Internet of Things in Real-Life—A Great Understanding

Mohammad Derawi and Hao Zhang

Abstract The internet of things (IoT) is a topic that each day increases by its name and has certainly opened great opportunities to set up powerful manufacturing systems and applications by gearing the growing ubiquity of wireless systems, RFID system, as well as sensor and mobile devices. A widespread range of real-life IoT applications have been implemented and deployed in recent years. To really realize and know how the development of IoT in businesses are set, this paper gives a great understanding of the topics IoT, greater IoT systems in businesses key-enabling-technologies (KET) and also goes into deeper explanations of now-a-days research challenges and trends. The key contribution of this paper is that it overviews the current IoT research working in real-life business thoroughly.

Keywords Internet of things (IoT) · ICT · Large data analytics · Enterprise systems · Business informatics (BI) · Near field communications (NFC) · Radio-Frequency identification (RFID) · Wireless sensor networks (WSNs)

1 Introduction

The internet of things (IoT) is a developing technology and is probable to give capable answers to convert the operation and role of many current systems such as transportation systems and manufacturing systems. For instance, when IoT is used for making intelligent transportation systems, the transportation authority will be able to track each vehicle's present location, monitor its movement, and forecast its future location and likely road traffic. The term IoT was first proposed to refer to uniquely identify interoperable connected objects with RFID technology [1]. Thereafter, scholars combine IoT with multiple technologies, for example, as

M. Derawi (✉) · H. Zhang
Smart Wireless Systems, Institute of Electronics, Gjøvik University College,
Gjøvik, Norway
e-mail: mohammad.derawi@hig.no

Q.-A. Zeng (ed.), *Wireless Communications, Networking and Applications*,
Lecture Notes in Electrical Engineering 348,
DOI 10.1007/978-81-322-2580-5_32

actuators, sensors, GPS devices, and mobile devices. Nowadays, a frequently accepted explanation for IoT is *"a scenario in which objects, animals or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction. [Tech Target Online]"* Precisely, the incorporation of sensors, RFID tags, and communication technologies serves as the basis of IoT and explains how a variety of physical objects and devices near us can be connected to the Internet and let these objects and devices to cooperate and connect with one another to reach mutual goals [2].

In various industries, there is a rising attention in applying IoT technologies. IoT has in the industries been used within project-domains such as food, agriculture, environmental monitoring, processing business, security surveillance, and more. For the meantime, the quantity of IoT journals is quickly growing. In this paper, we have conducted an extensive literature to aid researchers to comprehend the current status and future research opportunities regarding the use of IoT in business.

2 Background

The IoT can be seen as a worldwide network infrastructure with a number of linked devices that depend on communication, sensory, networking, and information processing technologies [2]. An opening technology for IoT is the RFID technology, which permits microchips to transmit the identification information to a reader via wireless communication. By applying RFID devices, users can identify, track, and monitor any entities attached with RFID tags automatically. RFID has been widely applied in logistics, pharmaceutical production, retailing, and supply chain management, since 1980s [3]. Another starting technology for IoT is the wireless sensor networks (WSNs), which mostly apply smart sensors to sense and monitoring. Its applications include environmental monitoring, healthcare monitoring, industrial monitoring, traffic monitoring, and so on [4]. The improvements in both RFID and WSN expressively contribute to the development of IoT. In addition, many other technologies and devices such as barcodes, smart phones, social networks, and cloud computing are being applied to form a widespread network for supporting IoT [5].

To this day, IoT has been gaining attraction in businesses such as logistics, manufacturing, pharmaceutics, and retailing. With the improvements in smart phones, wireless communication, and sensor network technologies, even more networked or smart objects are being elaborated in IoT. Consequently, these IoT-related technologies have therefore ended in a large impact on new information and communications technology (ICT) and enterprise systems technologies.

