Internet of Things 7 (2019) 100078

Contents lists available at ScienceDirect

Internet of Things

journal homepage: www.elsevier.com/locate/iot

Research article

The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model

In Lee

School of Computer Sciences Western Illinois University, Macomb, IL USA

ARTICLE INFO

Article history:
Received 12 April 2019
Revised 22 June 2019
Accepted 22 June 2019
Available online 25 June 2019

Keywords:
Internet of Things
IoT ecosystem
IoT architecture
IoT applications
Cloud computing
Enterprise
Platform
Business model
Value proposition
IoT service

ABSTRACT

The IoT has brought about a new paradigm in which a global network of machines and devices capable of interacting with each other is driving digital innovation in enterprises. Among various IoT sectors, the enterprise IoT has become the largest sector. In light of the growing importance of enterprise IoT and the research gap in this sector, this paper presents an IoT ecosystem, IoT architecture, and the IoT service business model essential for the selection and deployment of IoT services in various enterprise settings. Then, this paper illustrates how the IoT services can be developed to innovate hotel rooms.

© 2019 Elsevier B.V. All rights reserved.

1. Introduction

The IoT is recognized as one of the most important areas of future technology and is gaining a lot of attention from a wide range of industries [1]. The IoT brought about a paradigm shift that is radically changing ways of doing business by enabling enterprises to develop value-added services with their network of machines and devices, improve their service business models, and enhance their sustainability. For example, the ubiquitous deployment of wireless sensors is extending digital connectivity to tasks, processes, and machine and service operations [2]. By analyzing the data generated by the devices, enterprises can create a favorable brand image and engage in effective communication [3].

The growth of the IoT has been phenomenal in terms of sales volume and the number of enterprise and individual adopters. The combined markets of the IoT will reach about $520 billion in 2021, more than double the spending in 2017 [4]. Enterprise IoT, also called corporate IoT, refers to all connected devices used for various business purposes in the enterprise setting. Enterprise IoT is the largest of the three main IoT sectors - enterprise, home, and government [5]. According to a recent survey [6], 98 percent of survey respondents reported that most companies include enterprise IoT initiatives in their strategic road maps such as improving service operations, increasing visibility into operations, enabling new business models, and creating new product and service offerings. While large enterprises have been the early adopters and beneficiaries of the IoT innovations, an increasing number of small and medium-sized enterprises (SMEs) are also leveraging the IoT services to better serve customers, improve productivity, extend a market base, and stay competitive [7].

E-mail address: i-lee@wiu.edu

https://doi.org/10.1016/j.iot.2019.100078
2542-6605/© 2019 Elsevier B.V. All rights reserved.

The need for effective development of IoT applications under realistic conditions has generated various ecosystems of methodologies and integrated IoT platforms [8]. Many technology companies are developing various IoT platforms to help enterprises rapidly develop and deploy IoT services for their business operations and improvement. These platforms have become a key source for enterprises which have not employed technically capable engineers of the various fields of the IoT. IoT platforms provide basic functionalities and development tools for a variety of enterprise applications to be developed without expensive and time-consuming designing and programming efforts. A compound annual growth rate (CAGR) for IoT platforms is expected to be 39% between 2018 and 2023, with annual spending surpassing US$22 billion by 2023 [9]. Enterprise software and service companies and IoT startups account for the largest portion of IoT platform companies (22% and 32%, respectively), followed by industrial technology providers (18%), Internet companies, and telcos [10].

The purpose of enterprise IoT is to create value for business organizations and customers through IoT services. New IoT platforms are constantly emerging and provide potential opportunities and challenges for enterprise IoT. For enterprises, developing enterprise IoT services with various platforms provided by vendors are often preferred to in-house development. However, there is a lack of studies on the IoT ecosystem and IoT architecture pertaining to the development of enterprise IoT. For example, we still do not fully understand what the elements of the enterprise IoT ecosystem and architecture are and how they facilitate the development of specific enterprise IoT services. In light of the gap in research in the enterprise IoT sector, this paper presents an enterprise IoT ecosystem and architecture essential for deployment of successful IoT-enabled services. Then, this paper discusses how enterprises can plan IoT services with the use of the IoT service business model. This paper illustrates the use of the IoT service business model in the development of smart hotel rooms.

2. IoT ecosystem for enterprises and trends

Moore [11] suggests that an enterprise be viewed not as a member of a single industry but as part of a business ecosystem that crosses a variety of industries. The ecosystems can generally have either hub-centered star structure or a flat mesh-like structure [12]. The star structure can be found in the US where IoT ecosystems are created around major IT companies such as Google, Amazon, Facebook, and Apple which interact with a large number of small companies, but the flat mesh-like structure of the ecosystem is found in the Europe Union where the IoT ecosystem consists of small and agile companies [13].

