World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

Industrial internet of things: Applications and challenges

Raghunath [1, *], Mamatha Kotagi [1] and Vasant [2]

[1] *Department of Electronics and Communication Engineering. Government polytechnic kalaburgi Karnataka, India.*

[2] *Department of Electrical and Electronics Engineering Government polytechnic kalaburagi ,Karnataka, India.*

World Journal of Advanced Research and Reviews, 2023, 17(02), 933-939

Publication history: Received on 4 February 2023; Revised 26 February 2023; accepted on 28 February 2023 Article

DOI: https://doi.org/10.30574/wjarr.2023.17.2.0210

Abstract

The adoption and deployment of 'Internet of Things' (IoT) technologies are leading to architectural changes to Industrial Automation and Control System (IACS), including greater connectivity to industrial systems. Internet of Things (IoT) has provided a promising opportunity to build powerful industrial systems and applications by leveraging the growing ubiquity of radio-frequency identification (RFID), and wireless, mobile, and sensor devices. A wide range of industrial IoT applications have been developed and deployed in recent years. In an effort to understand the development of IoT in industries, this paper reviews the current research of IoT, major IoT applications in industries, and identifies research trends and challenges.

Keywords: Iot; Rfid; Iacs; Wi-Fi; Fsc; Wsn; Iiot

1. Introduction

Since the term Internet of Things (IoT) was first used in 1999, it has been applied to connected devices in consumer, domestic, business and industrial settings. Although there is a significant amount of literature attempting to define IoT, its uses, and its typical components, it is rarely made obvious how any of this applies in the industrial setting.

The first three industrial revolutions are characterised as being driven by mechanical production relying on water and steam power, use of mass labour and electrical energy, and the use of electronic, automated production respectively [1]. Whilst the supposed fourth industrial revolution ('Industry 4.0') was first proposed in 2011 in the context of the goal of developing the German economy [2]. This revolution is characterised by its reliance on the use of Cyber-physical systems (CPS) capable of communication with one another and of making autonomous, de-centralised decisions, with the aim of increasing industrial efficiency, productivity, safety, and transparency.

The Industrial Internet of Things (IIoT) is the use of Internet of Things (IoT) technologies in manufacturing". The definition of the Industrial Internet includes two key components: The connection of industrial machine sensors and actuators to local processing and to the Internet; The onward connection to other important industrial networks that can independently generate value. The main difference between the consumer/social Internets and the Industrial Internet is in how and how much value is created. For consumer/social Internets, the majority of value is created from advertisements" [3].

There is a growing interest in using IoT technologies in various industries [4]. A number of industrial IoT projects have been conducted in areas such as agriculture, food processing industry, environmental monitoring, security surveillance, and others. Meanwhile, the number of IoT publications is quickly growing.

[*] Corresponding author: Raghunath.

