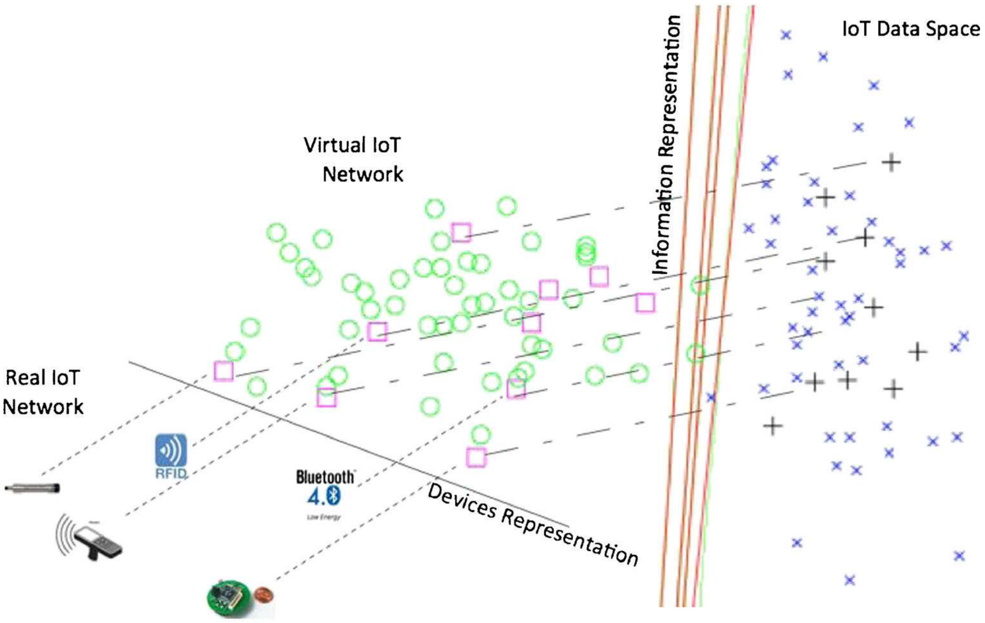
A service in IoT can be seen as a collection of data and associated behaviours to accomplish a particular function or feature of a device or portions of a device. In general, the services can be categorized into two types: *primary service* and *secondary service*. The former denotes services that expose the primary functionalities at a node, which can be seen as the basic component of services and can be included by another service. A secondary service can provides auxiliary functionality to primary service or other secondary services. A service may utilize other primary or secondary services and/or a set of characteristics that make up the service (Bluetooth SIG 2014; Li et al. 2012a, b). In IoT, each service may consist of one or more characteristics, which defines attributes of service, such as data structure, permission, descriptors, etc.

In the newly released Bluetooth SIG specification, a service can be well described with XML language for easy exchanges with other middleware. An example of "Health Thermometer Service" is illustrated below. The service provides the measurements of the health thermometer by an UUID (0x1809) as shown in Fig. 6 (Bluetooth SIG 2014; Li et al. 2012a, b; Li et al. 2014a, b); and it is unnecessary for the user to know how the measurement data is acquired.

The characteristics of a service include three components (Bluetooth SIG 2014; Li et al. 2012a, b):

- Declaration describes the properties of characteristic value such as reading, writing, indicator, as well as the value handles and types.
- Assigned values for properties.

Fig. 5 Objects mapping in IoT



- Descriptor provides accessary information about the characteristics.

Table 3 shows an example of the characteristics of a service.

3.5.4 Integration of service technologies

The service-oriented IoT extends existing architecture of IoT with unique service-oriented characteristics (Viriyasitavat, Xu and Viriyasitavat 2014a, b; Xu and Viriyasitavat 2014). The knowledge about services in such architecture must be represented appropriately to support discovery, detection, classification, composition, and testing.

As mentioned above, Fig. 3 has shown the architecture of IoT, which contains four layers: *interface layer*, *application layer*, *network layer*, and *sensing layers*. (1) The interface layer provides interface to external applications, services, etc.; (2) The application layer provides the functionalities that are built on top of an implementation of the IoT. The application layer is connected with the process modelling components for IoT-aware business processes; the processes can be executed in the process execution components; (3) The network layer contains three basic components: *service entity arrangements*, *virtual entity and information*, and *resources*. The arrangement and access of services to external entities and services is organized by the *service entity arrangements* component. The *virtual entity* (VE) component is functioning to associate VEs with relevant services; it is also a means to search for such services. The *resources* module provides the functionalities required by services for processing information and notifying application software and services about events related to resources and virtual entities; (4) Sensing layer involves sensing devices, such as RFID tags, sensor nodes, etc., that can record, collect, and process observations and measurements. The network layer is able to access the sensing layer with device-level API, which provides data exchanges between the applications in the real world.

