Frontiers of Engineering Management
DOI 10.15302/J-FEM-2016039

ENGINEERING MANAGEMENT THEORIES AND METHODOLOGIES

Li Da Xu

An Internet-of-Things Initiative for One Belt One Road (OBOR)

Abstract A wide range of industrial Internet of Things (IoT) applications have been developed and deployed in recent years. IoT has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of RFID, wireless, mobile and sensor devices. 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. As IoT has received support from governments and businesses across the globe, IoT will also greatly impact One Belt One Road (OBOR) in foreseeable future.

Keywords: Internet of Things (IoT), RFID, Wireless Sensor Networks, Near Field Communications, ICT

1 Introduction

The Internet of Things (IoT) is a term that has been introduced in recent years to describe objects that are able to communicate via the Internet. Haller, Kanouskos, and Schroth (2009) have provided the following definition: "A world where physical objects are seamlessly integrated into the information network, and where they, the physical objects, can become active participants in business processes. Services are available to interact with these 'smart objects' over the Internet, query their state and any information associated with them, taking into account security and privacy issues."

With the assumption that objects have digital functionality and can be identified and tracked automatically, IoT gives immediate access to information about the physical world and the objects and leads to innovative services with high efficiency. IoT is an emerging Internet-based information architecture, and is becoming a foundation for connecting things, sensors, actuators, and other smart technologies. In past years, IoT has changed business and industries.

The history of IoT has been reviewed by van Kranenburg and Bassi (2012). Two arguable pioneers who coined the term of Internet of Things (IoT) are Bill Gates in his book entitled "The Road Ahead" in 1995 and Kevin Ashton and Neil Gershenseld at MIT in 1999 for their research at Auto-OD Center (http://postscapes.com/internet-of-things-history; K. Ashton, "That 'Internet of Things' thing," http://www.rfidjournal.com/article/view/4986). This concept was further elaborated and noted that the era of the pervasive and ubiquitous computing is coming.

The first IoT conference was held in Europe in 2006–2008. Over 50 member companies, including Bosch, Cisco, Fujitsu, Google, Intel, SAP, and Sun formed an alliance to launch the Internet Protocol for Smart Object (IPSO) and to enable the IoT. CASAGRAS (Coordination and Support Action for Global RFID-related Activities and Standardisation) is a European Framework 7 project. It was considered as the international effort concerning regulations, standardization, and other requirements for realizing IoT. During that time, IoT was not yet a tangible reality, but was rather the prospective vision of a number of technologies that, combine together, could drastically change the way in which our society functions in the coming decade.

As mentioned above, the IoT was first co-proposed by Kevin Ashton to refer to uniquely identifiable interoperable connected objects with radio-frequency identification (RFID) technology, which then was being rapidly developed. Intelligent sensing and wireless communication technologies have become part of the IoT, and new challenges and research horizons have emerged. In 2005, ITU described IoT as 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" (ITU, 2005). It has been agreed that the IoT was born in 2008–2009.The IoT can be considered as a superset of connecting devices that are uniquely identifiable by existing near field communication (NFC) technologies. The words "Internet" and "Things" describe

Manuscript received May 15, 2016; accepted August 1, 2016

Li Da Xu (✉)
Old Dominion University, Norfolk, VA 23529, USA
Email: lxu@odu.edu

a world-wide inter-connected network based on sensory, communication, networking, and information processing technologies, which might be the new version of information and communications technology (ICT). *Figure 1* shows the evolution of IoT and the closely related technologies (Xu, 2014).

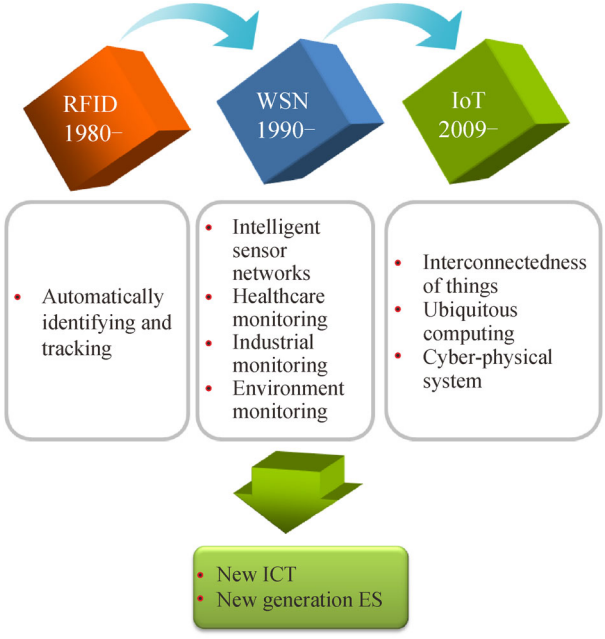

Figure 1. IoT, related technology and their impact on new ICT.

The IoT was initiated by the use of RFID technology, which is increasingly being used in diverse industrial sectors. The emerging wirelessly intelligent sensory technologies have significantly extended the sensory capabilities of devices, and therefore the original concept of IoT has been extended to ambient intelligence and autonomous control. To date, a number of technologies are involved in the IoT, such as RFID, intelligent sensing, WSN, near field communications (NFC), wireless communications, cloud computing, and others. All of these make the IoT becoming an evolving computing concept (*Figure 2*).

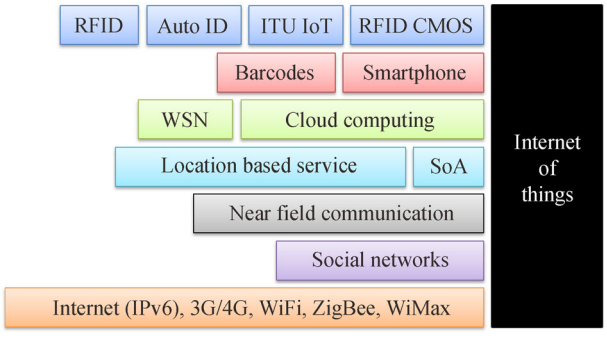

Figure 2. IoT-related technologies.

There are several different definitions for IoT, depending on the technology and implementation of the ideas that are moving forward. However, the basic idea of the IoT is that objects have a unique way of identification in virtual representation, which makes it possible that all of the things around us can be identified by the things around them. In IoT, for all things, data can be exchanged if needed, and data can be processed according to predefined schemes. The future of the Internet will consist of heterogeneous connected devices that will further extend the borders of the physical entities and virtual components world-wide. IoT will empower the connected things with new capabilities and will create many new real-world applications (Xu, 2015; Xu, He, & Li, 2014).

IoT can be of significance in a variety of industrial sectors, including the manufacturing sector. A manufacturing system consists of system components and their related interactions. Each component has an information unit for controlling the component. The impact of IoT on the manufacturing systems can be significant:

– Ubiquitous computing for manufacturing enterprises

Everything can be connected, so that the data can be acquired promptly and can be readily shared by all of the units. This makes it possible to integrate manufacturing resources with a much broader scope, including the resources within the organization and the inter-organizational resources from partners in the supply chain.

– Facilitating systems level optimization

The manufacturing system is targeted for a system level balance between flexibility and efficiency. On the one hand, the manufacturing system is modularized, and each module is optimized at the module level for its specified function; on other hand, the selection of modules and the assembling topologies offer the flexibility of a system configuration to meet various functions at the system level. The topology of system configuration can be optimized with the widely available information over the system.

– Real-time full control

Traditional enterprise systems are good for planning and scheduling which are more at the macro level. Such systems will be integrated with the real-time control systems at the micro level. Online data acquisition systems are not only used to provide real-time control at the machine level, but also to provide feedback at the macro level about any changes (and/or uncertainties), so that the plans and schedules can be adjusted to accommodate the changes and uncertainties promptly. In the MES (Manufacturing Execution System), with the emergence of IoT, it is expected to integrate with the online process control eventually (Logeais, 2008).

– Customer-empowered by real-time data availability

Besides the privilege of comparing products from different vendors, IoT allows customers to personalize the product requirements, and to place and change orders in real-time based on their needs. The satisfaction level of customers can be greatly enhanced.

IoT can be aligned with the architecture of a manufacturing system. *Figure 3* shows the relationship between the IoT and future manufacturing systems.

2 Enabling technologies

The characteristics of IoT include (1) the pervasive sensing of objects; (2) the integration of heterogeneous hardware and software; (3) the extreme large scale of its nodes. The existing literature has introduced the state of the art of the enabling technologies for IoT including architecture frameworks, standardizations, modeling techniques, communication protocols, identification and resolution frameworks, security, and privacy. To clarify the progress made on protocols, algorithms, and proposed solutions and to determine what are the unsolved issues, Atzori, Iera, and Morabito (2010) surveyed key enabling technologies for IoT in communication, identification, tracking, wired and wireless sensors, and distributed intelligence for smart objects.