An enterprise ecosystem helps enterprises work cooperatively and competitively among themselves to support new products/services, expand markets, and stimulate innovations. Mazhelis et al. [12] define an IoT business ecosystem as a special type of business ecosystem which is comprised of interacting IoT-related companies and individuals along with their socio-economic environment. They suggest the community of an IoT ecosystem consists of software platform providers, hardware platform providers, and the standards. In an enterprise IoT ecosystem, cross-industry stakeholders can add value to the ecosystem [14]. Since typical IoT services require integration of multiple devices and software modules often made by different vendors, most enterprises do not have the technical expertise required to develop the needed services. The understanding of the enterprise IoT ecosystem will help them leverage the right IoT platforms for the service development. For example, enterprises in supply chain management (SCM) would attempt to leverage SCM-related IoT platforms to develop the IoT services quickly and inexpensively [15].

2.1. Key players of the enterprise IoT ecosystem

An enterprise IoT ecosystem consists of a large number of stakeholders such as platform providers, thing providers, developers, and users [16]. Based on the survey of industry practices, this paper identifies five key players of the enterprise IoT ecosystem: (1) software platform developers (e.g., data platform developers, security platform developers, cloud service providers), (2) hardware platform developers (e.g., board manufacturers, controller developers, gateway device manufacturers, sensor manufacturers, device manufacturers), (3) network technology developers (e.g., telecom companies, connectivity platform developers, data network developers), (4) application/solution developers (e.g., data analytics developers, applications developers, system integrators), and (5) users and customers (e.g., corporate users, corporate customers, individual customers). These key players symbiotically and synergistically contribute to the innovation, expand markets, facilitate collaboration and competition in the industries, and ultimately benefit enterprises, users, and customers. Fig. 1 shows the five key players of the enterprise IoT ecosystem.

2.1.1. Software platform developers

IoT applications share a substantial part of their core functionalities. Packing those common functionalities into an IoT software platform enables IoT application developers to concentrate on the unique customizable aspects of their application, prevent unnecessary redundancy and duplication in application development [17], and reduce the complexity in developing, deploying, and managing IoT applications during the application lifecycle [18]. IoT software platforms include data platforms, security platforms, cloud-based platforms, and OS platforms.

IoT data platforms have been developed in both academic and industrial settings in order to facilitate IoT data management tasks such as cleaning, transforming, and storing data, especially in the context of big data [19]. The fusion of big data and IoT through IoT data platforms can provide new dimensions and opportunities for future generations of different services in the healthcare, finance, security, transportation, and education fields [20].

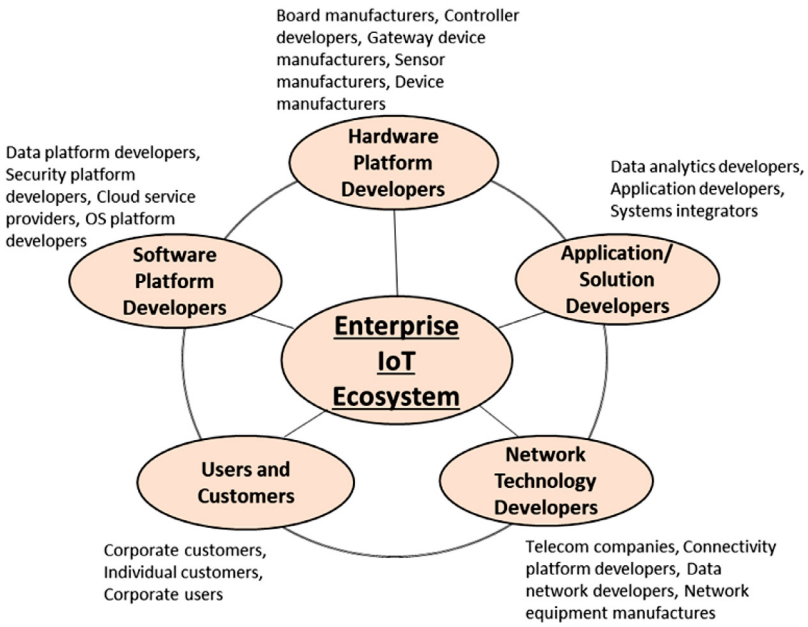

Fig. 1. The five key players of the enterprise IoT ecosystem.