3.6 Security and privacy

For IoT, security and privacy are two important challenges. To integrate the devices of sensing layer as intrinsic parts of the IoT, effective security technology is essential to ensure security and privacy protection in various activities such as personal activities, business processes, transportations, and

Fig. 6 An illustrate example of service in IoT

```
<?xml version="1.0" encoding="utf-8"?>
<service uuid = "1809">
  <uri>org.bluetooth.service.health_thermometer</uri>
  <description>Health Thermometer Service </description>
  <characteristic uuid = "2a1c", id = "xgatt_temperature_celsius">
    <description> Celsius temperature </description>
    <properties indicate = "true" />
    <value type = "hex"> 0000000000</value>
  </characteristic>
</service>
```

Table 3 Characteristics of a service (Bluetooth SIG 2014)

Handle	Type	Permissions	Value
39	0X2800 (Service UUID)	Read	E0:FF
40	0X2803 (Characteristic UUID)	Read	10:29:00:E1:FF

information protection (Tan et al. 2013; Wang et al. 2013; Xing et al. 2013). The applications of IoT might be affected by pervasive threats such as RFID tags attacks and data leakage. In RFID systems, a number of security schemes and authentication protocols have been proposed to cope with security threats. For example, Juels proposed the method of "block tag' to prevent the unauthorized tracing (Juels 2006). On the other hand, low-cost symmetric-key cryptography algorithms, such as Tiny Encryption Algorithm (TEA) and Advance Encryption Standard (AES), have been proposed to protect data exchange. Besides, the low-cost RFID tag has implemented some asymmetric key cryptography algorithm such as Elliptic curve cryptography (ECC) to security. On the other hand, the security protocols developed for WSN can be integrated as an intrinsic part of IoT. The following two aspects require further study: (1) The adaption of the existing Internet standards for interoperable protocols; (2) the security assurance for composeble services. The challenges in security and privacy protection are summarized as resilience to attacks, data authentication, access control, and client privacy.

4 Applications

IoT enables information gathering, storing and transmitting be available for things equipped with the tags or sensors. The tags have been widely used in supply chain management, manufacturing, environmental monitoring, retailing, smart shelf operations, healthcare, food and restaurant industry, logistic industry, travel and tourism industry, library services, and many other areas (Bi et al. 2014; Cai et al. 2014; Fang et al. 2014; Xu et al. 2014).

The IoT is of high importance to economy and society (Li et al. 2012b). To accelerate the applications of IoT, the development of IT infrastructure plays a key role (Xu et al. 2012a, b). It can be foreseen that the IoT will greatly contribute to address the social issues such as, healthcare monitoring, daily living monitoring, and traffic congestion controlling. IoT makes the interconnected of things amplify the profound effects.

Currently, IoT has already been deployed in many areas successfully:

- For users, a large number of hardware and software components (RFID tags, mobile phones, social networks, and mobile apps) have been developed for the consumers that allow users to access additional information regarding products.
- For manufacturers, an increasing number of products are made with unique identification technologies, such as barcodes, RFID tags, intelligent sensors on personal electronic devices, and home appliances. These identification technologies make products be monitored and tracked in their life cycles.
- It can increase the effectiveness of traditional industries by introducing new data exchange and processing techniques.

4.1 Industrial applications

IoT is able to improve the business transactions with smarter service networks, which will significantly improve the efficiency of real-time information processing and manage fine-grained applications, such as online-payment, critical data storage, aggregated QoS, and associated performance indicators.

IoT can reduce the gap between components in current digital economy, where services-centric economy is realized through networking transactions. Meanwhile, the business model can benefit from the IoT at the levels of intra- and inter-organizations. Enterprises using IoT can benefit from competitive products, more profitable and greener business models, optimized resources, and real-time information processing. The globally connected IoT can provide enterprises with the integrated service networks such as the example shown in Fig. 3. Manufacturers could be benefited, IoT enables the business partners to seamlessly integrate the enterprises resources (Table 4).

4.2 Social IoT (SIoT)

Recently the idea that integrates IoT with social networks has been proposed (Atzori et al. 2011) and a new paradigm "Social Internet of Things (SIoT)" is proposed to describe a world where things around human being can be intelligently sensed and networked. SIoT can perform things and service discovery effectively and improve the scalability of IoT similar to human social networks. The privacy and protection technologies used in social networks can be implanted into IoT to improve the security of IoT.

The concept of SIoT was motivated by popular social networks over the Internet (Social Internet of Things; Li et al. 2012a, b): Facebook, Twitter, and micro-blog; these networks are permeating people's daily life. Therefore, SIoT has attracted a great deal of attentions from the scientists and researchers in E-business, E-learning, sociology, psychology, and networking. The homophily (Fielding and Taylor 2002) method is proposed to establish higher levels of trust; it can be

Table 4 Industrial Applications of IoT

Industrial Deployment	Applications

Logistics and SCM (Supply Chain) Management	Goods Position Monitoring;
	Theft prevention;
	Container monitoring in SC;
	SC events monitoring

Access control	NCF Access control system;
	E-home;
	Security infrastructure

Control of industrial processes	Intelligent Quality control system;

helpful to optimize relationships among things (EPCglobal 2013; Li et al. 2012a, b). Marry (2013) and Welbourne et al. (2009) discussed the combination of social relationships into the future Internet.

Hernandez-Castro et al. (2013) discussed the integration of IoT and existing social networks (such as Facebook, Twitter, etc.). Fielding and Taylor (2002) investigated the potential of SIoT to support novel applications and networking services. In Fig. 7, an integration scheme of social networking into IoT is described and the system architecture for implementation an SIoT is given.