2.1 Ubiquitous computing

IoT is known for its ubiquitous computing and ambient intelligence. IoT is a concept in which the virtual world of information technology integrates seamlessly with the real world of things (Uckelmann, Harrison, & Michahelles, 2011). Guinard, Trifa, Karnouskos, Spiess, and Savio (2010) indicated two trends with respect to the devices. They are: (1) the hardware is getting smaller, less expensive, and more capable; and (2) the software industry is moving toward service-oriented approaches and especially for the business software, new complex applications are based on the collaboration of other services. In IoT, smart things/objects are expected to be active participants in communication processes; they are enable to interact among themselves, reacting autonomously to the sensed environment, and trigger actions and services with or without direct human intervention (Vermesan, 2009).

The trends for smart devices are: (1) applying data fusion and computation, for the scientific analysis of big data; (2) integrating devices, systems, and organizations for information sharing and real-time monitoring; (3) using anything / anytime / anywhere communication to sense, capture, measure, and transfer data; and (4) vertically, improving upon the performance of an individual device. They are becoming versatile, powerful, and intelligent to deal with the changes and complexity. Horizontally, a simple device without the functions of computation can be integrated; abundant information can be acquired for real-time processing.

2.2 RFID

RFID and WSN are the cornerstones of IoT. A simple RFID system is composed of an RFID and an RFID reader tag. Due to its capacity to identify, track, and trace, the RFID system is increasingly being used. RFID systems can provide precise real-time information about the involved devices, so they are successfully used in various industrial sectors. They can simplify operations processes, improve efficiency, and reduce costs. RFID's industrial applications are increasing significantly. Based on incomplete recent data, of all RFID-based applications, approximately, 56% were used for access control, 29% for supply chain, 25%

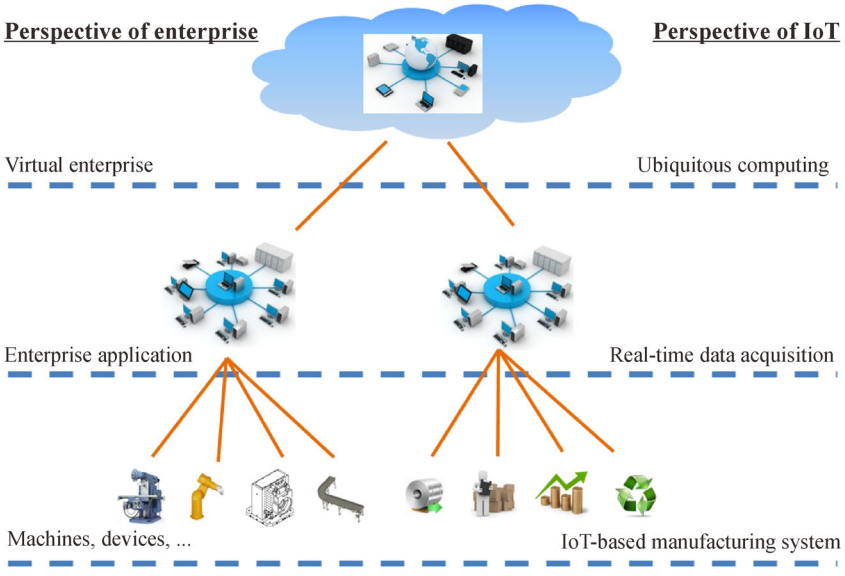

Figure 3. IoT for future manufacturing.

for motorway tolls, 24% for security control, 21% for product control, and 15% for asset management.

The emerging intelligent sensory technologies, including those related to infrared, γ-ray, pressure, vibration, electromagnetic, biosensor, and X-ray, can deliver all of the acquired information connected to IoT for analysis purposes. Several hardware solutions for RFID-based sensors have been proposed. The integration of data acquired by intelligent sensors with data delivered by RFIDs can make IoT capable of facilitating industrial information processing.

2.3 Wireless Sensor Networks (WSN)

The IoT is a network of all physical objects with identifiable IDs, which is based on Internet. WSN is attractive for many applications due to the fact that no wire connections for communication are required. Most of the ongoing WSN research focuses on energy-efficient routing, aggregation, and data management algorithms. One of the major challenges is to optimize the deployment of the large-scale systems and the integration of data from a large quantity of sources. The wireless network is an important infrastructure: (1) IPv6 makes it possible to connect an unlimited number of devices; (2) Wifi and Wimax provide high-speed and low-cost communication; (3) Zigbee/bluetooth/RFID provides the communication in low-speed and local communication; and (4) the mobile platform offers anything / anytime / anywhere communications.

2.4 RFID and WSN

Due to the needs of the continuous monitoring and controlling of everything, everywhere, computing systems are required to be ubiquitous and distributed. Some researchers have predicted that the computing technology's next revolution will be the widespread use of wireless computing and communication devices.

RFID and WSN represent two complementary technologies. RFID technology has advanced tremendously in recent years, as is evidenced by RFID's applications in various industrial sectors. RFID is capable of detecting and identifying objects that may form challenges to conventional sensor technologies. RFID tags are less expensive when compared to sensor nodes. It is preferable to use RFID tags instead of the sensor nodes of a WSN in many places; however, an RFID tag does not include information about the states of the targeted objects or the environment. Integrating with a WSN enables RFID readers and tags to have intelligence and allows an RFID network to be operated in multi-hop fashion. Many applications have been proposed to use RFID and WSN for various purposes including using RFID and WSN for power facility management, and integrating RFID into service infrastructures to improve traceability. Researchers have investigated the use of RFID and WSN with ZigBee; electronic labels were attached to the sensors to integrate the RFID with the WSN. Researchers have argued that an integration of RFID and WSNs is of great value in ensuring the accurate and timely localization and tracking of objects.

2.5 Cloud computing

Advances in automatic identification, wireless communications, intelligent sensing, and distributed data processing have narrowed the gap between the notion of ubiquitous computing and the world of networked sensing and intelligent 'things'. Despite the consensus about the great potential of the concept and the significant progress in a number of enabling technologies, there is a general lack of an integrated vision on how to realize it.

Cloud computing is a large-scale and low cost processing method which is based on an IP connection for computation and storage. In 2001, Google CEO Eric Schmidt proposed the Cloud Computing concept. In 2003, Google used cloud computing based on the Google appEngine (GAE), which was a large-scale application of PaaS. In 2006, Amazon announced the elastic computing server (EC2) as a successful application of IaaS mode. In 2007, China Mobile launched a plan to promote cloud computing.

The characteristics of cloud computing include the following (*Figure 4*):

- Ubiquitous network access: use is available through standard Internet-enabled devices;
- Location-independent resource pooling: processing and storage demands are balanced across a common infrastructure with no particular resource assigned to any individual user;
- On-demand self-service: individuals can set themselves up without requiring anyone's help;
- Rapid elasticity: consumers can increase or decrease capacity at will;
- Pay per use: consumers are charged fees based on their usage of a combination of computing power, bandwidth use, and/or storage.

Cloud computing is needed to address the dynamic and exponentially growing demands for real-time reliable data processing of IoT such as: edge technologies for sensors and actuators, identifications that allow an 'object' to participate in the IoT; interoperable service-oriented middleware and architectures to share real-world data among heterogeneous devices; networking technologies for wired and wireless networking to interconnect 'things'; decision-making application services that store, integrate, and process dynamic data streams from devices with limited computational capacity on a real-time basis. Cloud infrastructures also provide the storage and computing capabilities to address the IoT application services' needs to process big data. However, cloud computing is still far from mature, even without the considerations of standardization and interoperation. *Figure 4* shows the