In order to deliver high-quality facilities to clients, IoT's technical standards need to be designed for defining the requirement for information exchange, processing, and communications between objects. The realization of IoT depends on standardization, which provides interoperability, compatibility, reliability, and effective operations on a global scale [6]. Many countries and organizations are interested in the development of IoT standards because it can bring tremendous economic benefits in the future. Currently, several major organizations around the world are functioning on the development of various IoT standards [7, 8].

3 Design Pattern for IoT

The goal of IoT is to join different objects/things over the networks. As a key technology in integrating varied systems or devices, the service-oriented architecture (SOA) is a design pattern that can be applied to support IoT. The architecture has been effectively applied in research areas within the scopes of cloud computing, WSNs, and vehicular network [9]. Several concepts are already offered to produce multi-layer service-oriented architectures for IoT based on the selected technology, business technical requirements. As an example, the international telecommunication union (ITU) recommends that IoT design involves five diverse layers: sensing, accessing, networking, middleware, and application layers. The work of [10, 11] suggests to split the IoT system architecture into three main layers: perception layer, network layer, and service layer (sometimes labeled as the application layer). The authors in [8] created a three-layered architectural model for IoT that contains the application layer, the network layer, and the sensing layer. The authors in [12] designed and created an IoT application infrastructure that covers the physical layer, transport layer, middleware layer, and applications layer.

The scheme in an architectural manner of IoT is concerned with architecture styles, web services and applications, smart objects, networking and communication, business models and corresponding process, cooperative, security, data processing, etc. From the technology viewpoint, the design of an IoT architecture must consider extensibility, scalability, modularity, and interoperability among mixed devices. As things might move or need real-time interaction with their surroundings, an adaptive architecture is required to assist devices dynamically to interact with other objects. The decentralized and heterogeneous nature of IoT needs that the architecture delivers IoT effectual event-driven competence. Thus, SOA is being seen as a good method to attain inter-operability among heterogeneous devices in a multitude of way [13].

3.1 Sensing Layer

IoT is to be seen as a universal physical inner-connected net, where objects can be linked and controlled remotely. As we observe more devices equipped with RFID or brainy sensors, linking things becomes much more trivial [14]. In the sensing layer, the wireless smart systems with tags or sensors are currently able to sense and exchange information among different devices fully automatically. This technology improves expressively the capability of IoT to sense and identify things or environment. In some business sectors, intelligent service deployment systems and a universal unique identifier (UUID) are allocated to each service or device that may be wanted. A device with UUID can be simply recognized and retrieved. Therefore, UUIDs are critical for effective services deployment in a giant network like IoT [14].

3.2 Networking Layer

The part of networking layer is to link all things with each other and permit things to share the information with other associated things. Furthermore, the networking layer is talented of combining information from current IT infrastructures (i.e., transportation systems, business systems, power grids, healthcare systems, ICT systems, etc.). In SOA-IoT, services given by things are classically deployed in a mixed network and all related things are carried into the service Internet [15]. This procedure might include QoS management and control according to the necessities of users/applications. Instead, it is important for a dynamically altering network to automatically determine and plot things in a network. Things must be automatically allocated with roles to organize, manage, and plan the behaviors of things and be talented to shift to any other roles at any time as desired. These abilities permit devices to be able to collaboratively complete tasks. When designing the networking layer in IoT, designers need to address topics such as network management technologies for heterogonous networks (such as fixed, wireless, mobile, etc.), energy efficiency in networks, QoS requirements, service discovery and retrieval, privacy and security, data and signal processing [16].

3.3 Service Layer

The service layer is depended on the middleware technology that offers methods to flawlessly assimilate services and applications in IoT. The middleware technology offers the IoT with a cost-efficient stand, where the hardware and software stages can be reapplied. A main job in the service layer includes the service specifications for middleware, which are being created by numerous organizations. A well-designed service layer is capable to classify common application necessities and deliver APIs and protocols to sustenance required services, user needs, and applications. This layer also processes all service-oriented difficulties, i.e., information exchange and storage, data management, search engines, and communication [8]. This layer includes [8, 16] (1) Service discovery: finding objects that can give the needed services and information in an well-organized way; (2) Service composition: enabling the communication among connected things; (3) Trustworthiness management: pointing at determining trust and reputation functions that can assess and apply the information provided by other services to create a reliable system; (4) Service APIs: supporting the relations between services required in IoT.