Cloud computing has virtually unlimited capabilities in terms of storage and processing capacity, complements the IoT, and solves some of the IoT issues [21]. The IoT platform in the cloud plays the role of interpreter and distributor, storing data from a variety of devices and machines and sending them through gateways to the services chosen for processing [22]. For example, Bruneoet al. [23] integrated IoT infrastructure with OpenStack's cloud platform to develop a smart city project so that both IoT and server-class infrastructure are leveraged, abstracted, virtualized, and ultimately exposed in a homogeneous fashion through standardized APIs. Cloud service providers (CSPs) such as Microsoft, IBM, Amazon, and Google have lowered technology barriers to enterprises' IoT adoption by simplifying the IoT application development and providing the best practices at lower costs. Unlike traditional OSs, the OS for IoT devices should have a lightweight design, thus enabling the low code size, low complexity, and low power consumption [24]. For example, Google's Brillo OS is a lightweight version of Android that supports various IoT devices from different manufacturers as well as Wi-Fi, Bluetooth, and low-power communication protocols.

Many IoT software platforms provide such services as programming frameworks, machine-to-machine (M2M) integration, data and device management, security and storage, and protocol translation [25]. A number of researchers suggest desirable characteristics and functions of the IoT platforms. For the platforms to be attractive to application developers, platforms should be open, useful, easy-to-use, and API-enabled [10]. Lee et al. [26] suggest that software platforms (1) be programmable with an easy programming language, (2) provide high-level APIs for functions such as sensor and device management and communication, (3) support concurrent execution of multiple IoT applications with different functions, and (4) enable the companion IoT device to communicate with its host device (e.g. Android smartphone) and to be controllable via its host device. Yun et al. [27] suggest that an IoT software platform support portability across different hardware and operating systems, provide developers with an abstraction layer that can hide the complex underlying systems, and allow transparent access to a set of useful APIs for applications.

2.1.2. Hardware platform developers

Small, easy-to-use, and inexpensive hardware platforms have contributed to the rapid development of the enterprise IoT. Hardware platforms include IoT prototyping kits and off-the-shelf boards that are built with microcontrollers, processors, and other components. These platforms monitor physical events or may be connected to larger systems with the aim of extracting monitoring data [28]. Some of the popular IoT platform boards include Espressif ESP8266 boards, Raspberry Pi Compute Module 3 (CM 3), Intel Edison Compute Module, Adafruit Feather boards, Arduino IoT Product Line, Particle Wi-Fi IoT hardware, and littleBits [25]. IoT hardware platforms also include PCs, tablets, smartphones, sensors, actuators, and peripheral devices that are often built from various components. An important requirement in designing the IoT hardware platform is energy efficiency made possible by the miniaturization of hardware. Gardašević et al. [24] give a good overview of various hardware platforms. IBM, Intel, Arduino, and Raspberry Pi are some of the leaders in the IoT hardware platform market.

Many off-the-shelf IoT microcontrollers and single board computers are designed around system-on-a-chip (SoC) ICs which pack a variety of components onto a single chip such as a central processing unit (CPU), memory, input/output

ports, secondary storage, and networking units. Many specialty IoT devices based on commercial off-the-shelf boards quickly reach limits in speed, power consumption, and device size. To design more efficient IoT devices with tightly integrated chips, smaller PCBs, and lower overall cost per-device, developers often consider high-performance platforms that consist of graphics processors or fixed-function implementations in field-programmable gate array (FPGA) or application-specific integrated circuit implementations [29].

Sensors are another important hardware for collection of data from environments in real time. Some IoT sensors are connected to an IoT controller device where a certain event or information triggers an action [30]. Because battery-powered sensors have a limited energy lifespan, various energy-harvesting methods have been developed (e.g., solar energy using solar cells and solar thermoelectric generators, mechanical energy, and wind energy) [31]. Due to the challenges of integrating various proprietary hardware platforms for inexperienced developers, open-source hardware platforms gain popularity in the development of diverse and novel IoT applications [32].

2.1.3. Network technology developers

Major telecom operators, connectivity platform developers, data network developers, and network device manufacturers are frontiers of the IoT network technologies such as Bluetooth Low Energy (BLE), Zigbee, and low-power wide-area (LPWA) networks. Typically, device-to-device (D2D) / machine to machine (M2M) communication involves direct short-range communication between devices without the support of a network infrastructure [33]. One of the most popular D2D communication platforms for enterprise applications is Zigbee, which is a low-power, low data rate, and close proximity wireless ad hoc network. It is a short-range wireless communication protocol based on the IEEE 802.15.4-based specification, which is widely used in home automation and the industry where low power is required and data exchange is infrequent and low. Bluetooth, Radio Frequency Identification (RFID), and Near Field Communication (NFC) are also widely used for short range connectivity for devices.