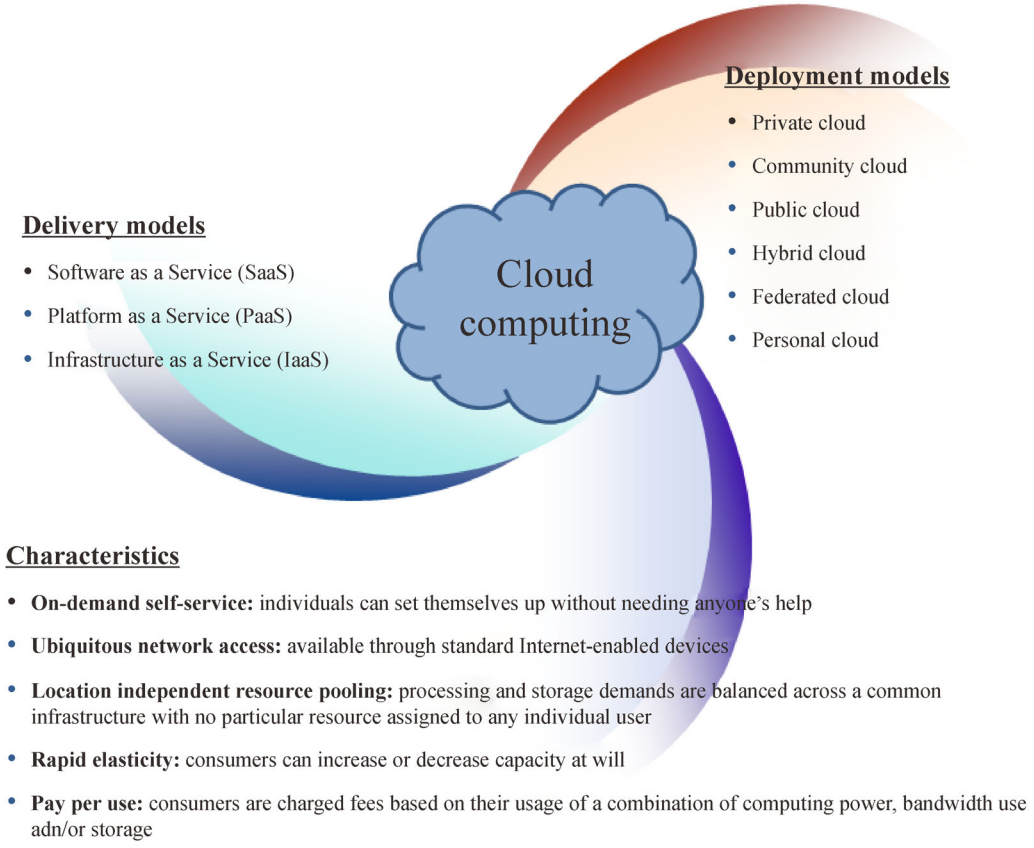

Figure 4. Characteristics, delivery and deployment models of cloud computing.

characteristics, delivery, and deployment models of cloud computing.

2.6 More on the enabling technologies of IoT

2.6.1 Communication technologies in IoT

Physical objects involve very diverse hardware specifications in aspects of communication, memory, data storage capacity, computation, and transmission power. All of these things can be well organized through networks that involve all kinds of communication technologies. For example, devices can be well organized by using a gateway for the communication over the Internet.

IoT involves a number of heterogeneous networks, such as WSNs, wireless mesh networks, mobile networks, WLAN, etc., with the services layer collecting information about all the things through the networks. These networks help things in IoT perform complex functions such as information exchange, computation, and others. The reliable communication between the gateway and the things can be helpful for centralized decision-making through IoT. The gateway is able to run complicated optimization algorithms locally. Therefore, the computational complexity is shifted from the things to the gateway, and a global optimal route and computational parameter values for the gateways can be obtained. This is feasible as the resulting complexity is affordable for standard gateway hardware capabilities.

Hardware capabilities and the communication requirements among different types of devices can be very different. From a hardware perspective, things can have very different memory, communication, and computation capabilities. Things can have very different Quality of Service (QoS) requirements in terms of delay, energy consumption, and reliability. For example, minimizing the energy usage for communication/computation purposes is a major constraint for those battery-powered devices without efficient energy-related techniques. On the contrary, this energy constraint is not critical for devices with a power supply connection.

IoT would also greatly benefit from the existing protocols in Internet such as IPv6, since this would make it possible to directly address any number of things needed through the Internet. The commonly used communication protocol 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 and IPv6

Details of the communication technologies can be found in Table 1.

2.6.2 Networks involved in IoT

There exist many cross-layer protocols for Wireless Sensor Networks (WSNs), Wireless Mesh Networks (WMNs), and Ad Hoc Networks (AHNs). However, they cannot be applied to the IoT for several reasons. First, the heterogeneity of the IoT means that things have largely diverse hardware capabilities, different QoS requirements, and individual characters. On the contrary, in WSN, nodes usually have very similar hardware specifications, common communication requirements, and a shared goal. Second, the Internet is involved in the IoT network architecture, from which it inherits a centralized and hierarchical architecture. In comparison, in WSN, WMN, and AHN, highly flat network architectures are considered, in which nodes communicate in a multi-hop fashion, and the Internet is not involved.

2.6.3 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. Its service-oriented architecture can promote encapsulation of services; by doing this, the details of services, such as the implementation of services and the protocols used, can be hidden from the concept of services. This makes it possible to decouple between components in the system and therefore to hide the heterogeneity from the service consumers. SOA-IoT allows applications to use the heterogonous objects as compatible services. On the other hand, the dynamic nature of IoT applications requires IoT to provide reliable and consistent service. There are a variety of service management architectures contributing to the IoT, such as the RFID edge controller in IBM's architecture.

2.6.4 Dynamic service composition in IoT

IoT has a service-oriented and context-aware architecture and is a subset of the future Internet; every virtual and physical object can communicate with every other object giving seamless service to other entities. Millions of devices in IoT need to be interoperable. The service-oriented IoT can make each component offer its functionalities as standard services, which might significantly increase the efficiency of both devices and networks that are involved in IoT. To better organize the services that the real objects provide, each service can find a virtual responding element in IoT.

In a service-oriented IoT, services can be created and deployed according to the steps as: (1) developing services composition platforms; (2) abstracting the devices' functionalities and communication capabilities; and (3) provision of a common set of services. The IoT makes it possible to build each real object a mirror in the IoT.

A service is a collection of data and associated behaviors that accomplish a particular function or feature of a device or of portions of a device. A service may reference other primary or secondary services and/or a set of characteristics that make up the service. 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 service basic component and can be included by another service. A secondary service can provide auxiliary functionality to the primary service or to other secondary services. In IoT, each service may consist of one or more characteristics which

Table 1

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
Wi-Max	70 Mbps	2–11GHz	50 km
UMTS/CDMA/EDGE/MBWA	2 Mbps	896	~

define the service data structure, permission, descriptors, and other attributes. In the newly released Bluetooth SIG specification, a service can be easily described with XML for easy exchange with other middleware. The OSGi platform is able to provide applications with a dynamic SOA architecture which can effectively enable the deployment of smart service. The advances in software industry show that the OSGi is an effective modular platform for service deployment in many applications. In IoT, the service composition based on the OSGi platform can be implemented by Apache Felix iPoJo.

2.6.5 Integration of different service technologies

The service-oriented IoT aims at developing an effective architecture for service operations in an IoT, which extends the pre-existing architectures of IoT and takes the unique characteristics of service-oriented IoT into consideration. The knowledge about services in the service-oriented IoT should be well represented to support discovery, detection, classification, composition, and testing.

The architecture of IoT can contain three basic layers: the application layer, the network layer, and the sensing layer. (1) 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 modeling components for IoT-aware business processes which can be executed in the process execution components; (2) The middle layer contains three basic components: service entity arrangements, virtual entity and information, and resources. The arrangement and access of IoT services to external entities and services is organized by the service entity arrangements component. The virtual entity (VE) component contains the functionality that associates VEs to relevant services as well as a means to search for such services. The resources module provides the functionalities required by services for processing information and for notifying application software and services about events related to resources and corresponding virtual entities; (3) The sensing layer involves sensing devices, such as RFID tags, sensor nodes, which can collect, record, and process observations and measurements. The network layer is able to access the sensing layer with device-level API, which facilitates the information exchange between the applications and the environment.

3 Standards

In the last decade, RFID-based identification has been widely used. Since 2010, due to the advances in intelligent sensors, wireless communication, and sensor network technologies, a number of networked things are involved in IoT. As a new generation networking technology, IoT will connect objects and systems through automatically communicating and exchanging data. The IoT spans a huge number of applications in which billions of things can be connected. To better provide services to end-users or applications, IoT technical standards should be developed which will define the specifications of information exchange, processing, and communications between things. The success of the IoT depends on standardization, which will provide interoperability, compatibility, reliability, and effective operations on a global scale (Table 2).