3.4 Interface Layer

Within IoT, a great number of devices involved are created by dissimilar manufacturers/vendors and they do not permanently fulfill the exact standards/protocols. This concludes in many interaction problems with exchange of information, communication, and cooperative event processing among different things. Also, the continuous increase of things contributing in an IoT makes it more difficult to dynamically connect, communicate, disconnect, and operate. There is also a need for an interface layer to make the management and interconnection of things easier. An interface profile (IFP) can be understood as a division of service standards that support interaction with applications deployed on the network. A decent interface profile is related to the implementation of universal plug and play (UPnP), which describes a protocol for enabling interaction with services provided by various things [16]. The interface profiles are applied to define the specifications between applications and services. The services on the service layer run directly on limited network infrastructures to successfully find new services for an application, as they connect to the network. Lately, an integration architecture (SIA) has been suggested to successfully interact among applications and services [17]. Traditionally, the service layer provides universal API for applications. However, the current research results on SOA-IoT reported [18] that service provisioning process (SPP) can also efficiently offer interaction between services and applications.

4 Technologies

4.1 Communication Technology

IoT may include many electronic devices, mobile devices, and industrial equipment. Dissimilar things have diverse communication, networking, data processing, data storage capacities, and transmission power. For example, numerous smart phones today have strong communication, networking, data processing, and data storage volumes. Associated to smart phones, heart rate monitor watches only have limited communication and computation abilities. All these objects can be linked by networking and communication technologies.

IoT includes several assorted networks such as WSNs, wireless mesh networks, and WLAN. Those networks assist objects in IoT to exchange information. A gateway has the skill to enable the communication or interaction of numerous devices over the Internet. The gateway can also influence its network information by performing optimization algorithms locally. Thus, a gateway can be applied to grip many multifaceted features involved in communication on the network [19].

Dissimilar objects may have changing QoS requirements, for example performance, energy efficiency, and security. Let us say, a lot of devices depend on batteries and thus reducing energy usage for these devices is a top concern. In distinction, devices with power supply connection frequently do not set energy saving as a top precedence. IoT could also importantly benefit by leveraging current Internet protocols such as IPv6, since this will make it possible to directly address any number of things required through the Internet [8]. The leading communication protocols and standards are NFC, RFID, IEEE 802.15.4 (ZigBee), IEEE 802.11 (WLAN), IEEE 802.15.1 (Bluetooth), multihop wireless sensor/mesh networks, IETF low power wireless personal area networks (6LoWPAN), traditional IP technologies such as IP and IPv6, and machine to machine (M2M).

4.2 Tracking/Identification Technology

The tracking and identification technologies within IoT are RFID systems, barcode, and intelligent sensors. A usual RFID system is a combination of an RFID reader and an RFID tag. The RFID system is gradually being applied, such as logistics, supply chain management, and healthcare service monitoring, due to its skill to identify, trace, and track devices and physical objects [6, 20]. Other pros of the RFID system include offering detailed real-time information about the involved devices, dropping labor cost, shortening business process, enlarging the accuracy of inventory information, and improving business efficiency. Modern development of the RFID technology focuses on the following aspects (1) active RFID systems with spread-spectrum transmission; and (2) technology of managing RFID applications [3, 8].

Still, there is a large space for the development of the RFID-based applications [19]. To further promote the RFID technology, RFID can be combined with WSNs to better track and trace things in real-time.