On the other hand, for the wide area network for long-range IoT communications, low-power wide-area (LPWA) technologies such as NarrowBand-Internet of Things (NB-IoT), Long Term Evolution for Machines (LTE-M), Sigfox, and LoRa are presently some of the key technologies. LPWA is suitable for the IoT applications that only need to transmit tiny amounts of information in a long range [34]. NB-IoT is an LPWA cellular IoT technology developed to connect a wide range of IoT devices and services with spectrum efficiency and deep coverage. While unlicensed LoRa has advantages in terms of battery lifespan, capacity, and cost, licensed NB-IoT offers advantages in QoS, latency, reliability, and range [34]. It is noted that no one-size-fits-all network technology exists since different IoT applications have different business and technical requirements in networking.

The fifth generation (5G) networks, a new generation in cellular mobile and wireless technology, are expected to be launched in 2020. The 5G technology can significantly expand the realm of the IoT applications and will enable massive IoT devices to interact each other in a new environment [35]. There is an anticipation that the 5G will meet the needs for high data rates, low latency, cost-efficient energy consumption, high scalability, improved connectivity, and high network security [36]. The 5G provides three categories of services with different performance requirements: enhanced mobile broadband (eMBB), massive machine-type communication (mMTC), and ultra-reliable low latency communication (UR-LLC) [37]. However, 5G-enabled IoT still lacks sufficient security and privacy guarantees after logical network slices and fog computing are built for individual services, which may impede the success of both the 5 G network and IoT applications [38].

2.1.4. Application/Solution developers

Third-party developers, systems integrators, and in-house developers often use various IoT platforms to develop domain-specific applications/solutions. Due to their complex, distributed nature, IoT applications/solutions are time-consuming to develop, are unreliable, and are not readily scalable. Furthermore, many enterprise IT professionals lack technical capabilities to develop end-to-end solutions for interconnected devices which often require middleware for inter-device integration and communications. To overcome this critical challenge, it is crucial for developers and engineers to leverage platforms to construct, benchmark, and optimize applications and services [39]. Developers are leveraging interoperable open platforms by composing IoT software and hardware platforms for different IoT services. For example, a developer may choose to integrate Microsoft Azure IoT Starter Kit with Cisco Fog and Intel Edison Compute Module to create a remote monitoring solution.

The co-existence of various kinds of devices, protocols, architectures, and programming languages make IoT systems complicated to develop even for experienced developers due to the lack of documentation from technical and conceptual perspectives [40]. Hence, systems integrators are important players in application/solution development due to their vast experience in integrating IoT solutions across manufacturers and industries. Enterprises oftentimes seek the advice of systems integrators to find architectural components and develop applications for users and customers. ABI Research [41] forecasts that IoT systems integration and consulting revenue will grow to over US$35.7 billion in 2022 from less than US$17 billion in 2017 at a compound annual growth rate of 16.1%.

2.1.5. Users and customers

Enterprises provide IoT-based services to users and customers to improve their business operations and customer services. Users and customers are both the beneficiaries and sources of revenues that keep the IoT innovation moving forward. Some of the ways IoT supports users and customers include improving machine maintenance, tracking ships and vehicles,

assisting customers' shopping, gaining efficiencies in checkout operations, and managing office security and utility [42–44]. Acceptance of IoT services by users and customers are critical for the IoT investment to fulfill its full potential. A recent study shows that perceived usefulness and perceived enjoyment of IoT services positively affect behavior in using IoT services, but perceived privacy risk negatively affects IoT adoption [45]. It is noted that these results are consistent with results of many other technology adoption studies.

2.2. Enablers of the IoT ecosystem

The IoT ecosystem has been evolving and growing over time. An enabler facilitates the change process. Therefore, identification and proactive management of enablers are critical for the growth of the ecosystem. Based on the survey of literature, this paper identifies interoperability and security/privacy as enablers of the IoT ecosystem. A recent survey on the interoperability and security in the IoT can be found in Di Martino et al. [46].

2.2.1. Interoperability

According to a McKinsey analysis [47], a substantial threat to the predicted economic value of IT is a lack of interoperability and 40% of the potential benefits of the IoT can be realized with the interoperability between IoT systems. Many IoT platforms and devices have been developed in the past, but most platforms were developed with proprietary technologies [48]. These proprietary platforms make it difficult to extend systems to support new services, integrate new data, and interoperate with other IoT systems [49]. Some of the proposed interoperability handling approaches include adapters/gateways, virtual networks/overlay-based solutions, software-defined networking (SDN), IP-based approaches, network function virtualization, open API, service-oriented architecture (SOA), semantic web technologies, and open standard [50].