Research in the past decade shows that there are a number of technical standards vital to the success of IoT proposed by various institutions in different countries. Among these, middleware, interfaces, and open standards in IoT are very important. The main research objectives in this area include: (1) designing policies and distributed architectures; (2) improving privacy and individual protection; (3) improving the trustworthiness, acceptability, and security of IoT; (4) standardization; (5) improving the development of fundamental technologies such as micro-MEMS and ubiquitous localization; (6) applications based on IoT, such as healthcare systems, environment monitoring, etc. IoT related standards have received much research attention around the world. In Japan, the “uID” was developed as a basic infrastructure platform that connects academic research to industrial research and development. In China, numerous 973 nationally supported projects for deep research on standards on the fundamental techniques in IoT have been initiated.

Developing standards for IoT requires consideration of the efficiency and availability of specifications. Currently, a number of institutions are working on the primary standards in IoT. Globally, the ITU (International Telecommunication Union), EPCglobal, IEC (International Electro-technical Commission), ISO (International Organization for Standardization), and IEEE have provided a set of standards to identify, capture, and share, using RFID technologies. In Europe, the European Telecommunications Standards Institute (ETSI) and the European Committee for Electro-technical Standardization (CEN/CENELEC) have released a set of standards regarding the fundamental techniques in IoT such as RFID, WSN, etc. In China, the China Communications Standards Association (CCSA) and the China Electronics Standardization Institute (CESI) are working on the standards of semi-passive RFID and high frequency (UHF) band RFID. In the US, the American National Standards Institute (ANSI) is working on the standards for managing IoT.

The lack of standards may decrease the competitiveness of IoT products. A global collaboration regarding standards is needed to deal with the lack of homogeneity among standards bodies. Formal contracts such as the World Standards Cooperation (WSC) should be able to govern the relationships between the international standards bodies and regional standards bodies. The balance among standards is very important at the early phase of IoT development, since it can help the developers and users to determine the best technical protocols for dynamic

applications and services in IoT. On the other hand, standardization of the technologies used in IoT is urgent, and might accelerate the spread of IoT technology.

4 Application

The IoT paradigm aims to bring an intelligent interconnection of objects in the physical world through information-sensing devices using network protocols and information systems, so that objects can communicate and interact with each other. IoT enables information gathering, storing, and transmitting to be available for things equipped with IoT tags. IoT tags have been widely used in many industrial sectors. IoT is not only an IT infrastructure, but it is, more importantly, an information system which is applied to sense the environment, and to measure, identify, position, track, and monitor objects. The front end is "sense, understand, and control" and the back end is for feedback and control.

It is very important to make efforts toward new applications. To improve tailings dam safety, a tailing dam monitoring and pre-alarm system based on IoT and cloud computing was accomplished with the capacities of real-time monitoring of the saturated line, impounded water level, and dam deformation (Sun, 2012). Pang, Chen, Han, and Zheng (2015) suggested that IoT is a promising solution for a personalized health care system. IoT accommodates updating in order to reach a more accurate treatment of chronic diseases such as diabetes. IoT allows the defining the solutions to happen closer to the patients, physician, and nurses, which allows an easier integration and acceptance of them. Traditional transaction monitoring mechanisms can only monitor system-level events and situations. In the digital business-aware transaction, IoT can help to obtain the real-time information processing of application-level events and the users can ascertain the business is operating in normal mode. IoT is able to improve business transactions with smarter service networks, which will significantly improve the efficiency of real-time information processing and can manage fine-grained applications such as online payments, critical data storage, aggregated QoS, and associated key performance indicators. IoT can reduce the gap between the components in the current digital economy, in which a services-centric economy is realized through network transactions. Mean-

Table 2

A List of Standards Involved in IoT

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 EPC™ 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, EPCglobal, 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

while, business processes can benefit from the IoT at three levels: (1) the level of individuals, such as consumer service and individual service; (2) the level of enterprises, such as business process and supply chain management; (3) the level of industry, which involves industrial and economic development. Enterprises that adopt IoT technology can benefit from more competitive products, more profitable and greener business models, resource optimization, and real-time information processing in business activities. The globally connected IoT can provide enterprises with integrated logistic service networks. Manufacturers can benefit from global availability, cost-efficient purchasing, and inventory management. The IoT-based infrastructure enables the business partners to seamlessly integrate enterprise resources. Large-scale applications are emerging in many industries such as IBM, Cisco Systems, and GE from smart grid to real-time transportation management and optimization. Although the IoT is at its infant stage, 43% of large Chinese organizations have begun to test and investigate the private clouds and infrastructures; this number is likely to increase.

ICT will provide innovative infrastructures, fulfilling the requirements of IoT including heterogeneity (different objects, sensors, protocols and applications, dynamicity (arrival and departure of objects), and evolution (support for new protocols and sensors). Gama, Touseau, and Donsez (2012) applied service-oriented middleware that tries to leverage the existing Internet of Things Architectural concepts to bring more flexibility and dynamicity. Alam, Chowdhury, and Noll (2011) discussed the secure access provision to IoT enabled services and interoperability in different administrative domains. A layered architecture of IoT has been proposed; on the application layer, a semantic overlay is proposed. Heer, Garcia-Moechon, Hummen, Keoh, Kumar and Wehrle (2011) used building automated control as an example to illustrate the challenges in a secure IP-based IoT with the focus on security protocols. The requirements of IoT architecture have been discussed from the perspective of security.

From the perspective of application, IoT can be viewed as an integrated information system based on the Internet to achieve high efficiency in industrial sectors such as transportation, healthcare, and many others. The nature of such an integrated information system shows: (1) massive amounts of data in real-time; (2) ambient intelligence, since the integration and fusion of information possess a synergized effect; (3) a multi-disciplinarity; and (4) dynamics.

The IoT is of high importance on economy and society. For its use to become more ubiquitous, the development of information technology infrastructures plays a key role. It can be foreseen that the IoT will greatly contribute to the addressing of societal issues such as healthcare monitoring, traffic congestion controlling in the future.

5 Global initiatives and IoT for One Belt One Road (OBOR)

5.1 Global initiatives

To take a leadership position, the UK government has launched a £5m project on IoT's technological foundation and innovation. In the US, the IoT has become a top priority research topic and are widely used in streamlining business logistics, industrial automation, air transportation, retailing, public-transit hubs, and healthcare. IBM and ITIF (The Information Technology & Innovation Foundation) released a report in 2009 which claimed that the new ICT technology development (including IoT) could be an effective way to improve the existing information technology infrastructure, and would have a greater positive impact on productivity and innovation. The US government has focused ICT strategies on energy efficiency, broadband technology opportunities, rural utilities service, and healthcare ICT. In the EU, the IoT European Research Cluster (IERC) FP7 (http://www.rfid-in-action.eu/cerp/) has hosted a number of integrated projects on the fundamental technologies of IoT, such as "Internet of Things Architecture (IoT-A)," which has mainly designed the reference model and architectures. In these projects, the applications and end-users provide the precise requirements to drive the theoretical work. Meanwhile, the European Telecommunications standards Institute (ETSI) is working on the policy making. In China, the "Sensing China" project, which assumes that if everything around had an identification tag that could collect data and could be accessed through the Internet, it would be possible to keep track of the status of the things in IoT and monitor any number of parameters, was officially launched in June 2010 by the government. Meanwhile, Republic of Korea has launched RFID/USN and a "New IT Strategy" program to advance its IoT infrastructure development. The government of Japan launched "u-Japan x ICT" and "i-Japan strategies" in 2008 and 2009 that aim at deploying the IoT into all aspects of daily living.

5.2 IoT for One Belt One Road (OBOR)

The 4th Industrial Revolution & the Global Internet of Things Innovation Summit of Chinese Economic and Trade Cooperation Organization Summit was held at Diaoyutai State Guest House in Beijing on June 28, 2016. Here's the excerpts of the 'One Belt One Road' Global Internet of Things Innovation Union Advocacy initiative" (http://europe.chinadaily.com.cn/business/2016-06/28/content_25890359.htm):

"On July 2008, the first International Internet of Things Standardization Conference was held in Shanghai, which initiated the China's possession of the power to speak on international standard of Internet of Things;

On September 2014, International Standardization Organization passed the Internet of Things system structural criteria approval, which is led by China. From there, China starts to lead the trends of development of global Internet of Things. The opportunity for China in the era of Internet of Things has arrived.

With the arrival of a new round of information revolution, countries around the world are finding themselves on the fast track of a new round of technology revolution and industry renovation. Germany has proposed the Industry 4.0, which is supported by Internet of Things. The US is accelerating the process of advancing the information physical system big data strategy. Different from other countries, China has the advantages in exceptional industry demands and market space. Chinese's confidence in innovation will create a new 'Chinese Miracle' in the era of Internet of Things.