4.3 Service Management

Service management is the way to implement and manage quality of IoT services that meet the requirements of applications or users. The SOA can be applied to summarize services by hiding the implementation details of services such as protocols applied [21]. Here it is possible to decouple between components in a system and therefore hide the heterogeneity from end users. An SOA-IoT lets application to apply heterogeneous objects as compatible services [10]. Instead, the lively nature of IoT applications needs IoT to deliver consistent and reliable services. An actual SOA can diminish the influence caused by device moves or battery failure.

A service is a group of data and associated performances to achieve a particular function or feature of a device or portions of a device. A service might locate other main or subordinate services and/or a set of characteristics that make up the service. The services can be characterized into two types: main service and secondary service. The first mentioned means services that represent the primary functionalities, which can be seen as the elementary service component and can be included by another service. The last mentioned secondary service can offer supplementary functionalities to the primary service or other secondary services. A service can consist up to many features, which describes service data structures, descriptors, permission, and other attributes of a service [16, 22].

4.4 Network

There are not so many cross-layer protocols for wireless networks, i.e., wireless sensor and actuator networks (WSANs) or ad hoc networks (AHNs) [15]. Still, they need vision beforehand such that they can be applied to the IoT. The purpose is that IoT often have varied communication and computation capabilities, and varying QoS requirements. In difference, nodes in WSNs classically have similar necessities for hardware and network communication. In addition, the IoT network applies the Internet to support information exchange and data communication. In difference, WSNs and AHNs do not have to include the Internet for communication.

5 Applications

The IoT applications are still new and in its initial phase [22]. Nevertheless, the usage of IoT is quickly developing and rising. Some limited IoT applications are in a development stage and/or deployed in various businesses including health-care service, inventory and production management, transportation, workplace and home support, security, surveillance, and environmental monitoring. In [8,19], they offer a universal introduction to IoT applications in numerous domains. The design of manufacturing IoT applications requests to consider multiple goals. Dependent on the planned business application, designers may need to create a trade off among these objectives to attain a fit of cost and benefits. Below are some IoT applications in business.

5.1 Healthcare

IoT offers new chances to expand healthcare [10]. Driven by IoT's ubiquitous identification, communication, and sensing capacities, all objects in the healthcare systems (equipment, people, medicine, etc.) can be chased and monitored constantly [23]. Enabled by its universal connectivity, all the healthcare-related information (diagnosis, logistics, treatment, prescription, recovery management, daily activity and economics) can be composed, managed, and shared professionally. For instance, a patient's oxygen rate can be composed by sensors and directed to the doctor's office. By applying the personal computing devices (mobile phone, laptop tablet, etc.) and mobile internet access (Wi-Fi, Edge, 3G, LTE, etc.), the IoT-based healthcare facilities can be mobile and adapted [24].

5.2 Mining Production

Mine protection is a huge concern for a lot of nations because of the working condition. To avoid and decrease coincidences inside the mining, a necessity is to apply IoT technologies to sense mine tragedy signals in order to mark quick warning, ruin forecasting, and safety improvement of underground production possible [25]. By applying RFID, Wi-Fi, and other wireless communications technology and devices, mining businesses can monitor the position of underground miners and analyze dangerous security data composed from sensors to improve safety measures. Enhanced research is required within safety characteristics of IoT devices applied in this area.

5.3 Firefighting

Even in firefighting, IoT is applied for safety arena to sense possible fire and provide early notice for possible fire tragedies. Recently the research of [26] exemplify an infrastructure of IoT applications applied for emergency management in China, where RFID tags and/or bar codes are committed to firefighting goods to create countrywide firefighting management systems and product information databases. By leveraging mobile RFID readers, RFID tags, sensor networks, smart video cameras, and wireless communication networks, the firefighting expert can perform automatic analysis to realize real-time environmental monitoring, forecast fire warning, and emergency rescue as needed.