4.3 Healthcare applications

Healthcare is an important application area of IoT (Xu, Xu, Cai et al. 2014). IoT is adopted to enhance service quality and reduce costs. A number of medical sensors or devices are used to monitor medical parameters such as body temperature, blood glucose level, and blood pressure. Advances in sensor, wireless communication, and data processing technologies are the driving force for implementing IoT in healthcare systems. The emerging wearable body sensor networks (WBSNs) were developed to monitor patient activities or medical parameters continuously (Miorandi et al. 2012). The IoT might provide healthcare systems with the interconnection of such heterogeneous devices to obtain a comprehensive picture of health parameters.

IoT can be used to improve the current assisted living solutions. The medical devices that connected to IoT include medical sensors and wearable sensors. These sensors can be used to gather the healthcare information and transmit to remote medical centres. IoT with wearable biosensors has been applied in monitoring patients, tracking daily activities, and caring elderly. It can be foreseen that the IoT with intelligent medical sensors will enhance the quality of life significantly and prevent the occurrence of health problems. As a

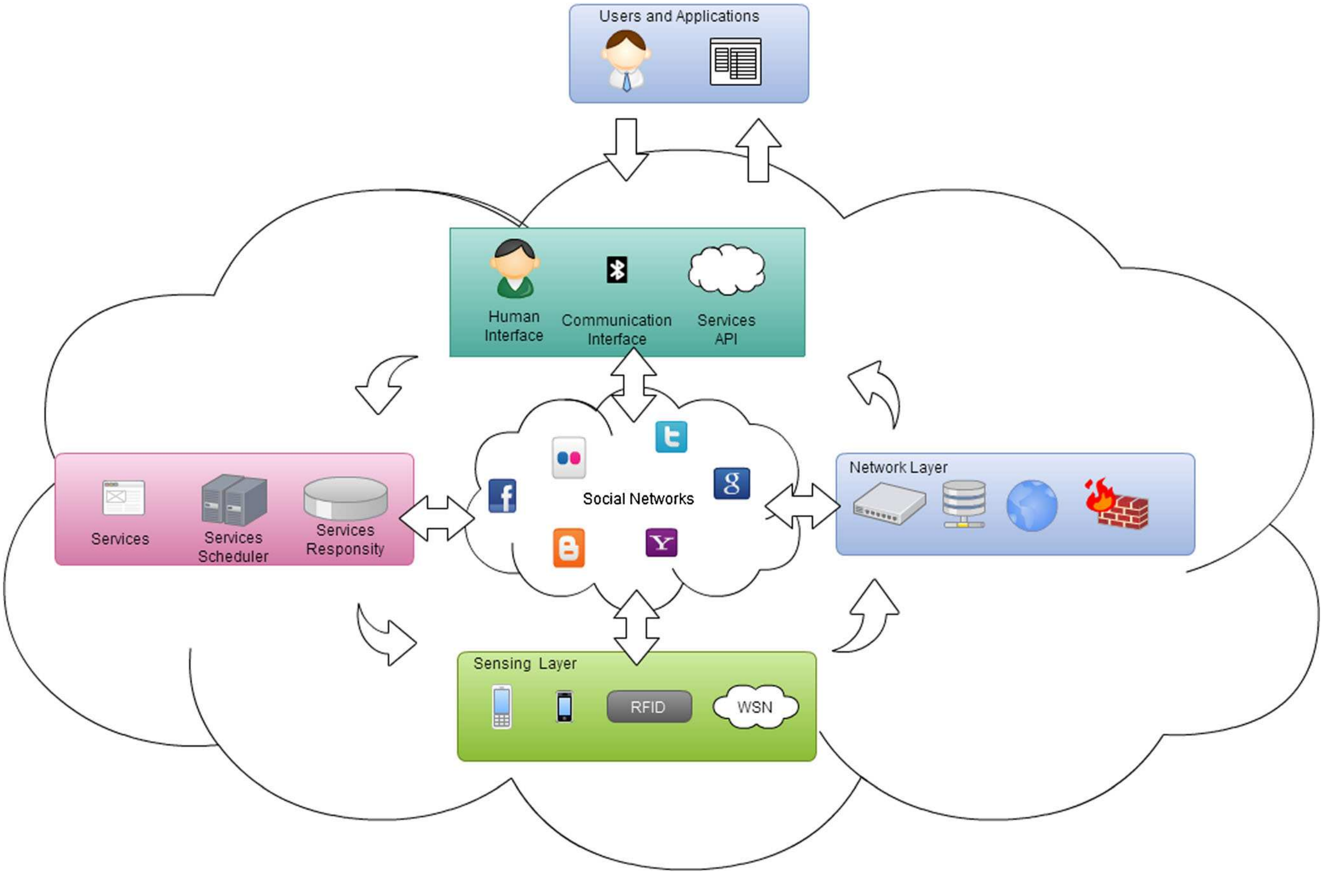


Fig. 7 Architecture for the Social IoT

matter of fact, low cost medical sensors can be connected with other things in IoT wirelessly; it becomes feasible to develop implantable sensors to monitor health conditions of patients. For example, the BLE-based technologies are applied to connect things in our daily lives such as smartphones, body sensors, home appliances and personal computers for the applications in healthcare, fitness, security, and home entertainment.