Along with the implementation of 'One Belt One Road' advocacy, the year 2016 is first year under the 13th Five Year Plan. Today, Chinese chambers of commerce, scientists, entrepreneurs and idea banks from various regions are going to create a cooperation platform and together establish an All-Connected World.

Here, we advocate that:

1) With 'One Belt One Road' as the link, we establish Global Internet of Things Innovation Union to promote the development of Internet of Things industry promotion law and standard system, innovate the Internet of Things financial services system, co-build the Internet of Things data sharing platform and jointly devote ourselves in the development of global real economy.

2) We propagate the spirit of the Silk Road, innovate 'One Belt One Road' Internet of Things industry's top-level design and the underlying framework and create Global Internet of Things' high-end value chain which benefits all parties.

3) We create 'One Belt One Road' Internet of Things industry's multi-variant collaborations ecological chain, promote mutual beneficial cooperation which is with multi-agent, all-around and cross-domain, fully distribute the bonus from global Internet of Things leading-edge technology revolution and promote the 'One Belt One Road' Internet of Things technology to benefit people's livelihood.

4) We lead the general trend of global information revolution, co-create 'One Belt One Road' Internet of Things think tank, gather the wisdom from the world's best scientists and entrepreneurs who work in Internet of Things to benefit 'One Belt One Road.'

Let us together, forge the long spanning historical Silk Road to a new future-oriented, global reaching Silk Road with sustainable wisdom, peace and happiness."

5.3 Key IoT applications in One Belt One Road

Currently 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, transportation, workplace and home support, security and surveillance. OBOR is a long-term plan designed to expedite the build-up of infrastructure along the ancient 14th Century Silk Road and the newer Maritime Silk Road to open new markets and facilitate trade, capital flows, and economic integration. The scale of the initiative is breathtaking which covers 60% of the world's population, around 30% of the world's GDP and access to China's accumulated $3 trillion in foreign reserves. Investments along the "New Silk Road" will include information architectures such as IoT. Below are some IoT applications in industries in OBOR.

5.4 IoT in infrastructure building

IoT solutions have been developed in many infrastructure areas: smart cities, environmental monitoring, smart homes/building, and so on. In smart buildings, IoT can help to improve the quality of building management and can reduce the consumption of resources. In recent years, the term "Smart Cities" has been proposed to denote the cyber-physical ecosystem emerging through the deployment of intelligent sensors and novel services over city-wide scenarios. In China, the "Sensing China" project was launched in June 2010; it assumes that if everything around us could have an identification tag that could broadcast information to the Internet, people could keep track of the status of the things through IoT and could monitor any number of parameters. With the successful deployment of IoT in a community or in a city, the huge impacts of IoT on all aspects of life can be foreseen.

5.5 IoT in healthcare industry

Healthcare is an important application area for IoT, which can enhance service quality and reduce costs (Yin, Zeng, Chen, & Fan, 2016). In healthcare, a number of medical sensors or devices can be used to monitor medical parameters such as body temperature, blood glucose level, blood pressure, heart rate, etc. Advances in sensors, wireless communication, and data processing technologies are the driving forces of implementing IoT into healthcare systems. The emerging wearable body sensor networks (WBSNs) can be used to continuously monitor patient activities or medical parameters (Yan et al., 2015). IoT can provide healthcare systems with interconnection of such heterogeneous devices and can help in obtaining a comprehensive picture of health parameters (Pang, Chen, Han, & Zheng, 2015).

IoT that interconnects with wearable biosensors can help healthcare services with patient parameter monitoring, daily activity tracking (steps walked, calories burned, exercises performed, etc.), and the care of the aging. It can

be foreseen that IoT-equipped intelligent medical sensors can significantly enhance the quality of life and can even prevent the onset of health problems. The low-cost medical sensor technology is able to wirelessly connect with other things in IoT, which can make it possible to develop implantable wireless identifiable sensors to monitor the health parameters of a patient's life. Recent BLE-based technologies can help with interconnection in the healthcare, security, and home entertainment industries. BLE-based technologies enable a device to communicate with objects that are integrated with respective chips, such as mobile phones, watches, mobile body sensors, home appliances, and personal computers. Through this, all things can be connected with IoT.

On the other hand, the development of mobile devices and mobile health applications creates a huge market for IoT in the health care sector. The individual mobile health applications that assist cardiology practices to measure blood pressure, and diabetes treatment facilities to record blood glucose, have been developed. A new concept named the Health Internet of Things (HIoT) has been proposed (Fielding & Taylor, 2002). It is based on the use of sensor technologies and wireless networks for the monitoring of medical parameters. IoT technologies can be used to improve assisted living solutions. Medical devices that connect to IoT (including medical sensors and wearable sensors) can be used to gather the healthcare information that can be transmitted to remote medical centers.

IoT provides new opportunities to improve healthcare. 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. 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. The wide spread of mobile internet service has expedited the development of the IoT-powered in-home healthcare (IHH) services. Security and privacy concerns are two major challenges that currently limit the further development of IoT in health care.

5.6 IoT in transportation and logistics

IoT will play an increasingly important role in transportation and logistics industries. 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. Furthermore, IoT is expected to offer promising solutions to transform transportation systems and automobile services (Zhou, Liu, & Wang, 2012). 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 (Qin, Long, Zhang, & Huang, 2013). Zhang, Chen, and Lu (2012) 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. 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 regulations are needed to prevent unauthorized access to or disclosure of the privacy data.

5.7 IoT in food supply chain

Today's food supply chain (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 (Pang, Chen, Han, & Zheng, 2015). 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: the field devices such as WSN nodes, RFID readers/tags, user interface terminals, etc., the backbone system such as databases, servers, and many kinds of terminals connected by distributed computer networks, etc., and 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 technologies can be used to facilitate the challenge of analyzing the tremendous data collected from food supply chain.

5.8 IoT in mining industry

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 (Wei, Zhu, & Du, 2011). 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.

5.9 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 (Zhang & Yu, 2013). Recently Ji and Qi (2010) illustrate an infrastructure of IoT applications used for emergency management in China. Their IoT application infrastructure contains sense layer, transmission layer, support layer, platform layer, and applications layer. Their IoT infrastructure has been designed to integrate both local-based and sector-specific emergency systems.

6 Challenges, open problems and future research

6.1 Challenges and open problems

Cooper and James (2009) discussed the challenges of data management in IoT. Databases are distributed which are different from traditional centralized ones; a very large number of nodes handle volumes that are vast, the speed is fast; and the data/information space is global. Currently there are fast, reliable, inexpensive e-infrastructures that provide communication services. However, the required new network is far more complicated, since the web is growing not arithmetically but exponentially.

As far as the applications are concerned, many challenges exist in adapting IoT. Researchers have discussed the challenges of IoT in the aspects of data explosion, data interpretation, fault tolerance, interaction, power supply, scalability, security and privacy, software complexity, and interoperability. Atzori, Iera, and Morabito (2010) agreed that it is challenging to make a full interoperability of interconnected devices possible, to enable the adaptation and automation for a high degree of smartness, and to assure security and privacy. It is believed that there is a clear need for developing a reference architectural model that will allow interoperability between different systems. Sperner, Meyer, and Magerkurth (2011) emphasized that a unified reference architecture is a key prerequisite for realizing interoperability with the IoT for integration with business processes.

The key technological drivers, potential applications, and challenges in IoT have been studied recently. The main enabling factor of IoT is the integration of several technologies and communication solutions: identification and tracking technologies, networks, enhanced communication protocols, and distributed intelligence for smart objects. From the perspective of business users, the most important considerations will be in automation, manufacturing, logistics, business process management, intelligent transportation, etc. Fleisch (2010) proposed a term called High Resolution Management (HRM) to leverage the power of integrated data to increase visibility and to exploit it for business excellence. In many cases, businesses try to reduce the number of product variants even as they are trying to offer a rich set of customized products and services. IoT can help, although with great challenges, in developing appropriate technologies.

IoT resembles the "wild west" of a couple of centuries ago. It is a vast, mostly unexplored territory without clear borders.

6.2 Technical challenge

Although a lot of IoT research efforts have been made, in addition to the challenges introduced above, many other challenges still exist:

1) Designing a service oriented architectures in which service-based things might suffer from performance and cost limitations for IoT is a challenge. In addition, the automated service composition according to the requirements of applications also is a challenge.

2) From the viewpoint of service, the lack of a commonly accepted service description language makes the services development incompatible in different implementation environments. In addition, a powerful services discovery and search engine should be very helpful to spread the IoT technology.