One of the promising interoperability handling approaches is standardization. Standardized common functionalities enable enterprises to create interoperable applications and solutions. Leading IT firms have created various industry alliances to establish standards and device interoperability. An industry alliance called the Thread Group (http://www.threadgroup.org). addresses the interoperability challenge by providing a certification program that validates a device's conformance to the specification as well as its interoperability against a blended network comprised of multiple certified stacks. The Alliance for Internet of Things Innovation (AIOTI) was initiated by the European Commission in 2015 with the aim of creating a dynamic European IoT ecosystem between the different IoT players such as large companies, SMEs and startups as well as well-known European research centers, universities, associations, and public bodies (https://aioti.eu/). The Alliance also aims to foster experimentation, replication, and deployment of IoT and support convergence and interoperability of IoT standards. The oneM2M is a global partnership established by eight ICT standard development organizations (SDOs) to standardize a M2M service layer platform that can be readily embedded within various hardware and software, and relied upon to connect devices with M2M application servers (http://www.onem2m.org/). Currently, there are nearly 200 corporate members from all industrial sectors. oneM2M specifications provide a framework to support applications and services such as utilities, transportation, healthcare, industrial automation, smart homes, connected cars, and public safety.

Governments need to set policies and regulations on IoT-enabled services to achieve their full economic and societal potential. Governments and other policy-making organizations can proactively support the development of interoperability standards for IoT devices and systems. They also need to address intellectual property rights and licensing to facilitate the adoption of the standards by the industries.

2.2.2. Security/Privacy

Security and privacy concerns are a major hindrance to the adoption of IoT-enabled services. Security and privacy are all the more important in the context of enterprises. Working and living in a space that is filled with sensors and cameras that monitor every action open up opportunities for cybercriminals [51]. A lack of security in enterprise IoT systems can also provide intruders with access to sensitive customer data related to privacy and business transactions. Trust in and adoption of the IoT services depends on the security/privacy protection they provide. As the growing number and variety of connected devices are introduced into the IoT networks, the potential security threats grow exponentially. Some of the IoT applications are used to monitor high security infrastructures such as the smart grid and hazardous material production facilities. Other IoT applications collect sensitive personal data such as person's location, health and wellness, and purchasing behavior that enterprises want to analyze. The potential threat on the security of these applications may be alleviated by establishing IoT security protocols such as authentication, authorization, access control, and non-repudiation and incorporating security protection mechanisms such as data encryption, firewalls, and security analytics into the IoT systems.

Incorporating privacy requirements in the very early stages of the IoT development is essential for creating sufficient public confidence and facilitating the adoption of IoT systems [52]. Many IoT devices are low energy and lightweight. These devices devote most of their available energy and computation resources to supporting core functions, making the task of supporting security and privacy quite challenging [53]. The IoT can utilize blockchain in securing many IoT-oriented applications by publishing and storing data as a public ledger that is infeasible to modify since every user or node in the system retains the same ledger as all other users or nodes in the network [54]. Blockchain provides decentralized security and privacy, but involves significant energy, delay, and computational overhead that are not yet suitable for most resource-constrained IoT devices [53]. While blockchain is likely to play an important role in the IoT security, these technical challenges will have to be overcome before a wide adoption of blockchain in the IoT takes place.

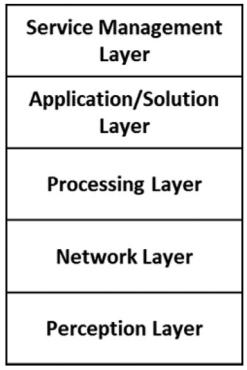

Fig. 2. Five-layer architecture of the enterprise IoT.

Governments can play a significant role in addressing security concerns related to the use of IoT services. In the US, as of July 2018, three pending bills were proposed [55]. The Cyber Shield Act of 2017 (S. 2020, 115 Cong. (2017)) is a voluntary bill where manufacturers of IoT devices adhere to certain IoT security protocols and in return are given government certification that their devices are secure. Another voluntary bill, the Internet of Medical Things Resilience Partnership Act of 2017 (the Medical Things Act) (H.R. 3985, 115 Cong. (2017)), would establish a working group of public and private entities led by the Food and Drug Administration (FDA) to recommend voluntary frameworks and guidelines for the security and resilience of Internet of Medical Things devices. The Cybersecurity Improvement Act would require a vendor of IoT devices to meet certain criteria before a U.S. government agency can purchase the device. The legislation requires that the IoT devices are patchable, do not contain known vulnerabilities, rely on standard protocols, and do not contain hard-coded passwords.