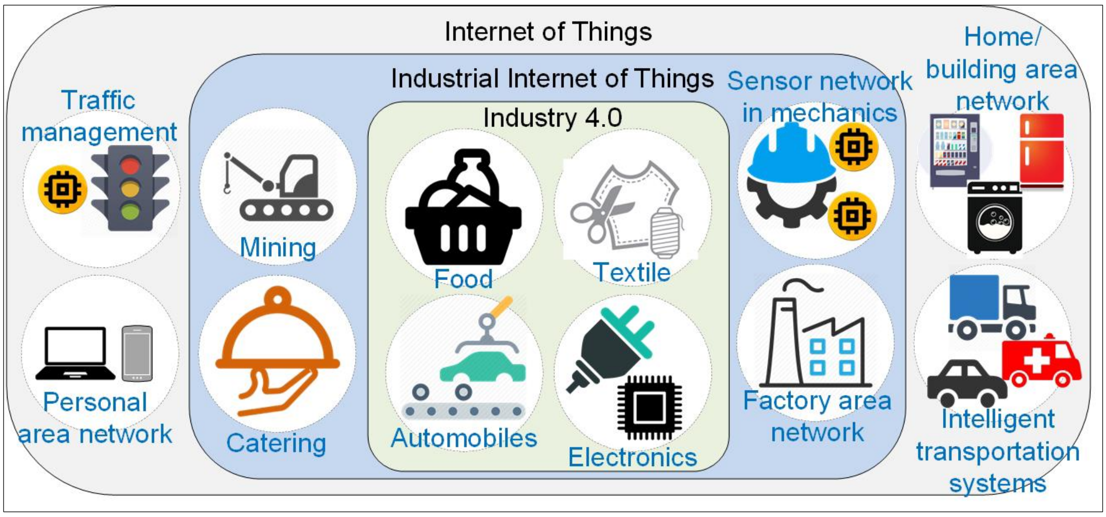

Figure 1 IoT, IIoT, and Industry 4.0

IoT has been gaining attraction in industry such as logistics, manufacturing, retailing, and pharmaceutics. With the advances in wireless communication, smartphone, and sensor network technologies, more and more networked things or smart objects are being involved in IoT. As a result, these IoT-related technologies have also made a large impact on new information and communications technology (ICT) and enterprise systems technologies (Fig. 2).

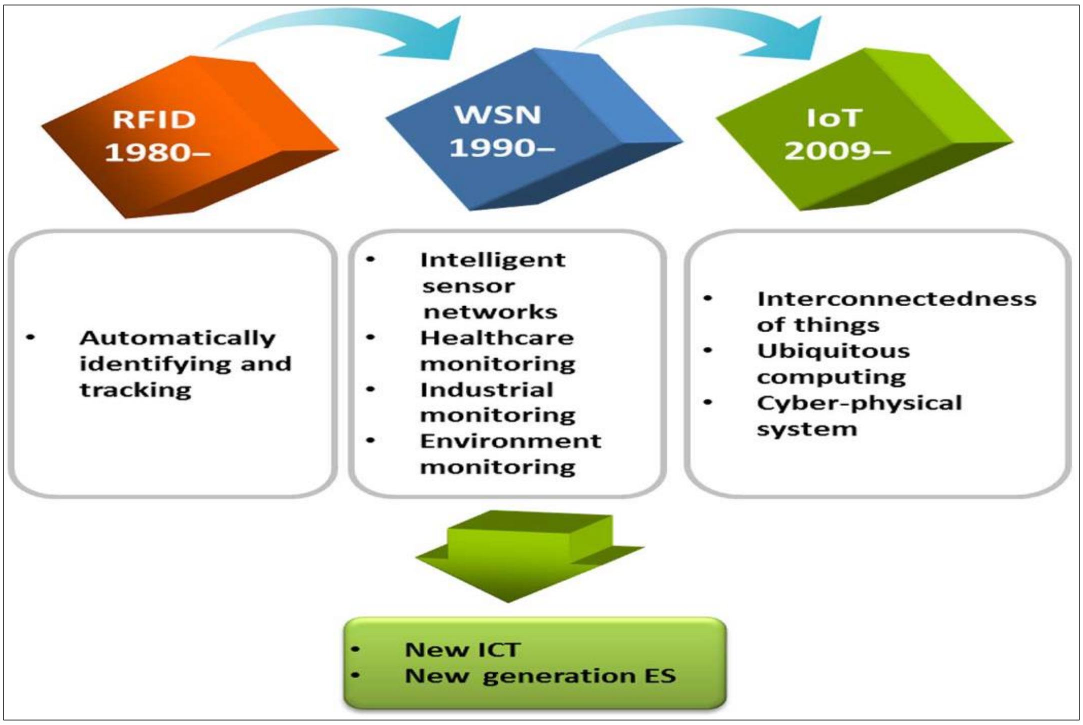

Figure 2 IoT-related technology and their impact on new ICT and enterprise systems

2. Service oriented architecture of iiot

The Service oriented Architecture of IIoT Contain 4 layers as given in the Table 1**.**