3) IoT is taking place in an ICT environment and it is affected by everything connected. Therefore, it is challenge to integrate IoT with the current ICT systems.

6.3 Standardization challenge

The rapid growth of IoT makes standardization difficult; however, it plays a key role in the uptake of IoT. The standardization in IoT aims at lowering the entry barriers to the new service providers and users, which can improve the interoperability and can allow products or services to better compete at a higher level. The open standards in IoT (such as security standards, communication standards, identification standards, etc.) might be the key enablers for the spread of IoT technologies and will embrace a fully inclusive range of edge technologies. The specific issues regarding IoT standardization include: interoperability, semantic interoperability (Xiao, Guo, Gong, & Li, 2016), access level issues, and security and privacy issues.

6.4 Security and privacy challenge

In IoT, security and privacy are two important challenges. To integrate the sensing layer devices into the IoT, it is necessary to develop effective security technology, which provides security and privacy protection for IoT activities. The applications in IoT may face challenges such as physical attacks to RFID tags, data stores; integrity of codes protection; and the availability of things. In RFID systems, a number of security schemes and authentication protocols have been proposed to cope with security threats. Juels (2006) proposed a “block tag” to prevent unauthorized tracing. On the other hand, low-cost symmetric-key cryptography algorithms, such as Tiny Encryption Algorithm (TEA) and Advanced Encryption Standard (AES), have been proposed to protect the information exchange in IoT. It is reported that low-cost RFID tags have implemented some asymmetric key cryptography algorithms, such as Elliptic Curve Cryptography (ECC). On the other hand, the security protocols developed for WSN can be integrated into IoT as an intrinsic part of IoT.

Information privacy is one of the most sensitive subjects in IoT. The availability of data in IoT makes it difficult to protect information generated by personalized services. To design a proper data and privacy protection mechanism, many factors need to be taken into consideration. User authentication/authorization can involve numerous technologies, such as access control, trust management, etc.

In IoT, numerous applications can be involved. Therefore, it is necessary to develop a high degree security mechanism. The challenges in security and privacy protection include resilience to attacks, data authentication, access control, and client privacy, among others.

Social acceptance of the new IoT technologies and services will strongly rely on the trustworthiness of the information and the protection of private data. Although numerous projects have been launched in security and privacy, a reliable security protection mechanism for IoT still needs to be researched.

In the aspect of data confidentiality, privacy, and information trust, technically, the following challenges need to be solved: (1) the definition of security and privacy from the viewpoint of social, legal, and cultural aspects; (2) a trust and reputation mechanism; (3) communication security; (4) the privacy of communication and user data; and (4) security on services and applications.

As described above, every physical object in IoT can find a responding counterpart that can provide services for applications or users. Each object should be well addressed and labeled in IoT. The interconnection between things might bring unprecedented convenience and as well as security issues. Therefore, strong security protection is necessary in IoT to avoid attacks and malfunctions. In traditional networks such as the Internet, security protocols and privacy assurance are widely used to protect privacy and communication security. However, traditional lightweight cryptography and security protocols are not safe enough for IoT. Current security protocols and mechanisms must be improved and then integrated into IoT in order to provide better protection.

On the other hand, a strong legal and technical framework is also essential. Due to the complex nature of IoT, the protection of billions of intelligent things is very difficult. Things might face a lot of threats such as data leakage, identify theft, and threats coming from external networks. Therefore, IoT must provide strong security protection for all components at all stages, from the sensing layer to the application layers, from identification to services provision, from RFID tags to IT infrastructure governance. Information should be secured from the beginning of its existence to the end of its life cycle. In IoT, heterogeneity greatly affects the security protection of networks; it is easy to suffer threats from communication channels, cryptography, and route selection.

6.5 Innovation management challenge

IoT is a complex network that might be managed by a number of stakeholders, wherein services should be provided openly. Therefore, open new services/applications development should be supported without creating

excessive burdens for market entry or other operation barriers. In addition, the cross-domain systems-supported innovation is still a challenge for IoT.

6.6 Future research

In recent years, the idea to integrate the IoT with social networks has been proposed in (Fielding & Taylor, 2002) and a new paradigm named "Social Internet of Things (SIoT)" has been proposed to describe a world in which things around us can be intelligently sensed. It is predicted that SIoT can effectively perform things and service discovery and can improve the scalability of IoT in human social networks. Meanwhile, the privacy and protection in social networks can be implanted into IoT in order to improve the security of IoT. The idea of SIoT is motivated by the popular social networks: Facebook, Twitter, and micro-blogging, which permeate everyday life. The SIoT has attracted attention from many areas including e-business and e-learning. The homophily method to establish higher levels of trust can be helpful to use in optimizing the relationships between things (Fielding & Taylor, 2002). There are discussions about the combination of social relationships into the future of the Internet (National Intelligence Council, 2008; Welbourne, et al., 2009). Hernandez-Castro, Tapiador, Peris-Lopez, Li, and Quisquater (2008) discussed the integration of IoT into existing social networks such as Facebook, Twitter, etc. Fielding and Taylor (2002) investigated the potential of SIoT to support novel applications and networking services for the IoT in more effective and efficient ways. An integration scheme of social networking into IoT has been described and the system architecture for implementing a SIoT has been developed, as *Figure 5* shows.

IoT emphasizes the connections between things, which covers the reasoning, context-awareness, and transactions. The emerging technologies, including sensing, ubiquitous computing, cloud computing, wireless sensing, and so on, make IoT capable of connecting machine-to-machine (M2M) networks, sensor networks, and even the ubiquitous networks. IoT will provide our daily lives with more connectivity and intelligence. The trend in IoT is the fusion of sensing and the Internet, in which all sensed things are able to intelligently provide services for us.

6.7 Service-oriented architecture for Internet of Things

The key idea of IoT addresses the fact that things are interconnected. A well-designed IoT framework is necessary to guarantee the operations of IoT; it helps to reduce the gap between the physical and the virtual worlds. The architecture of IoT involves multiple key issues including architecture design, networking and communication, smart objects, services and applications, business models and corresponding processes, cooperative data processing, and security, among others. *Figure 6* summarizes the basic service-oriented architecture of IoT, which includes four layers, depending on the basic functionalities:

- Sensing layer, which is integrated with existing hardware to sense the information of things;

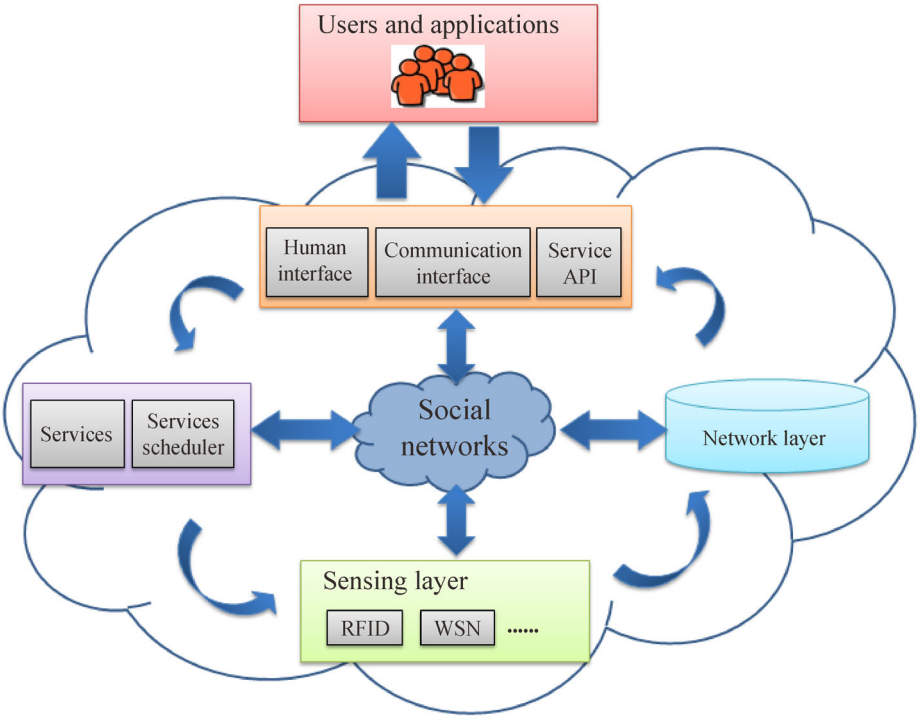

Figure 5. A proposed architecture of social IoT.

• Networking layer, which is the basic networking support over a wireless or wired network;
• lService layer, which is used to create and manage services to users or applications;
• Interface layer, which provides the interaction methods to users/applications.