5.4 Transportation and Logistics

The IoT is going to have a gradually important role in transportation and logistics business [8]. As even more physical objects are attached with RFID tags, bar codes, or sensors, transportation and logistics companies are able to retrieve real-time tracking of physical objects from a beginning to a terminus across the whole supply chain [27]. Additionally, IoT is likely to result in great solutions to convert transportation systems and automobile services [28]. As vehicles have progressively stable networking, sensing, communication, and data processing capabilities, IoT technologies can be applied to enhance these capabilities and share resources between automobiles everywhere. As an example, IoT technologies make it possible to monitor each vehicle' existing location, estimate its movement, and forecast its future location. Lately, an intelligent informatics system, the iDrive, created by BMW applied numerous sensors and tags to track the abovementioned examples. In the paper of, a smart monitoring system to monitor humidity/temperature inside fridge trucks by using RFID tags, sensors, and wireless communication technology is designed. Even other researchers today are developing autopilot for vehicles that automatically will detect streetwalkers or other vehicles for retrieving the so called smart driving. Thus, security and privacy protection are the important aspects for the widespread usage of IoT in transportation and logistics.

6 Challenges and Trends

IoT technologies and applications are still in their infancy and still widely accepted by the business community [22]. Still, there are great research challenges business use such as technology, standardization, security, and privacy [8, 19]. Thus, future-related works are required to discourse these challenges and study the features of different businesses to guarantee stable IoT devices. A satisfactory understanding of business characteristics and requirements on issues such as security, cost, privacy, and risk is required before IoT will be widely accepted and deployed in businesses.

While a great amount of research efforts have been made on IoT technologies, there are still some challenges some technical challenges which we will describe here.

(A) A great challenge in IoT is to design a SOA, in which service-based things might hurt from performance and cost limitations. Furthermore, scalability subjects frequently ascend as increasingly physical items are linked to the network. When the quantity of things is huge, scalability is problematic at dissimilar levels including data transfer and networking, service provisioning and data processing and management [19].

(B) From a network point of view, IoT is a complex assorted network that contains the joining between numerous types of networks through various communication technologies. Presently, there is a deficiency of widely accepted common platform that hides the heterogeneity of highlighting networks/communication technologies and delivers a see-through naming service to various applications [19]. Huge amounts of data transmission across the network at the similar period might cause common delay, conflict, and communication issues. It is a puzzling task to create networking technologies and standards that can let data collected by a great number of devices to move efficiently within IoT networks, which is a great challenge within research [6].

(C) From the service point of view, an absence of a frequently accepted service description language creates the service development and integration of resources of physical objects into value-added services problematic. The developed services could be mismatched with different implementation and communication environments [8, 21].

(D) Since IoT is frequently grounded on an outdated ICT setting and it is affected by anything connected to the network, it requires great amount of work to be integrated as IoT with present IT systems. Additionally, with the great number of things connected to the Internet, an enormous amount of real-time data flow will automatically be shaped by connected things [29]. The data may not have much expressive worth unless researchers discover an actual way to examine and comprehend it [30]. Analyzing or mining enormous amounts of data produced from both IoT applications and existing IT systems to originate valuable information needs robust big data analytics skills, which might be thought-provoking for numerous end users.

Regarding regulations and standardization, it is the fast developments of IoT that makes the regulations and standardization tough. Nevertheless, standardization has a significant part for the additional development and spread of IoT. The aim of standardization is to lower the entrance barriers for the new service providers and users, to expand the interoperability of different applications/systems and to permit products or services to better perform at a higher level. A cautious standardization process and a lot of organization efforts are needed to guarantee devices and applications from different nations to be able to exchange information [19]. Numerous standards applied in IoT (e.g., security standards, communication standards, and identification standards) might be the main enablers for the spread of IoT technologies and must to be designed to embrace developing technologies. Precise issues in IoT standardization include interoperability issue, radio access level issues, semantic interoperability, and security and privacy issues [31].