Table 1 A Four-Layered Architecture for IoT

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

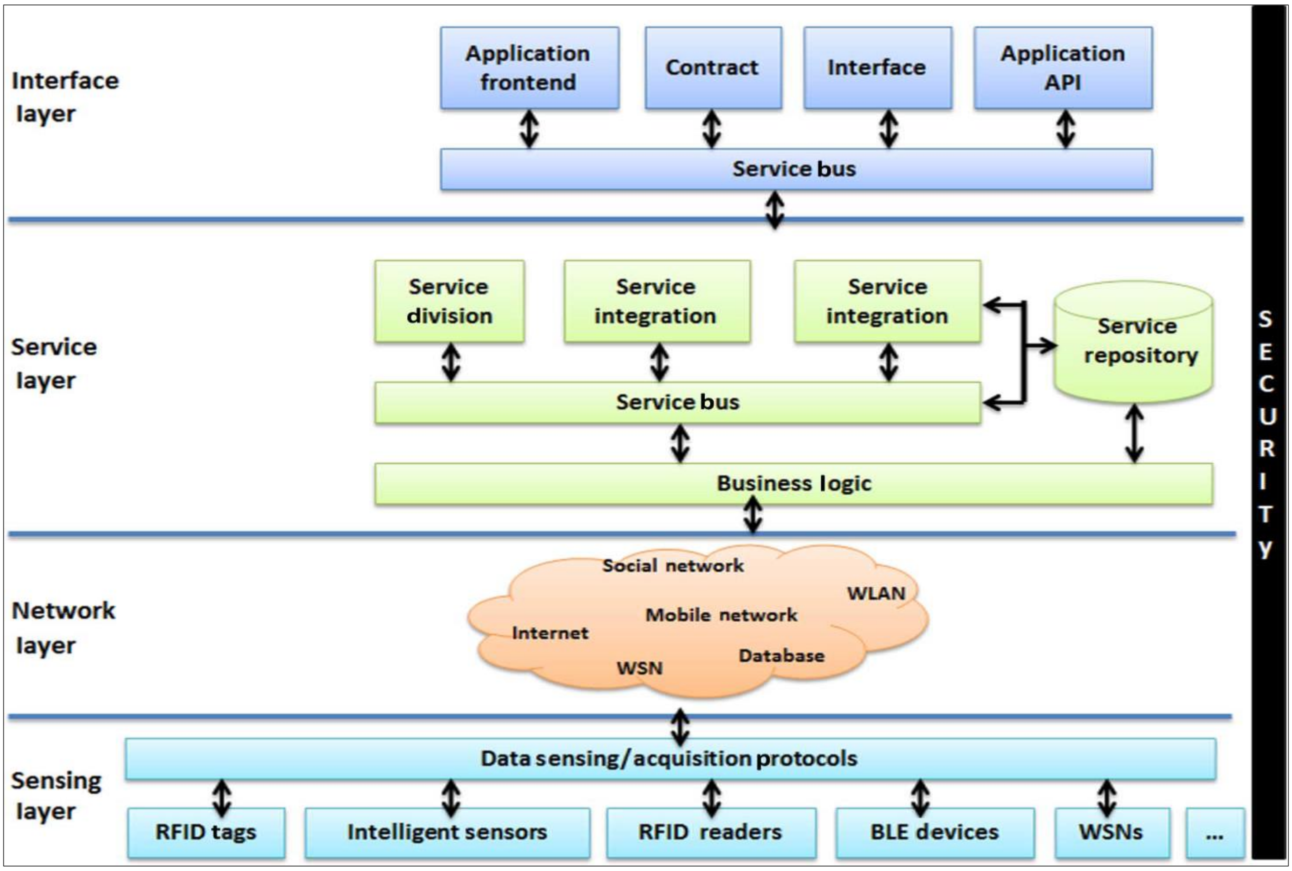

Figure 3 Service oriented Architecture of IoT

2.1. Sensing Layer

IoT can be considered as a world-wide physical inner connected network, in which things can be connected and controlled remotely. As more and more devices are equipped with RFID or intelligent sensors, connecting things becomes much easier [5]. In the sensing layer, the wireless smart systems with tags or sensors are now able to automatically sense and exchange information among different devices. These technology advances significantly improve the capability of IoT to sense and identify things or environment. In some industry sectors, intelligent service deployment schemes and a universal unique identifier (UUID) are assigned to each service or device that may be needed. A device with UUID can be easily identified and retrieved. Thus, UUIDs are critical for successful services deployment in a huge network like IoT [5], [6].

2.2. Networking Layer

The role of networking layer is to connect all things together and allow things to share the information with other connected things. In addition, the networking layer is capable of aggregating information from existing IT infrastructures (e.g., business systems, transportation systems, power grids, healthcare systems, ICT systems, etc.). In SOA-IoT, services provided by things are typically deployed in a heterogeneous network and all related things are brought into the service Internet [8], [7]. This process might involve QoS management and control according to the requirements of users/applications. On the other hand, it is essential for a dynamically changing network to automatically discover and map things in a network. Things need to be automatically assigned with roles to deploy, manage, and schedule the behaviours of things and be able to switch to any other roles at any time as needed.