3. Architecture of enterprise IoT

Architectural aspects of the IoT is an actively studied research area. Overall, architecture has a significant bearing on the field itself and needs to be investigated [56]. A well-structured architecture of the IoT will help enterprises create innovative services. The enterprise IoT ecosystem discussed in the previous section provides the technology platforms needed for the implementation of the architecture of the IoT. While there is no agreed architecture of the IoT among researchers, they typically employ a multi-layered approach, with each layer dedicated to certain functions such as communication/sensing, data processing, and knowledge processing/reasoning [57]. For successful IoT service development, IoT architecture needs to be established and updated continuously to commission and decommission various IoT assets and services. A three-layer architecture was proposed in the early stage of the IoT evolution [58,59]. Chen et al. [60] propose the architecture for the IoT with three basic layers (a perception layer for data collection, a network layer for data transmission, and an application layer for object recognition and inter-object relationship). With the advances in the IoT, researchers proposed four-layer and five-layer architectures [61–63]. The five-layer architecture adds a processing layer and a business layer on top of the three-layer architecture.

The above mentioned five-layer architecture presents common layers for many domain areas. However, the five-layer architecture does not reflect the nature of the enterprise IoT environment. To take into consideration unique services of enterprise IoT, we present a modified five-layer architecture of enterprise IoT as shown in Fig. 2. The five-layer architecture of the enterprise IoT represents an abstract architectural view for a myriad of the enterprise IoT systems.

The architecture of the enterprise IoT consists of a perception layer, a network layer, a processing layer, an application layer, and a service management layer. While the perception layer, network layer, processing layer, and application layer of the architecture of enterprise IoT are the same as those of the existing five-layer architecture, the service management layer replaces the business layer of the existing five-layer architecture. The architecture of enterprise IoT enhances the usability of the architecture for enterprises and ensures that a variety of enterprise applications seamlessly connect a myriad of enterprise IoT devices and can be accessible to users and customers. In the following, the modified five-layer architecture is presented with a detailed discussion on the application layer and the service management layer.

3.1. Perception layer

The perception layer plays a sensing role for the back-end IoT system. It is also known as a sensor layer. The perception layer consists of different devices such as sensors, RFID tags and readers, video cameras, and smart phones which are used to identify objects and locations and collect data from the surrounding environment. The perception layer often generates enormous quantities of data that need to be aggregated and analyzed to respond to various triggering events in real time.

3.2. Network layer

The network layer, also known as transmission layer, transmits data collected from the sensors to the processing layer over various networks. It acts as a bridge between the perception layer and the application layer. This layer provides the infrastructure to support wireless or wired connections among devices. The network layer uses Internet gateways, switching, and routing devices along with communication technologies such as WiFi, LTE, Bluetooth, 3G, and Zigbee [64]. The deployment, management, and scheduling of networks are essential for the network layer [65].

3.3. Processing layer

The processing layer, also called the middleware layer, cleanses, stores, analyzes, and processes data that are transported from the network layer. The processing layer contains such platforms as database management, data analytics, and cloud computing. Due to the big data generated from the IoT devices, many IoT applications require massive data storage, huge processing speeds to enable the real time decision making, and high-speed broadband networks to stream data, audio, or video [1]. Cloud computing became a suitable technology for handling huge data streams and processing them for the massive amount of IoT devices in real time. A complex distributed infrastructure of the IoT requires simplifying the development of new applications and solutions. The processing layer can hide the details of platforms and is ideal for IoT application development.

3.4. Application layer

The application layer consists of a set of problem-specific applications/solutions that interact with users, solve problems, and share problems and solutions with other applications. The application layer is also responsible for integrating data and information and presenting them to the users in a user-friendly format. At the application layer, key requirements such as accuracy, energy efficiency, and low-latency may vary depending on the type/sector that the IoT application is developed for [66]. To facilitate application development with heterogeneous devices at the application layer, a number of application layer protocols are utilized [67]. Among them, most of the popular IoT applications use either Constraint Application Protocol (CoAP) or the Message Queue Telemetry Transport (MQTT) [68].

The application layer facilitates the development of myriads of enterprise IoT applications. It is necessary for managers to understand what types of enterprise applications are provided at the application layer. Lee and Lee [1] identified three categories for enterprise IoT applications: monitoring and control, big data and business analytics, and information sharing and collaboration. To reflect more recent developments in the enterprise IoT applications, this paper presents more comprehensive categories: (1) operational enterprise IoT, (2) analytical enterprise IoT, and (3) collaborative enterprise IoT.

3.4.1. Operational enterprise IoT

Operational enterprise IoT applications are used to support or improve day-to-day user and customer activities. This paper identifies three types of operational enterprise IoT applications: monitoring and control, automation, and process management.