On the other hand, the rapid development of mobile devices and health applications creates a huge market for the application of IoT. Individual mobile health applications have been developed to serve healthcare tasks such as the measurement of blood pressure or recording of blood glucose (Peris-Lopez et al. 2006). A new concept named as 'Health Internet of Things (HIoT)' was proposed to exploit sensor technologies and wireless networks in monitoring medical conditions (Jara et al. 2013; Vilamovska et al. 2012).

4.4 Infrastructure

IoT has also been developed in many infrastructure areas: smart cities, environmental monitoring, and smart homes and building. In smart buildings, IoT is used to improve the quality of building and reduce wastes. The term 'Smart Cities' has been proposed as a cyber-physical ecosystem with intelligent sensors and novel services citywide. For example, the 'Sensing China' project was launched in China in June 2010. After the completion of the project, it was anticipated that everything would have an identification tag that could broadcast the information to Internet. People could track the usage of the things and monitor any variables or objects; the collected data can be utilized to reduce wastes and costs (Fielding and Taylor 2002). The successful deployment of IoT in a community or even a city can be foreseen.

4.5 Security and surveillance

In a virtual model of IoT, every physical object can find a responding counterpart that can provide services to users. Each object should be well addressed and labelled in IoT. However, the interconnections among things might bring unprecedented security issues (Roman and Lopez 2009); strong security protection is necessary to avoid attacks and malfunctions. In traditional networks, such as Internet, security protocols and privacy assurance are widely used to protect privacy and communication. However, the security techniques applied in the conventional networks are insufficient to IoT (Kang et al. 2014). Existing security protocols and mechanisms should be improved before they can be readily applied in IoT.

On the other hand, the legal and technical framework is also necessary. Due to the dynamics, uncertainties and complexity of IoT, protecting thousands even millions of intelligent things is a very challenging task. Besides, the heterogeneity greatly affects the security protection of networks that might suffer treats. Things may be under multiple threats such as data leakage and threats from external networks. Therefore, security technologies should provide the strong protection for all levels of system components at all stages: from sense layer to interface layers, from identification to service provision, and from RFID tags to IT infrastructure. In other words, information should be secured from the beginning of its existence to the end of its life cycle.

Information privacy is one of the most sensitive subjects for IoT. The need of easy accessibility of data brings the challenge to protect the information in the personalized services. To design the privacy protection mechanism, some factors should be taken into considerations. For example, the stage of use authentication involves the developments of access control and trust management (Fielding and Taylor 2002; Frenken et al. 2008; Hepp et al. 2007).

5 Open problems and future directions

5.1 Technical challenges

Although significant research efforts have been made for the development of IoT, there still are several major challenges:

(1) Design an SoA for IoT is still a big challenge, in which service-based things might suffer in terms of their performances including cost. In addition, the automated service composition based on the requirements of applications is still a challenge.
(2) From the viewpoint of network, IoT is a very complex heterogeneous network, which includes the connections among various types of networks through various communication technologies. The devices and methodologies for addressing things management is still a challenge.
(3) From the viewpoint of service, lacking of a common accepted service description language makes the services incompatible in different implementation environments. In addition, a powerful service discovery and searching engine should be very helpful to advance IoT technology.
(4) The IoT is taking place in an ICT environment and could be affected by all connected things. It is a challenge to integrate IoT with the current ICT systems.

5.2 Standardization

Standardization plays a key role in the development of IoT. The standardization of IoT aims at lowering the entry barriers to the new service providers and users; standardization can improve the interoperability and allow products or services to compete better at a higher level (Jiang et al. 2012a, b, 2013). However, the rapid growth of IoT makes the standardization difficult. The specific issues of IoT standardization include interoperability, radio access level issues, semantic interoperability, and security and privacy issues. The open standards of IoT, such as security standards, communication standards and identification standards, might be several key enablers for the expansion of the IoT technologies.

5.3 Security and privacy protection

The social acceptance of the new IoT technologies and services will strongly rely on the trustworthiness of information and protection of private data. Although a number of projects have been developed for security and privacy protection, a reliable security protection mechanism for IoT is still in demand for data confidentiality, privacy, and trust (Zheng et al. 2014a). Technically, the following issues should be addressed: (1) the definition of security and privacy from the social, legal and cultural perspectives; (2) the trust mechanism; (3) the communication security; (4) the privacy of communication and user data; and (5) security of services and applications.

5.4 Innovation in IoT environment

IoT is a complex network that might be managed by a number of stakeholders, where services should be provided publically. Therefore, open and new services or applications should be supported without creating excessive burdens for the market entry or other operation barriers. In addition, the cross-domain systems supporting innovation are still lacking.