2.3. Service Layer

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

layer will be able to identify common application requirements and provide APIs and protocols to support required services, applications, and user needs. This layer also processes all service-oriented issues, including information exchange and storage, data management, search engines, and communication.

2.4. Interface Layer

In IoT, a large number of devices involved are made by different manufacturers/vendors and they do not always follow the same standards/protocols. As a result of the heterogeneity, there are many interaction problems with information exchange, communication between things, and cooperative event processing among different things. Furthermore, the constant increase of things participating in an IoT makes it harder to dynamically connect, communicate, disconnect, and operate. There is also a necessity for an interface layer to simplify the management and interconnection of things. An interface profile (IFP) can be seen as a subset of service standards that support interaction with applications deployed on the network.

3. Key iot Applications in Industries

Depending on the intended industrial application, designers may have to make a trade-off among goals to achieve a balance of cost and benefits. Below are some IoT applications in industries.

- Using IoT in the healthcare service industry [9]. IoT provides new opportunities to improve healthcare [11]. 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 [10]. 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 [12].
- Using IoT in Food Supply Chain (FSC) [13]. Today's FSC is extremely distributed and complex. It has large geographical and temporal scale, complex operation processes, and large number of stakeholders. The complexity has caused many issues in the quality management, operational efficiency, and public food safety. IoT technologies offer promising potentials to address the traceability, visibility, and controllability challenges. It can cover the FSC in the so-called farm-to-plate manner, from precise agriculture, to food production, processing, storage, distribution, and consuming. Safer, more efficient, and sustainable FSCs are expectable in the future. A typical IoT solution for FSC (the so-called Food-IoT) comprises three parts: a) the field devices such as WSN nodes, RFID readers/tags, user interface terminals, etc.; b) the backbone system such as databases, servers, and many kinds of terminals connected by distributed computer networks, etc.; and c) the communication infrastructures such as WLAN, cellular, satellite, power line, Ethernet, etc.
- Using IoT for safer mining production. Mines safety, 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 [14]. 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.

- Using IoT in transportation and logistics. IoT will play an increasingly important role in transportation and logistics industries [8]. As more and more physical objects are equipped with bar codes, RFID tags or sensors, transportation and logistics companies can conduct real-time monitoringmof the move of physical objects from an origin to a destination across the entire supply chain including manufacturing, shipping, distribution, and so on [15]. Furthermore, IoT is expected to offer promising solutions to transform transportation systems and automobile services [16]. 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 [17]
- Using IoT in firefighting. IoT has been used in the firefighting safety field to detect potential fire and provide early warning for possible fire disasters. In China, RFID tags and/or bar codes are being attached to firefighting products to develop nationwide firefighting product information databases and management systems. By leveraging RFID tags, mobile RFID readers, intelligent video cameras, sensor networks, and wireless communication networks, the firefighting authority or related organizations could perform automatic diagnosis to realize real-time environmental monitoring, early fire warning and emergency rescue as needed. Researchers in China are also using IoT technologies to construct fire automatic alarming systems in order to raise the nation's firefighting management and emergency management to a new level [18].

4. Research challenges

To realize the true potential of IIoT, we need to address several challenges. We discuss some of these challenges below.

A. Energy consumption and management Industries are the largest consumers of power in any country, thus, require dynamic power management. Depending on the type of the industry, energy consumption varies, which may even be different according to seasons particularly in the case of the food and textile industries. Energy consumption affects the network lifetime and is therefore an important factor in IIoT. In IIoT, not only sensors but actuators and robotic devices are also involved. Therefore, many data packets are continuously being exchanged resulting in a higher energy consumption. Since energy is a valuable resource, it affects time synchronization as well. Algorithms that are able to deal with time synchronization and energy consumption tradeoff, are more suitable for an effective and scalable IIoT environment. Dynamically managing power is an essential element of IIoT. Systematic mechanisms are required to adapt to the changing demand of an industry, during different times of the day, according to different prices and grid load. Some industries may even be run at night to cope with the power load.

B. Interoperability of devices: In IIoT, multiple subsystems and external systems would work together, causing interoperability issues [19]. For example, a smart industry is connected to an external smart grid, a production plant is connected toWoT service, and a production system of a factory is connected to storage system of the same factory, and so on. Several sensors and systems would be heterogeneous. Therefore, system and sensor integration as well as interoperability mechanisms become more of a challenge. Since many of the tasks (such as in a manufacturing environment where actuators are tasked to take actions) would be delay-sensitive, therefore, the integration and interoperability has to be not only seamless, but deliver high performance.