Monitoring and control: Monitoring and control applications collect data on equipment performance, energy usage, health conditions, and environmental conditions, and allow controllers to send alerts for anomalies and possibly deliver a solution in real time anywhere, anytime. In the manufacturing area, an IoT application may be used to monitor machines and detect abnormal or undesirable operations at a manufacturing facility. Health monitoring is another promising application area. A personal health monitoring system monitors an individual user's health condition real time and notifies the user when a change of the condition needs attention [69]. Smart medicine-boxes can remind patients of their dosage and interact with body sensors to efficiently monitor and plan any change in the dosage [70]. Retailers are deploying smart-shelves to keep track of stocks to detect potential theft and misplacement.

Automation: With the advancement of the IoT, enterprises are developing IoT applications for automation purposes. For example, an IoT office automation system enhances the safety of employees and energy efficiency for the company by automatically regulating the use of electricity for heat, lights and many other office appliances. Retailers gain efficiencies through IoT-enabled checkout automation. Amazon automated its checkout at Amazon Go stores in 2018, utilizing IoT-based sensor technology and computer vision technology. Other major retailers are also experimenting with cashier-free check-out using cameras, sensors, and RFID.

Process management: The integration of IoT applications into core business processes is important in enhancing the operational value of enterprise IoT. It is important to identify the types of IoT applications that influence the effectiveness and efficiency of business processes. For example, with beacons that connect to mobile phones to track customers within the store, retailers can launch custom promotions in real time, texting personalized coupons to encourage in-store purchases. A store layout can be optimized by analyzing the vast streams of data about customers' movements at the store. An internal value chain would be improved by using IoT-enabled inventory management. Enterprises even achieve green manufacturing by reducing energy for manufacturing operations with responsive lights for production spaces, smart washing machines, and energy-efficient thermostats [71].

3.4.2. Analytical enterprise IoT application

IoT devices and machines generate enormous amounts of data and transmit them to the business intelligence and analytics tools for human decision making. These data are analyzed to discover and resolve any business issues such as changes in customer behaviors and market conditions, to increase customer satisfaction, and to provide value added services to customers. This paper identifies two types of analytical enterprise IoT applications: diagnostic IoT application and predictive IoT application.

Diagnostic IoT application: Business analytics tools may be embedded into IoT devices such as wearable health monitoring sensors so that real time decision making can be made at the source of data. The IoT and advances in business analytics now make it possible to analyze vast amounts of individual health data and provide diagnostics. Real-time production dashboards bring together the vast streams of data generated by sensors throughout the operation, providing a comprehensive view of whereabouts and conditions of individual machines and equipment at any given time. Diagnostics can improve visibility, responsiveness, decision-making, quality control, and safety [72]. IoT applications can also measure performance indicators, such as fuel consumption and driving distance of automobiles, and provide diagnostics to reduce fuel expenses [73].

Predictive IoT application: Predictive IoT applications discover operational patterns, spot areas of potential improvement, or predict future outcomes, leading to lower cost and higher productivity. Predictive IoT applications utilize vast amounts of data to help construct predictive pricing models based on customer preferences, as well as the usage context which can benefit both companies and consumers [74]. Smart grid and smart metering systems may collect usage data and environmental data and utilize predictive analytics to discover usage patterns and forecast the future utility demand.

3.4.3. Collaborative enterprise IoT

Collaborative enterprise IoT applications allow different IoT devices to interact and collaborate to achieve specified goals. They share some common characteristics with social IoT (SIoT) in that different IoT devices interact and establish relationships with each other to achieve some specific goals. However, collaborative enterprise IoT applications are typically operated under a single governing body of the applications, whereas there are multiple owners/entities interacting through their devices in the social IoT (SIoT).

Collaboration in the IoT system can occur between people, between people and things, and between things. The IoT can go beyond systems within individual plants to connect multiple plants in different regions [72]. The IoT helps supply chain partners collaborate with each other for a supply chain execution in real time and improve the efficiency and effectiveness of supply chain [75].

Sensing a predefined event is usually the first step for collaboration. In the supply chain area, information sharing and collaboration enhance the situational awareness and avoid information delay and distortion. The IoT can provide a vastly improved retail ecosystem that can enhance the retailers' ability to create value, competitiveness, and business performance [76]. Multiple IoT devices are often used to collaborate with each other for retail store management. For example, if there are sensors throughout a retail store, they can send alerts to the store manager's mobile device whenever refrigerators they are monitoring go out of function. The manager can then look on the employee status report to find who is available. The employees will receive the manager's task assignments via their mobile devices. Another collaborative usage scenario is the use of smartphones, sensors, and RFID. A customer enters a shopping mart's premises and turns on her smartphone app. The smartphone app interacts with a refrigerator at home to provide a check-list of required grocery items. It then collaborates with the store inventory system to find the location of these items. Once the customer picks up the items, the invoice is delivered to the smartphone and the customer then proceeds with the amount payable using his/her online credit card [77].