5.5 Development strategies

IoT has been developed in different regions and nations in three main strategies:

- Opportunity investment strategy. In the nations such as US, the short or mid-term return on investment drive the development of smart energy, smart cities, and RFIDs. Through the social media network, a number of services and applications such as location-based services, augmented reality, and smartphones, are guiding the development of IoT.
- Stakeholder strategy. In the regions such as EU, a number of short-term (4–5 years) IoT projects are launched by the public-private partnerships investments. This strategy is cost-efficient and convenient, and has been widely used in some IoT applications such as healthcare, automotive, home appliances, and so on.
- Integrated strategy. In developing countries such as China, the IoT infrastructure, software, services/applications are integrated. China is focusing on the IoT based on the integrated view, and a number of state supported projects have been launched, such as "Sensing China" that integrate IoT fully into its IT infrastructures.

Although it is not yet clear which strategy is more efficient, all of them can promote IoT and its applications. However, how to synergize the strengths of available resources at a strategic level possesses another challenge.

6 Summary

In the past few years, IoT has been developed rapidly and a large number of enabling technologies have been proposed. The IoT has been the trend of the next Internet. This paper has surveyed recent progresses on IoT from the perspective of enabling technologies. In particular, the role of SoA in IoT has been introduced and related enabling technologies to implement SoA have been discussed. Existing applications of IoT have been classified into business, social networks, healthcare, infrastructure, and security and surveillance. Finally, open problems and challenges related to IoT have been discussed.

References

Alcaraz, C., & Lopez, J. (2010). A security analysis for wireless sensor mesh networks in highly critical systems. *IEEE Transactions on Systems, Man, and Cybernetics Part C: Applications and Reviews, 40*(4), 419–428.

Atzori, L., Iera, A., & Morabito, G. (2011). SIoT: giving a social structure to the internet of things. *IEEE Communication Letters, 15*(11), 1193–1195.

Bi, Z., Xu, L., & Wang, C. (2014). Internet of Things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2300338.

Bluetooth SIG. (2014). Generic Attributed Profile (GATT). *Bluetooth SIG Specification*, https://www.bluetooth.org/en-us/specification/assigned-numbers/generic-attribute-profile.

Broll, G., Rukzio, E., Paolucci, M., Wagner, M., Schmidt, A., & Hussmann, H. (2009). Perci: pervasive service interaction with the internet of things. *IEEE Internet Computing, 13*(6), 74–81.

Cai, H., Xu, L., Xu, B., Xie, C., Qin, S., & Jiang, L. (2014). IoT-based configurable information service platform for product lifecycle management. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306391.

Chi, Q., Yan, H., Zhang, C., Pang, Z., & Xu, L. (2012). A reconfigurable smart sensor interface for industrial WSN in IoT environment. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306798.

Ciganek, A., Haseman, W., & Ramamurthy, K. (2014). Time to decisions: the drivers of innovation adoption decisions. *Enterprise Information Systems, 8*(2), 279–308.

Dada, A., & Thiesse, F. (2008). Sensor applications in the supply chain: the example of quality-based issuing of perishables. *LNCS, 4952*, 140–154.

Deng, R. H., Li, Y., Yung, M., & Zhao, Y. (2010). A new framework for RFID privacy. *LNCS, 6345*, 1–18.

EPCglobal. (2013). Radio-frequency identity protocols class-1 generation-2 uhf rfid protocol for communications at 860–960 MHz, Version 1.2.0, http://www.gs1.org/gsmp/kc/epcglobal/uhfc1g2/uhfc1g2_1_1_0-standard-20071017.pdf.

ETSI. (2013). The European Telecommunications Standards Institute, [cited 2013 May 20]; available from http://www.etsi.org/.

Fan, Y., Yin, Y., Xu, L., Zeng, Y., & Wu, F. (2014). IoT based smart rehabilitation system. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2302583.

Fang S., Xu, L., Zhu, Y., Ahati, J., Pei, H., Yan, J., et al. (2014). An integrated system for regional environmental monitoring and management based on Internet of Things. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2302638.

Fielding, R. T., & Taylor, R. N. (2002). Principled design of the modern web architecture. *ACM Transactions Internet Technology, 2*(2), 115–150.

Fleisch, E. (2013) What is the Internet of things? *[cited 2013 May 20]; available from* http://www.im.ethz.ch/education/HS10/AUTOIDLABS-WP-BIZAPP-53.pdf.

Floerkemeier, C., Roduner, C., & Lampe, M. (2007). RFID application development with the Accada middleware platform. *IEEE Systems Journal, 1*(2), 82–94.

Frenken, T., Spiess, P., & Anke, J. (2008). A flexible and extensible architecture for device-level service deployment. *LNCS, 5377*, 230–241.

Gama, K., Touseau, L., & Donsez, D. (2012). Combining heterogeneous service technologies for building an Internet of Things middleware. *Computer Communications, 35*(4), 405–417.

Guinard, D., Trifa, V., Pham, T., & Liechti, O. (2009). Towards physical mashups in the web of things. *Proc. IEEE Sixth International Conference on Networked Sensing Systems (INSS 09),* Pittsburgh, PA, pp.196–199.

Guinard, D., Trifa, V., Karnouskos, S., & Spiess, P. (2010). Interacting with the SoA-based internet of things: discovery, query, selection, and on-demand provisioning of web services. *IEEE Transactions on Service Computing, 3*(3), 223–235.

Guo, J., Xu, L. D., Xiao, G., & Gong, Z. (2012). Improving multilingual semantic interoperation in cross-organizational enterprise systems through concept disambiguation. *IEEE Transactions on Industrial Informatics, 8*(3), 647–658.