When talking about the privacy and information security, then the approval and wide spread of new IoT technologies and services will mainly depend on the information security and data privacy defense, which are two challenging matters in IoT because of its mobility, deployment, and complexity [32]. A great mount of current technologies are available for customer use, but not appropriate for business applications that have severe safety and security requirements. To make information secure, current encryption technology retrieved from the WSNs or other networks must be prudently studied. As IoT gives access to numerous daily things to be tracked, monitored, and connected, even a lot of personal and private information can be collected automatically [8]. Shielding privacy in the IoT environment is getting even more serious than the usual ICT environment because the numbers of attack paths on IoT bodies are much greater [13]. For instance, a health monitor will collect patient's information, such as pulse rate, oxygen, and sugar level and then send the information straight to the doctor's office over the network. When the information is transferred via the network, then patient's data could be pinched. Still it should be mentioned that the definition of privacy and legal interpretation are still unclear. Although the existing network security technologies offer a basis for privacy and security in IoT, more research needs to be performed. A consistent security protection mechanism for IoT needs to be researched. The research are from the description of security and privacy from the perspective of social, culture, and legal; trust and reputation mechanism; communication security; security on services and applications and privacy of communication/user-data,

Regarding research trends, the development of IoT set-ups will probably follow an incremental method and enlarge from current identification techniques, such as RFID. The global collaboration efforts and system-level viewpoint are required to address the above IoT-related challenges [19]. Furthermore, to make research address the mentioned challenges, we also identify a few additional research developments.

6.1 Green IoT Technologies

As IoT involves billions of linked sensors communicating via the wireless network, the power usage of sensors is a big worry and restraint for the widespread of IoT. Saving energy should become a serious design goal for IoT devices, such as wireless sensors [33]. There is an essential to create energy-efficient methods that can decrease the power consumption of sensors [34].

6.2 Context-Aware IoT Middleware Solutions

When huge amount of sensors are linked to the Internet, it is not possible for public to process all the data composed by these sensors. Context-awareness computing techniques, such as IoT middleware, are recommended to better understand sensor data and assist to decide what data needs to be processed [29]. Presently, most IoT middleware solutions do not have context-awareness competences. The European Union has acknowledged context awareness as an important IoT research area and specified a time frame (2015–2025) for context-aware IoT computing research and development [20].

6.3 Social Networking with IoT Solutions

There is a great interest to apply social networking to improve the communications among dissimilar IoT things. A new paradigm, named Social Internet of Things (SIoT), was newly presented by [35]. There is a tendency for the change from IoT to a novel vision named Web of Things that permits IoT objects to become dynamic actors and peers on the Web [36].

6.4 IoT and Cloud Computing

Clouds provide a respectable way for things to get associated and permit us to entree different things on the Internet. Further investigation will focus on implementing novel platforms that provide “sensing as a service” on the cloud [37].

6.5 Artificial Intelligence and Smart Objects

In [38] the researchers suggest to generate Internet of Intelligent Things by carrying artificial intelligence into things and communication networks. Upcoming IoT systems would have features counting “self-optimization, self-configuration, self-protection, and self-healing” in it [39]. Smart objects are becoming more intellectual [40] and context-aware with larger memory, processing, and reasoning capabilities in the future.

7 Conclusion

This paper surveys and reviews the recent researches on IoT from the real-life perspective. Initially, we present the background and service-oriented architecture models of IoT and then debate the central technologies that might be applied in IoT. Following, we present some main real-life applications of IoT followed by an analysis of the research challenges and future trends related with IoT. A difference from other IoT survey papers, a main input of this survey paper, is that it emphasizes on manufacturing IoT applications and the challenges and likely research opportunities for upcoming investigators.