The service-oriented architectures (SOA) can be imperative for the service providers and requestors in IoT, and can help achieve interoperability between heterogeneous devices. In designing the architecture for IoT, the extensibility, scalability, and interoperability among heterogeneous devices and their business models should be taken into consideration. Since things move on a real-time basis and interact with their environment, an adaptive architecture is required in order to make devices interact dynamically with other things to support the unambiguous communication of events. The decentralized and heterogeneous nature of IoT requires an architecture that can provide IoT with efficient event-driven capability.

An SOA approach will allow the decomposing of the complex system into multiple simpler and well-defined subsystems in IoT; by doing this, the software and hardware in IoT can be effectively reused. SOA has been successfully applied in existing wireless sensor networks. For IoT, a commonly accepted service-oriented architecture should provide IoT extensibility, scalability, modularity, and interoperability among heterogeneous things, where the functionalities and capabilities can be abstracted into a common set of services. An extension of the SOA vision of IoT paradigm is shown in *Figure 6* (Roman & Lopez, 2009).

6.8 Sensing layer

IoT can be considered as a truly world-wide physical interconnected network, in which things can be connected and controlled remotely. The ensemble of applications and services leveraging such technologies opens a plethora of new business and market opportunities in many areas, including healthcare, industrial processes, and many others. In the sensing layer, the wireless smart systems on tags or sensors are able to automatically sense and exchange information between devices.

In the past few years, technological advances in sensing and wireless communication capabilities have made devices equipped with RFID or intelligent sensors more accessible and more versatile. The capability of IoT to sense and identify things or environments has been significantly improved, and therefore its usability has been enhanced for more and more applications. In IoT, the identification and retrievability make a thing hold a digital identity that can be easily specified in the digital domain. In some industrial sectors, an intelligent services deployment scheme has been developed, in which each service is assigned a universal unique identifier (UUID) that can be recognized by other things that need that service. Through this, a device can be easily used to look up and retrieve the appropriate information. Such UUIDs are critical for the deployment of successful services in a huge network like IoT. The identifiers, for example, might refer to names and addresses.

In designing the sensing layer of an IoT (see *Figure 6*), one is concerned primarily with the following issues:

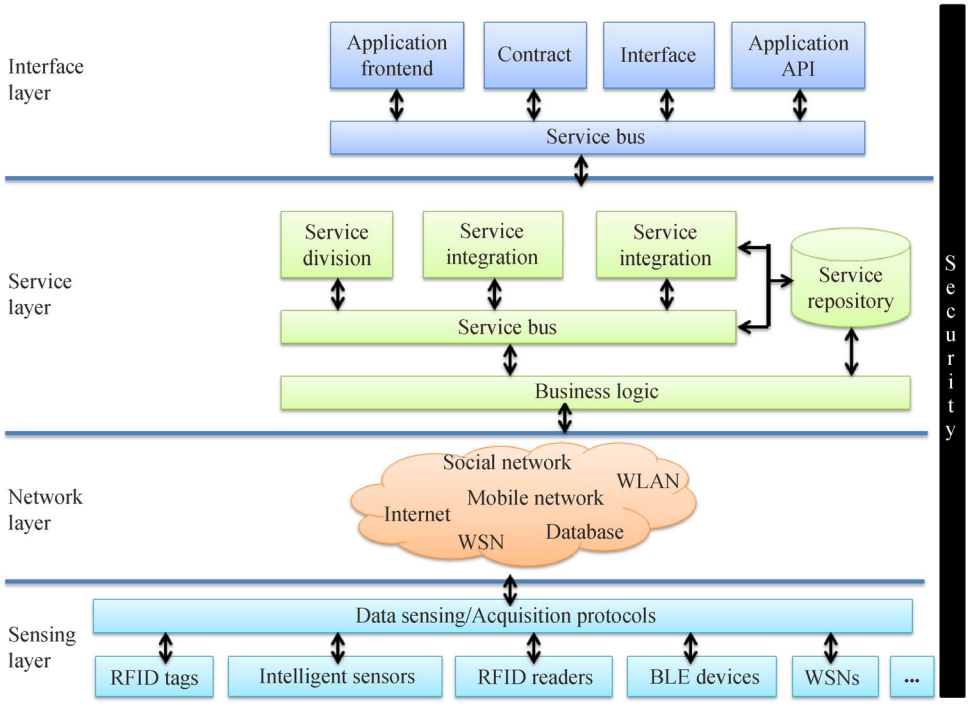

Figure 6. Service-oriented architecture for IoT.

• Cost, size, resource, and energy consumption. The things might be equipped with sensing devices such as RFID tags, sensor nodes, or intelligent devices which should be designed with very limited resources and should be very cost effective.

• Deployment. The sensing things (RFID tags, sensors, etc.) in IoT might be deployed on a one time, incremental, or random basis, depending upon the requirements of applications.

• Heterogeneity. The variety of things with different properties make the IoT very heterogeneous.

• Communicability. All things should be accessible, retrievable, and communicable.

• Networked. Things are organized as multihop, mesh, or ad hoc networks.

IoT is a very complex network in which a large number of hardware and software platforms are involved. IoT may consist of a number of heterogeneous systems, for which the following issues need to be addressed:

• Energy-efficient communications between things;

• Cognitive radios of things;

• Communication spectrum and frequency allocation;

• Wireless coexistence of WLAN, ZigBee, Bluetooth, etc.

In the sensing layer, the hardware issues include wireless identifiable systems design, ultra-low cost tags, and smart/mobile sensors.

6.9 Networking layer

The role of the networking layer in the IoT is to connect all things together. It allows them to become aware of their surroundings. In the networking layer, things can share the sensed information (that is very important for intelligent event processing and management related to IoT) with the connected things. Even more, the networking layer might be capable of aggregating information from existing IT infrastructures (e.g. business, transportation, power grids, healthcare, ICT systems, etc.) which can be further sent to the crucial services for decision-making. In SOA-IoT, services are always provided by things that are deployed in the heterogeneous network; related things are brought into the service Internet. This process might involve a QoS guarantee for the services that is very different according to the requirements of its users/applications. On the other hand, it is essential for a dynamically changing network to automatically discover and map things in networks. Things need to be assigned roles automatically to deploy, manage, and schedule the behaviors of things and to be able to switch to any roles at any time, as required. This enables devices to collaboratively perform tasks. In the networking layer, following issues required to be addressed:

• Network management technologies for heterogonous networks, including fixed, wireless, mobile, etc.;

• Energy efficient in networks;

• QoS requirements;

• Discovery and search engine technologies;

• Data and signal processing;

• Security and privacy.

6.10 Service layer

The service layer relies on the middleware technology, which is a key enabler of services and applications in IoT. Middleware technology can provide the IoT with a cost-efficient platform in which the hardware and software platforms can be reused.

The service layer in IoT involves activities in the field of middle service specifications; most of them are undertaken by various standards developed by different organizations. Therefore, a commonly accepted service layer is important for IoT. A well-designed service layer will be able to identify a minimum set of common requirements of applications, application programming interfaces (APIs), and protocols to support required applications and services.

This layer processes all service-oriented activities, including information exchange and storage, the management of data, an ontologies database, search engines, and communication. This layer includes following components:

• Service discovery. Finding objects that can provide the required service and information in an efficient way.

• Service composition. Enabling interaction among connected things. The discovery phase exploits the relationships of things to find the desired service, and the service composition component is able to schedule or re-create more suitable services in order to obtain the most reliable services for the request.

• Trustworthiness management. Aiming at understanding how the information provided by other services has to be processed.

• Service APIs. Providing the interactions between services required in IoT.

6.11 Interface layer

In IoT, a large number of devices which have been made by different manufacturers and hence do not always comply with the same standards are involved. These heterogeneous things might inevitably cause interaction problems between things, such as information exchanging, communication, cooperative processing of dynamical events, etc. The increasing number of things in an IoT makes it difficult to dynamically connect, communicate, disconnect, and operate. There is a strong need for an effective interface mechanism to simplify the management and interconnectedness among and between things.

An interface profile (IFP) can be seen as a subset of service standards that allows minimal interaction with applications running on application layers. One illustration of an interface layer is the implementation of Universal Plug and Play (UPnP), which specifies a protocol for

seamless interaction among services that offered by different things. 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 it connects to the network, to dynamically retrieve metadata about it and the services it hosts. A SOCRADES Integration Architecture (SIA) has been proposed that can be used to effectively interact between applications and the service layer. A Representational State Transfer (REST) is defined to increase interoperability for a loose coupling between services and distributed applications, which will make the interaction between services and applications more effective. Traditionally, the service layer provides a universal API for applications. Recent research on SOA-IoT shows that a service provisioning process (SPP) can effectively provide interaction between the applications and services.