Hachani, S., Gzara, L., & Verjus, H. (2013). A service-oriented approach for flexible process support within enterprises: application on PLM systems. *Enterprise Information Systems, 7*(1), 79–99.

He, W., & Xu, L. (2014). Integration of distributed enterprise applications: a survey. *IEEE Transactions on Industrial Informatics, 10*(1), 35–42.

He, W., Yan, G., & Xu, L. (2014) Developing vehicular data cloud services in the IoT environment. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2299233.

Hepp, M., Siorpaes, K., & Bachlechner, D. (2007). Harvesting Wiki consensus: using wikipedia entries as vocabulary for knowledge management. *IEEE Internet Computing, 11*(5), 54–65.

Hernandez-Castro, J. C., Tapiador, J., Peris-Lopez, P., & Quisquater, J. (2013). Cryptanalysis of the SASI ultra-light weight RFID authentication protocol, *[cited 2013 May 20]; available from* http://arxiv.org/abs/0811.4257.

Hunter, D., Yu, H., Pukish, M., Kolbusz, J., & Wilamowski, B. (2012). Selection of proper neural network sizes and architectures-a comparative study. *IEEE Transactions on Industrial Informatics, 8*(2), 228–240.

IERC. (2013). Coordinating and building a broadly based consensus on the ways to realise the internet of things in Europe, *[cited 2013 May 20]; available from* http://www.internet-of-things-research.eu/pdf/Poster_IERC_A0_V01.pdf.

Ilic, A., Staake, T., & Fleisch, E. (2009). Using sensor information to reduce the carbon footprint of perishable goods. *IEEE Pervasive Computing, 8*(1), 22–29.

ITU. (2013). The internet of Things, International Telecommunication Union (ITU), *Internet Report [cited 2013 May 20]; available from* http://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-IR.IT-2005-SUM-PDF-E.pdf.

Jara, A. J., Zamora-Izquierdo, M. A., & Skarmeta, A. F. (2013). Interconnection framework for mHealth and remote monitoring based on the internet of things. *IEEE Journal on Selected Areas in Communications, 31*(9), 47–65.

Jardim-Goncalves, R., Grilo, A., Agostinho, C., Lampathaki, F., & Charalabidis, Y. (2013). Systematisation of interoperability body of knowledge: the foundation for enterprise interoperability as a science. *Enterprise Information Systems, 7*(1), 7–32.

Jiang, H., Zhao, S., Zhang, Y., & Chen, Y. (2012a). The cooperative effect between technology standardization and industrial technology innovation based on Newtonian mechanics. *Information Technology and Management, 13*(4), 251–262.

Jiang, H., Zhao, S., Qiu, S., & Chen, Y. (2012b). Strategy for technology standardization based on the theory of entropy. *Information Technology and Management, 13*(4), 311–320.

Jiang, H., Zhao, S., Wang, X., & Bi, Z. (2013). Applying electromagnetic field theory to study the synergistic relationships between technology standardization and technology development. *Systems Research and Behavioral Science, 30*(3), 272–286.

Jiang, L., Xu, L., Cai, H., Jiang, Z., Bu, F., & Xu, B. (2014). An IoT oriented data storage framework in cloud computing platform. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306384.

Joshi, G. P., & Kim, S. W. (2013). Survey, nomenclature and comparison of reader anti-collision protocols in RFID, *IETE Technical Review, [cited 2013 May 20]; available from* http://tr.ietejournals.org/text.asp?2008/25/5/285/44659.

Juels, A. (2006). RFID security and privacy: a research survey. *IEEE Selected Areas in Communications, 24*(2), 381–394.

Kang, K., Pang, Z., Xu, L., Ma, L., & Wang, C. (2014). An interactive trust model for application market of the Internet of Things. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306799.

Karpischek, S., Michahelles, F., Resatsch, F., & Fleisch, E. (2009). Mobile sales assistant – an NFC-based product information system for retailers. *Proceedings of the First International Workshop on Near Field Communications 2009*, Hagenberg, Austria, 2009, pp.20–23.

Kataev, M., Bulysheva, L., Emelyanenko, A., & Emelyanenko, V. (2013). Enterprise systems in Russia: 1992–2012. *Enterprise Information Systems, 7*(2), 169–186.

Kirtsis, D. (2011). Closed-loop PLM for intelligent products in the era of the internet of things. *Computer-Aided Design, 43*(5), 479–501.

Klair, D. K., Chin, K.-W., & Raad, R. (2010). A survey and tutorial of RFID anti-collision protocols. *IEEE Communications Surveys and Tutorials, 12*(3), 400–421.

Kranenburg, V. (2013). Moscow futurodesign lab co-create urban intelligence: designing smart interfaces between people and city, *[cited 2013 May 20]; available from* http://www.theinternetofthings.eu/content/moscow-futurodesign-laboratory-workshop-co-create-urban-intelligence-designing-smart-interfa.

Kranenburg, R., & Anzelmo, E. (2011) The Internet of Things, *1st Berlin Symposium on Internet and society*, Oct 25–27, 2011.