References

1. Ashton, K.: Internet of things. RFID J. [Online] Available: http://www.r.djournal.com/articles/view?4986
2. Kranenburg, R.V., Anzelmo, E., Bassi, A., Caprio, D., Dodson, S., Ratto, M.: The internet of things. In: Proceedings of the 1st Berlin Symposium on Internet Society, Berlin, Germany, pp. 25–27 (2011)
3. Sun, C.: Application of RFID technology for logistics on internet of things. AASRI Procedia **1**, 106–111 (2012)
4. He, W., Xu, L.: Integration of distributed enterprise applications: A survey. IEEE Trans. Ind. Inf. **10**(1), 35–42 (2014)
5. Wang, L., Xu, L., Bi, Z., Xu, Y.: Data. ltering for RFID and WSN integration. IEEE Trans. Ind. Inf. **10**(1), 408–418 (2014)
6. Bandyopadhyay, D., Sen, J.: Internet of things: Applications and challenges in technology and standardization. Wirel. Pers. Commun. **58**(1), 49–69 (2011)
7. ITU Ngn-Gsi Rapporteur Group: Requirements for Support of USN Applications and Services in NGN Environment, Geneva. International Telecommunication Union (ITU), Switzerland (2010)
8. Atzori, L., Iera, A., Morabito, G.: The internet of things: a survey. Comput. Netw. **54**(15), 2787–2805 (2010)
9. Domingo, M.C.: An overview of the internet of things for people with disabilities. J. Netw. Comput. Appl. **35**(2), 584–596 (2012)
10. Jia, X., Feng, O., Fan, T., Lei, Q.: RFID technology and its applications in internet of things (IoT). In: Proceedings of the 2nd IEEE Int. Conf. Consum. Electron.,Commun. Netw. (CECNet), Yichang, China, Apr. 21–23, pp. 1282–1285 (2012)
11. Liu, C.H., Yang, B., Liu, T.: Efficient naming, addressing and profile services in Internet-of-Things sensory environments, Ad Hoc Netw. to be published
12. Xu, L.D., He, W., Li, S.: Internet of things in Industries: a survey. IEEE Trans. Ind. Inf. **10**(4), 2233–2243 (2014)
13. Wu, Y., Sheng, Q.Z., Zeadally, S.: RFID: Opportunities and chal-lenges. In: Next-Generation Wireless Technologies, N. Chilamkurti, Ed. New York, Springer, ch. 7, pp. 105–129 (2013)
14. Han, C., Jornet, J.M., Fadel, E., Akyildiz, I.F.: A cross-layer communi-cation module for the internet of things. Comput. Netw. **57**(3), 622–633 (2013)
15. Guinard, D., Trifa, V., Karnouskos, S., Spiess, P., Savio, D.: Interacting with the soa-based internet of things: Discovery, query, selection, and on-demand provisioning of web services. IEEE Trans. Serv. Comput. **3**(3), 223–235 (2010)
16. Romero, D., Hermosillo, G., Taherkordi, A., Nzekwa, R., Rouvoy, R., Eliassen, F.: RESTful integration of heterogeneous devices in pervasive environments. In: Distributed Applications and Interoperable Systems. Berlin, Germany: Springer-Verlag, ch. 01, pp. 1–4 (2010)
17. Zhou, H.: The Internet of Things in the Cloud: A Middleware Perspective. CRC Press, Boca Raton, FL, USA (2012)
18. Zhu, Q., Wang, R., Chen, Q., Liu, Y., Qin,W.: IoT gateway: Bridging wireless sensor networks into internet of things. In: Proceedings of the IEEE/IFIP 8th International Conference Embedded Ubiquitous Comput. (EUC), Hong Kong, China, Dec. 11–13, pp. 347–352 (2010)
19. Lim, M.K., Bahr, W., Leung, S.: RFID in the warehouse: A literature analysis (1995–2010) of its applications, benefits, challenges and future trends. Int. J. Prod. Econ. **145**(1), 409–430 (2013)
20. Liu, Y., Zhou, G.: Key technologies and applications of internet of things. In: Proceedings of the 5th International Conference on Intelligent Computation Technology Automation (ICICTA), Zhangjiajie, China, pp. 187–200 (2012)
21. Xu, L.: Enterprise systems: state-of-the-art and future trends. IEEE Trans. Ind. Inf. **7**(4), 630–640 (2011)