7 Summary

As reported by Pretz in 2013, the next generation of Internet should be a things-connected network, wherein things are wirelessly connected via smart sensors and are able to interact without human intervention (Pretz, 2013). Some basic technologies have been already developed and applied in the automotive, healthcare, food supply chains, and transportation. Information sharing is one of the features of IoT that is able to help to build global collaboration in industry. Efforts have been made on the development, standardization, security, and application aspects of IoT.

Currently, depending on the area or country, IoT has been developed following three approaches:

- Opportunity investment approach. In the US, the short or mid-term return on investment drives the development of smart energy, smart cities, and RFID. Through social media networks, a number of services and applications for IoT are prominent: such as smart phones, location-based services, and augmented reality.
- In the EU, the IoT are developed using a "stakeholder approach" in which a number of short-term (4–5 year) IoT projects are launched by public-private partnerships investments. This approach is cost-efficient, and has been widely used in some IoT applications such as healthcare, automotive, and home appliances.
- An integrated approach. In China, the IoT infrastructure, software, and services/applications are integrated. The government contributes to the design of the IoT from the view of a global perspective, and a number of state-supported projects have been launched, such as "Sensing China," which are trying to integrate IoT fully into the IT architecture.

Although it is not yet clear which approach is more efficient, all of them can promote the improvement of the fundamentals of social-technical development. In the past few years, IoT has developed very quickly and a large number of fundamental technologies have been proposed. This paper introduces the recent research on IoT from the viewpoint of technologies. We introduce the service oriented architecture models of IoT and the fundamental technologies that can be used in IoT. We introduce the applications of IoT from several aspects. We list the open research problems in IoT. The IoT is the trend of next Internet and it has received support from governments and businesses across the globe. According to Lima, a country's absorptive capacity for technological innovation and the capacity for transferring technology is very important (Lima, 2016). To OBOR countries, IoT is a technological innovation which needs to be transferred across the OBOR. Relating to the economic development of OBOR, IoT will greatly impact OBOR in foreseeable future.

References

Alam, S., Chowdhury, M., & Noll, J. (2011). Interoperability of security-enabled internet of things. *Wireless Personal Communications*, 61, 567–586.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: a survey. *Journal of Computer Networks*, 54, 2787–2805.

Cooper, J., & James, A. (2009). Challenges for database management in the internet of things. *IETE Technical Review*, 26, 320–329. Available at: http://tr.ietejournals.org/text.asp?2009/26/5/320/55275.

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

Fleisch, E. (2010). *What is the internet of things*? *An economic perspective*. Retrieved from https://www.researchgate.net/publication/227984761_What_is_the_Internet_of_Things_An_Economic_-Perspective.

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

Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., & Savio, D. (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.

Haller, S., Kanouskos, S., & Schroth, C. (2009). The internet of things in an enterprise context. *Future Internet Systems*, 5468, 14–28.

Heer, T., Garcia-Moechon, O., Hummen, R., Keoh, S. L., Kumar, S. S., & Wehrle, K. (2011). Security challenges in the IP-based internet of things. *Wireless Personal Communications*, 61(3), 527–542.

Hernandez-Castro, J., Tapiador, J., Peris-Lopez, P., Li, T., & Quisquater, J. (2008). *Cryptanalysis of the SASI ultra lightweight RFID authentication protocol with modular rotations*. Retrived from http://www.so.com/link?url = http%3A%2F%2Fwww.researchgate.net%2Fpublication%2F220488939_Cryptanalysis_of_the_SASI_Ultralightweight_RFID_Authentication_Protocol_with_Modular_Rota-

tions&q =+ Cryptanalysis + of + the + SASI + Ultralightweight + RFID + Authentication + Protocol + with + Modular + Rotations&ts = 1472525764&t = 35ae65870adbcc4b63118bd1a6d4853-&src = haosou.

ITU. (2005). *ITU internet report 2005: the internet of things*. Retrived from http://wenku.baidu.com/link?url = SPgqVux42HJ5EJbm0T-ZA_q_9iqWp12nZ69SBgCdUStd3Hq7hzBMb3KW3UaDX-H_4e0nxFtbtqK9ox5c8HJeK1MwaS3Dkwr4xSwedkk0gzhsu.

Ji, Z., & Qi, A. 2010. The application of internet of things (IOT) in emergency management system in China. *In Proceedings of 2010 IEEE International Conference on Technologies for Homeland Security (HST)*, 139–142.

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

van Kranenburg, R., & Bassi, A. (2012). *IoT challenges*. Retrieved from http://link.springer.com/article/10.1186%2F2192-1121-1-9.

Lima, R. (2016). Economic growth and human capital in the post-knowledge era: a focus on positive externalities and spillover effects of knowledge in Italy and the emergency of the less developed areas. *Journal of Industrial Integration and Management*, 1(3).

Logeais, G. (2008). *The internet of things in the context of manufacturing*. Retrieved from http://docbox.etsi.org/workshop/2008/200812_WIRELESSFACTORY/SAP_LOGEAIS.pdf.

National Intelligence Council. (2008). *Disruptive civil technologies: six technologies with potential impacts on US interests out to 2025*. Retrieved from http://globaltrends.thedialogue.org/publication/disruptive-civil-technologies-six-technologies-with-potential-impacts-on-us-interests-out-to 2025/.

Pang, Z., Chen, Q., Han, W., & Zheng, L. (2015). Value-centric design of the internet-of-things solution for food supply chain: value creation, sensor portfolio and information fusion. *Information Systems Frontiers*, 17, 289–319.

Pretz, K. (2013). *The next evolution of the internet*. Retrieved from http://theinstitute.ieee.org/.

Qin, E., Long, Y., Zhang, C., & Huang, L. (2013). Cloud computing and the internet of things: technology innovation in automobile service. *Lecture Notes in Computer Science*, 8017, 173–180.

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

Sperner, K., Meyer, S., & Magerkurth, C. (2011). Introducing entity-based concepts to business process modeling. *Business Process Model & Notation-Third International Workshop*, 95, 166–171.

Sun, E., Zhang, X., & Li, Z. (2012). The internet of things (IOT) and cloud computing (CC) based tailings dam monitoring and pre-alarm system in mines. *Safety Science*, 50(4):811–815.

Uckelmann, D., Harrison, M., & Michahelles, F. (2011). An architectural approach towards future internet of things. *Architecting the Internet of Things*, 1–24.

Vermesan, O. (2009). *Internet of things vision and the technology behind connecting the real, virtual and digital worlds*. Retrieved from http://www.grifs-project.eu/data/File/CERP-IoT%20SRA_IoT_v11.

Wei, Q., Zhu, S., & Du, C. (2011). Study on key technologies of internet of things perceiving mine. *Procedia Engineering*, 26, 2326–2333.

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 Computing*, 13, 48–55.

Xiao, G., Guo, J., Gong, Z., & Li, R. (2016). Semantic input method of Chinese word senses for semantic document exchange in e-business. *Journal of Industrial Information Integration*, 1(3): 31–36.

Xu, L. (2014). Engineering informatics: state of art and future trends. *Frontiers of Engineering Management*, 1(3): 276–288.

Xu, L. (2015). *Enterprise Integration and Information Architectures*. Florida: CRC Press.

Xu, L., He, W., & Li, S. (2014). Internet of things in industries: a survey. *IEEE Transactions on Industrial Informatics*, 10(4): 2233–2248.

Yan, H., Xu, L., Bi, Z., Pang, Z., Zhang, J., & Chen, Y. (2015). An emerging technology—wearable wireless sensor networks with applications in human health condition monitoring. *Journal of Management Analytics*, 2(2), 121–137

Yin, Y., Zeng, Y., Chen, X., & Fan, Y. (2016). The Internet of things in healthcare: an overview. *Journal of Industrial Information Integration*, 1(1), 3–13.

Zhang, Y., Chen, B., & Lu, X. (2012). Intelligent monitoring system on refrigerator trucks based on the internet of things. *Wireless Communications and Applications*, 72, 201–206.

Zhang, Y.C., & Yu, J. (2013). A study on the fire IOT development strategy. *Procedia Engineering*, 52, 314–319.

Zhou, H., Liu, B., & Wang, D. (2012). Design and research of urban intelligent transportation system based on the internet of thinge. *Communications in Computer and Information Science*, 312, 572–580.