Krapelse, H. J. (2013). RFID application in healthcare – scoping and identifying areas for RFID deployment in healthcare delivery, RAND Europe. *[cited 2013 May 20]; available from* http://www.rand.org/pubs/technical_reports/TR608z1.html.

Lam, C., & Ip, W. (2012). An improved spanning tree approach for the reliability analysis of supply chain collaborative network. *Enterprise Information Systems, 6*(4), 405–418.

Li, L. (2012). Effects of enterprise technology on supply chain collaboration: analysis of China-linked supply chain. *Enterprise Information Systems, 6*(1), 55–77.

Li, L. (2013). Technology designed to combat fakes in the global supply chain. *Business Horizons, 56*(2), 167–177.

Li, L., & Liu, J. (2012). An efficient and flexible web services-based multidisciplinary design optimisation framework for complex engineering systems. *Enterprise Information Systems, 6*(3), 345–371.

Li, S., Xu, L., Wang, X., & Wang, J. (2012a). Integration of hybrid wireless networks in cloud services oriented enterprise information systems. *Enterprise Information Systems, 6*(2), 165–187.

Li, Y., Hou, M., Liu, H., & Liu, Y. (2012b). Towards a theoretical framework of strategic decision, supporting capability and information sharing under the context of Internet of Things. *Information Technology and Management, 13*(4), 205–216.

Li, Q., Wang, Z., Li, W., Li, J., Wang, C., & Du, R. (2013a). Applications integration in a hybrid cloud computing environment: modelling and platform. *Enterprise Information Systems, 7*(3), 237–271.

Li, S., Xu, L., & Wang, X. (2013b). Compressed sensing signal and data acquisition in wireless sensor networks and internet of things. *IEEE Transactions on Industrial Informatics, 9*(4), 2177–2186.

Li, L., Li, S., & Zhao, S. (2014a). QoS-aware scheduling of service-oriented Internet of Things. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306782.

Li, S., Oikonomou, G., Tryfonas, T., & Chen, TM. (2014). A distributed consensus algorithm for decision-making in service-oriented Internet of Things. *IEEE Transactions on Industrial Informatics.* doi:10.1109/TII.2014.2306331.

Malatras, A., Asgari, A., & Bauge, T. (2008). Web enabled wireless sensor networks for facilities management. *IEEE Systems Journal, 2*(4), 500–512.

Marry, W. (2013). Disruptive civil technologies six technologies with potential impacts on us interests out to 2025, *[cited 2013 May 20]; available from* http://swemgovdocs.blogs.wm.edu/.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: vision, applications and research challenges. *Ad hoc Networks, 10*(7), 1497–1516.

Mitrokotsa, A., Rieback M. R., & Tanenbaum, A. S. (2013). Classifying RFID attacks and defences. *[cited 2013 May 20]; available from* http://www.cs.vu.nl/~ast/publications/isf-2009.pdf.

Mutti, C., & Floerkemeier, C. (2008) CDMA-based RFID systems in dense scenarios: Concepts and challenges. *Proc. IEEE Int. Conf. on RFID*, Las Vegas, NV, pp. 215–222.

Panetto, H., & Cecil, J. (2013). Editorial Information systems for enterprise integration, interoperability and networking: theory and applications. *Enterprise Information Systems, 7*(1), 1–6.

Pautasso, C., & Wilde, E. (2009). Why is the web loosely coupled? A multifaceted metric for service design. *Proc. 18th International World Wide Web Conference (WWW 09)*, pp. 911–920.

Peris-Lopez, P., Hernandez-Castro, J. C., Estevez-Tapiador, J. M., & Ribagorda, A. (2006). M^{2}AP: a minimalist mutual-authentication protocol for low-cost RFID tags. *Lecture Notes in Computer Science, 4159*, 912–923.

Pretz, K. (2013). The Next Evolution of the Internet. *[cited 2013 May 20]; available from* http://theinstitute.ieee.org/technology-focus/technology-topic/the-next-evolution-of-the-internet.

Ren, L., Zhang, L., Tao, F., Zhang, X., Luo, Y., & Zhang, Y. (2012). A methodology towards virtualisation-based high performance simulation platform supporting multidisciplinary design of complex products. *Enterprise Information Systems, 6*(3), 267–290.

Roman, R., & Lopez, J. (2009). Integrating wireless sensor networks and the internet: a security analysis. *Internet Research, 19*(2), 246–259.

Roman, R., Alcaraz, C., Lopez, J., & Sklavos, N. (2011). Key management systems for sensor networks in the context of the Internet of Things. *Computers and Electrical Engineering, 37*(2), 147–159.

Tan, W., Xu, W., Yang, F., Xu, L., & Jiang, C. (2013). A framework for service enterprise workflow simulation with multi-agents cooperation. *Enterprise Information Systems, 7*(4), 523–542.

Tao, F., Cheng, Y., Xu, L., Zhang, L., & Li, B. (2014a). CCIoT-CMfg: cloud computing and Internet of Things based cloud manufacturing service system. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306383.

Tao, F., Zuo, Y., Xu, L., & Zhang, L. (2014b). IoT based intelligent perception and access of manufacturing resource towards cloud manufacturing. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306397.