22. Wang, S., Zhang, Z., Ye, Z., Wang, X., Lin, X., Chen, S.: Application of environmental internet of things on water quality management of urban scenic river. Int. J. Sustain. Develop. World Ecol. **20**(3), 216–222 (2013)
23. Plaza, I., Martín, L., Martin, S., Medrano, C.: Mobile applications in an aging society: Status and trends. J. Syst. Softw. **84**(11), 1977–1988 (2011)
24. Wei, Q., Zhu, S., Du, C.: Study on key technologies of internet of things perceiving mine. Procedia Eng. **26**, 2326–2333 (2011)
25. Ji, Z., Qi, A.: The application of internet of things (IOT) in emergency management system in China. In Proceedings of the. IEEE International Conference on Technol. Homeland Security (HST), pp. 139–142 (2010)
26. Karakostas, B.: A DNS architecture for the internet of things: A case study in transport logistics. ProcediaComput. Sci. **19**, 594–601 (2013)
27. Zhou, H., Liu, B., Wang, D.: Design and research of urban intelligent transportation system based on the internet of things. Commun. Comput. Inf. Sci. **312**, 572–580 (2012)
28. Zhang, Y., Chen, B., Lu, X.: Intelligent monitoring system on refrigerator trucks based on the internet of things. Wirel. Commun. Appl. **72**, 201–206 (2012)
29. Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D.: Context aware computing for the internet of things: A survey. IEEE Commun. Surv. Tuts.
30. Wang, F., Ge, B., Zhang, L., Chen, Y., Xin, Y., Li, X.: A system framework of security management in enterprise systems. Syst. Res. Behav. Sci. **30**(3), 287–299 (2013)
31. Wan, J., Jones, J.: Managing IT service management implementation complexity from the perspective of the Warfield version of systems science. Enterp. Inf. Syst. **7**(4), 490–522 (2013)
32. Xia, F.: Wireless sensor technologies and applications. Sensors **9**(11), 8824–8830 (2009)
33. Yaacoub, E., Kadri, A., Abu-Dayya, A.: Cooperative wireless sensor networks for green internet of things. In Proceedings of the 8th ACM Symposium on QoS Security Wireless Mobile Network. Paphos, Cyprus, pp. 79–80 (2012)
34. Atzori, L., Iera, A., Morabito, G., Nitti, M.: The social internet of things (SIoT)-when social networks meet the internet of things: Concept, archi-tecture and network characterization. Comput. Netw. **56**(16), 3594–3608 (2012)
35. Guinard, D., Trifa, V., Mattern, F., Wilde, E.: From the internet of things to the web of things: Resource-oriented architecture and best practices. In: Architecting the Internet of Things, pp. 97–129. Springer, New York, NY, USA (2011)
36. Fang, S., Xu, L., Pei, H., Liu, Y.: An integrated approach to snowmelt food forecasting in water resource management. IEEE Trans. Ind. In-format. **10**(1), 548–558 (2014)
37. Arsénio, A., Serra, H., Francisco, R., Nabais, F., Andrade, J., Serrano, E.: Internet of intelligent things: bringing artificial intelligence into things and communication networks. Stud. Comput. Intell. **495**, 1–37 (2014)
38. Kortuem, G., Kawsar, F., Fitton, D., Sundramoorthy, V.: Smart objects as building blocks for the internet of things. IEEE Internet Comput. **14**(1), 44–51 (2010)
39. Ding, Y., Jin, Y., Ren, L., Hao, K.: An intelligent self-organization scheme for the internet of things. IEEE Comput. Intell. Mag. **8**(3), 41–53 (2013)
40. Alemdar, H., Ersoy, C.: Wireless sensor networks for healthcare: a survey. Comput. Netw. **54** (15), 2688–2710 (2010)