C. Service level agreement and interoperability of services: Along the same line of interoperability of nodes, services' interoperability will be a challenge as well, especially in the case of a service level agreement (SLA). Resource federation of different IIoTs, SLA matching, SLA monitoring and violation, are important factors that need to be considered for scalable IIoT and for enabling inter-IIoTs communication. When relying on third party cloud-IoT services, the key concern is the performance delivered to the customer. Many of the IIoT applications (such as autonomous vehicles, vehicleto- vehicle communications, robotic communications in manufacturing and so on) would be sensitive to security and delay requirements. SLAs must have some of the following essential attributes: meaningful - that is relevant to the involved parties; measurable - so that the acquired service can be compared with the agreed upon service; controllable - such that the factors that determine service satisfaction can be modified to achieve the required service; affordable - the SLA must be cost-effective for the involved services; and acceptable that is the involved parties need to mutually agree on the SLA, rather than one dictating it to the other [20].

D. Security and privacy of data and workers: IIoT would be vulnerable to attacks that can affect the availability, confidentiality, and integrity of transmitted or stored data. With increased connectivity, more data is generated which may be susceptible to theft and misuse because several industrial deployments would be outdoor, such as construction and mining. When multiple nodes and systems communicate with each other, data communication and storage are more prone to intrusion and theft. The data can be misused and may even result in manufacturing malfunctions, which can have drastic effects on production, factory premises, and personnel working there. Moreover, interoperability features might increase security and privacy vulnerabilities in the IIoT environment, resulting in not only attacks but information misuse as well. Since different systems will be combining their resources in an interoperable IIoT scenario, there is increased likelihood that the data, information, and commands could be tampered with.

E. Context and semantics-aware service provisioning: Given the dynamic environment in industry, the ability to discover web-services on the go to create an extended and flexible business process is much needed. An example of a context-aware service in a smart factory environment can be different temperature settings according to different products in a factory. In the case of IIoT, context-awareness can be primary [21], such as gathering context without any existing contextual information; or secondary, such as gathering context from an existing contextual information. Both types have different complexities and outcomes, and hence require more intelligence and efficiency. The same data can be used to derive different insights for different scenarios or even domains commonly known as sensing as a service. For example, data on different temperature settings for different products can be used in the transportation or cargo industry when designing the cargo compartment and cooling equipment. In the case of the medical domain, food stabilizers can be developed according to the related contextual information such as products ingredients,age, life, and required temperature settings. Moreover, developing semantic web-based services can be very important in the industrial scenario. Services are annotated on the basis of shared ontologies, which help in the discovery of web services, according to the semantics [22].

F. Fault detection and reconfiguration: As the IIoT system becomes increasingly automated and heterogeneous entities are involved, the chances of failure increase. Device malfunction, delayed communication, and connectivity failures are some common examples. A complete IIoT system must be robust and be capable of not only detecting and withstanding common faults but also be capable of detecting faults in time. Advanced fault detection algorithms will have to be applied at the hub, gateway, or middleware that is responsible for coordinating different machines and devices. Accuracy and timeliness are also important in detecting faults because one faulty object may hinder the whole manufacturing or industrial process, resulting in financial loss, energy loss, and loss of other related resources. A faulty network of sensors or machines should be able to reconfigure itself with no human intervention. If a sensor is not working due to some malfunctioning, it can be put to sleep until replaced and the sensor network settings can be reconfigured. In this way, not only the robustness is ensured, but energy is also saved.

G. User-friendliness in the product deployment and usage: Industrial workers may not be fluent with the most recent technologies, which makes it even more challenging to design devices and user-interfaces for an IIoT system. Unlike the typical traditional IT system and common IoT systems where either user interaction is low, or the user is well-aware of the technology he/she is using, in the industrial domain, factory workers with different backgrounds and experience are distributed over a large area. For example, in a factory or agricultural field, people in these areas will be deploying the devices and sensors with a low knowledge of electronics and communication. Creating seamless adaptation of the IIoT technology and user-friendly interfaces can help acceptance of IIoT.