Ulmer, J., Belaud, J., & Le Lann, J. (2013). A pivotal-based approach for enterprise business process and IS integration. *Enterprise Information Systems, 7*(1), 61–78.

van Looy, A., Backer, M., & Poels, G. (2014). A conceptual framework and classification of capability areas for business process maturity. *Enterprise Information Systems, 8*(2), 188–224.

Vermesan, O. (2013). CERP-IoT strategic research agenda. *[cited 2013 May 20]; available from* http://www.rfid-in-action.eu/cerp/.

Vilamovska, A. M., Hatziandreu, E., Schindler, H. R., Oranje-Nassau, C. V., Vries, H., Krapels, J. (2012). Study on the requirements and options for RFID application in healthcare Identifying areas for Radio Frequency Identification deployment in healthcare delivery: a review of relevant literature. *Directorate General Information Society and Media, European Commission*. Santa Monica, CA, USA: The RAND Corporation.

Viriyasitavat, W., Xu, L., & Viriyasitavat, W. (2014a). Compliance checking for requirement-oriented service workflow interoperations. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2301132.

Viriyasitavat, W., Xu, L., & Viriyasitavat, W. (2014b). A new approach for compliance checking in service workflows. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2301143.

Wang, C. (2012). Editorial advances in information integration infrastructures supporting multidisciplinary design optimization. *Enterprise Information Systems, 6*(3), 265.

Wang, X., & Xu, X. (2012). DIMP: an interoperable solution for software integration and product data exchange. *Enterprise Information Systems, 6*(3), 291–314.

Wang, F., Ge, B., Zhang, L., Chen, Y., Xin, Y., & Li, X. (2013). A systems framework of security management in enterprise systems. *Systems Research and Behavioral Science, 30*(3), 287–299.

Wang, C., Bi, Z., & Xu, L. (2014). IoT and cloud computing in automation of assembly modelling systems. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2300346.

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., & Borriello, G. (2009). Building the internet of things using RFID: the RFID ecosystem experience. *IEEE Internet Computer, 13*(3), 48–55.

Wilamowski, B. (2010). Challenges in Applications of Computational Intelligence in Industrial Electronics. *Proceedings of IEEE International Symposium on Industrial Electronics (IEEE ISIE 2010)*, Bari, Italy, July 4–7, 2010, pp. 15–22.

Xiao, G., Guo, J., Xu, L., Gong, Z. (2014). User interoperability with heterogeneous IoT devices through transformation. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306772.

Xing, Y., Li, L., Bi, Z., Wilamowska-Korsak, M., & Zhang, L. (2013). Operations research (OR) in service industries: a comprehensive review. *Systems Research and Behavioral Science, 30*(3), 300–353.

Xu, L. (2011a). Enterprise systems: state-of-the-art and future trends. *IEEE Transactions on Industrial Informatics, 7*(4), 630–640.

Xu, L. (2011b). Information architecture for supply chain quality management. *International Journal of Production Research, 49*(1), 183–198.

Xu, L., & Viriyasitavat, W. (2014). A novel architecture for requirement-oriented participation decision in service workflows. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2301378.

Xu, L. D., Viriyasitavat, W., Ruchikachorn, P., & Martin, A. (2012a). Using propositional logic for requirements verification of service workflow. *IEEE Transactions on Industrial Informatics, 8*(3), 639–646.

Xu, L. D., Wang, C., Bi, Z., & Yu, J. (2012b). AutoAssem: an automated assembly planning system for complex products. *IEEE Transactions on Industrial Informatics, 8*(3), 669–678.

Xu, B., Xu, L., Cai, H., Xie, C., Hu, J., & Bu, F. (2014). Ubiquitous data accessing method in IoT-based information system for emergency medical services. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306382.

Zheng, X., Martin, P., Brohman, K., & Xu, L. (2014a). CLOUDQUAL: a quality model for cloud services. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2306329.

Zheng, X., Martin, P., Brohman, K., & Xu, L. (2014b). Cloud service negotiation in IoT environment: a mixed approach. *IEEE Transactions on Industrial Informatics*. doi:10.1109/TII.2014.2305641.

Shancang Li received his B.S. and M.S. degrees in mechanical engineering and Ph.D. degree in computer science from Xi'an Jiaotong University, China, in 2001, 2004 and 2008, respectively. He is currently with the Faculty of Engineering at the University of Bristol and a member of the Cryptography Research Group. His current research interests include mobile security, wireless sensor networks, Internet of Things, and applications of wireless technologies.

Li Da Xu serves as the Founding Chair of IFIP TC8 WG8.9, the Founding Chair of the IEEE SMC Society Technical Committee on Enterprise Information Systems. His affiliations include the Institute of Computing Technology, the Chinese Academy of Sciences, the University of Science and Technology of China, Shanghai Jiao Tong University, and Old Dominion University, USA.

Shanshan Zhao received both her B.S. and M.S. degrees in mechanical engineering from Xi'an Technological University in 2001 and 2004, respectively. She earned her Ph.D. degree in mechanical engineering from Xi'an Jiaotong University in 2008. She is currently an academic visitor at the University of the West of Scotland, UK. Her current research interests include intelligent information system, IoT, intelligent manufacturing, and augmented reality.