5. Conclusion

Recent advances in virtual sensor networking, robotics, and communication technologies have paved the way for autonomous industrial environment. Theoretically, there is a huge potential of IIoT and Industry 4.0. However, it brings a lot of challenges as well, which can be converted to opportunities if better planning and standardization are done. In this paper, we present an architectural introduction of IIoT and Industry 4.0 We discuss some interesting use case scenarios related to different industries, such as transportation, smart grid, food & restaurants, advertisement, and tourism. We also discuss some noteworthy challenges and how they can be converted into opportunities. Some of the challenges include context-aware and semantics-aware service provisioning in IIoT, interoperability of different devices and services, security & privacy, and energy consumption. This work can be very useful in terms of understanding the potential of IIoT and Industry 4.0. It will also motivate future research directions in IIoT for a wide range of application domains.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] D. Lukač, 'The fourth ICT-based industrial revolution', 23rd Telecommunications Forum Telfor, IEEE, 2015, pp. 835–838.

[2] Industrie 4.0 Available: vailable: https://www.bmbf.de/de/zukunftsprojektindustrie- 4-0-848.html.

[3] D. Floyer, Defining and Sizing the Industrial Internet, Wikibon, June 27, 2013 [online], (2013) Available: http://wikibon.org/wiki/v/Defining_and_Sizing_the_ Industrial_Internet.

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

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

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

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

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

[9] Z. Pang, Q. Chen, J. Tian, L. Zheng, and E. Dubrova, "Ecosystem analysis in the design of open platform-based in-home healthcare terminals towards the internet-of-things," in Proc. 2013, 15th Int. Conf. Adv. Commun. Technol. (ICACT), Pyeongchang, Korea, pp. 529–534.

[10] H. Alemdar and C. Ersoy, "Wireless sensor networks for healthcare: A survey," Computer Networks, vol. 54, no. 15, pp. 2688–2710, 2010.

[11] Q. Wei, S. Zhu, and C. Du, "Study on key technologies of internet of things perceiving mine," Procedia Eng., vol. 26, pp. 2326–2333, 2011.

[12] I. Plaza, L. Martín, S. Martin, and C. Medrano, "Mobile applications in an aging society: Status and trends," J. Syst. Softw., vol. 84, no. 11, pp. 1977–1988, 2011.

[13] Z. Pang, Q. Chen, W. Han, and L. Zheng, "Value-centric design of the internet-of-things solution for food supply chain: Value creation, sensor portfolio and information fusion," Inf. Syst. Front., to be published.

[14] Q. Wei, S. Zhu, and C. Du, "Study on key technologies of internet of things perceiving mine," Procedia Eng., vol. 26, pp. 2326–2333, 2011.

[15] [15] B. Karakostas, "A DNS architecture for the internet of things: A case study in transport logistics," Procedia Comput. Sci., vol. 19, pp. 594–601, 2013.

[16] H. Zhou, B. Liu, and D. Wang, "Design and research of urban intelligent transportation system based on the internet of things," Commun. Comput. Inf. Sci., vol. 312, pp. 572–580, 2012.

[17] E. Qin, Y. Long, C. Zhang, and L. Huang, "Cloud computing and the internet of things: Technology innovation in automobile service," LNCS 8017, New York, NY, USA, 2013, pp. 173–180.

[18] Y. C. Zhang and J. Yu, "A study on the fire IOT development strategy," Procedia Eng., vol. 52, pp. 314–319, 2013.

[19] O. Givehchi, K. Landsdorf, P. Simoens, and A. W. Colombo, "Interoperability for industrial cyber-physical systems: An approach for legacy systems," IEEE Transactions on Industrial Informatics, vol. 13, no. 6, pp. 3370–3378, 2017.

[20] A. V. Papadopoulos, S. A. Asadollah, M. Ashjaei, S. Mubeen, H. Pei- Breivold, and M. Behnam, "Slas for industrial iot: Mind the gap," in Future Internet of Things and Cloud Workshops (FiCloudW), 2017 5th International Conference on. IEEE, 2017, pp. 75–78.

[21] C. Perera, C. H. Liu, S. Jayawardena, and M. Chen, "A survey on internet of things from industrial market perspective," IEEE Access, vol. 2, pp. 1660–1679, 2014.

[22] K. Sivashanmugam, K. Verma, A. P. Sheth, and J. Miller, "Adding semantics to web services standards," 2003.