3.5. Service management layer

The top layer of the enterprise IoT architecture is the service management layer which is responsible for the selection and delivery of the IoT services of the enterprise. The service management layer is a starting point for developing a set of enterprise IoT services. In this paper, service management refers to the activities and supporting procedures that are performed by an organization to plan, design, implement, operate, and improve enterprise IoT services used by customers. IoT services refers to activities performed to create values for users and customers through the use of applications/solutions. Any domain-specific IoT services should support high-level enterprise strategies. IoT services create value for the users and customers which can be measured by the user's willingness to pay and reuse the services.

The service management layer provides the direction for the four lower-level layers. A key element of the service management layer is the IoT service business model. However, there are only few studies focused on the IoT business models. The Business Model Canvas [78] was applied to model several IoT business models (e.g., [74–82]). Based on the survey of the literature, this paper proposes the IoT service business model.

4. IoT service business model

Based on the literature review on the business model components, we derive four essential components of the IoT service business model: value proposition, networked activities, resources, and sustainability.

4.1. Value proposition

Value proposition refers to a substantial value of a product/service to a target customer for which the customer is willing to pay [83]. The value proposition of the IoT services needs to be compelling to users and customers, achieve cost savings, and/or contribute to revenue generation. Dijkman et al. [79] find the value proposition is the most important component of the IoT business model and identify the following as important types of value proposition: convenience/usability, getting the job done, performance, possibility for updates, and comfort. The value proposition from IoT services is derived when new services or new values are perceived by users and customers from the adoption of IoT services. For example, an IoT-enabled smart hotel room will enhance the convenience and comforts of hotel customers.

4.2. Networked activities

A network refers to a network of platform developers, partners, device suppliers, and other enterprises that add value to the development of the IoT services. Dijkman et al. [79] identify software developers, launching customers, data scientists, and hardware producers as important participants in the network. Value is co-created by the activities of the participants in the network [84]. Therefore, participants in the value network should be concerned about improvement of any networked activities. The significance and weight of network participants are measured based on the magnitude of their value addition to the IoT service development.

4.3. Resources

This component allows enterprises to assess sustainable and developmental resources and to examine these resources in terms of the opportunities and threats for establishing a competitive advantage from the IoT service development. From a resource-based view, every enterprise has a unique set of resources that the firm can leverage to exploit opportunities and counter threats [85]. Two important questions for enterprise to develop the IoT service are: (1) what kinds of existing resources the enterprise can leverage to deliver the IoT services and (2) what resources it needs to differentiate itself from the competitors. The key resources of enterprises include the employees, technologies, products, services, facilities, equipment, marketing channels, and brand. Acquiring and retaining resources for the success of the IoT services are key resource development activities.

4.4. Sustainability

To meet the stakeholders' needs in the future, sustainability is concerned with managing triple bottom lines, frequently referred to as profit, people, and planet. Sustainability is becoming an integral part of business models in a drive to achieve long-term corporate growth and profitability and to fulfill environmental and social responsibilities at the same time. Therefore, the development of IoT services should take into consideration the impacts on people, planet, and profit. For example, to balance people, planet, and profit, sustainable enterprises need to consider the impact of manufacturing IoT services on environments to achieve less waste production, a less polluted environment, and socially responsible business practices.

By integrating sustainability into IoT service decision-making, enterprises are more likely to include economic, environmental, and social considerations in all aspects of services on an ongoing basis. In addition, profit is generated through an extended timeline for the return on investment and profit formula which defines how the enterprise creates net value from the IoT services to the users and customers. On the cost side there are IoT service development costs and on the revenue side there are subscription fees, usage fees, and asset sales, which all serve as important types of sustainability [79]. Although IoT services may require initial investment costs, the value they create may eventually pay off [1]. The investments in IoT-enabled green manufacturing typically lead to enhanced brand and public relations, which in turn lead to increased revenue and profit. For long-term sustainability, the value created from offering the IoT services to the users and customers should be greater than the cost of providing the services.

5. Illustration of IoT service business model

According to Iansiti and Lakhani [2], adopting the IoT in the modern economy will allow firms to achieve competitive advantage. Some of the value creation include superior experience for customers and users, positive impact on marketing and advertising, and greater efficiency and responsiveness in manufacturing. The development of any enterprise IoT services will be driven by the guide of the IoT service business model at the service management layer. Once a desired service is identified, the IoT architecture will be implemented to fulfill the requirements of the enterprise IoT service. The following illustrates the use of the IoT service business model with a real case of the smart hotel room development at Marriott International (see Table 1).

Marriott International has teamed with two IT companies, Samsung and Legrand, to develop a smart hotel room [86]. Marriott's Innovation Lab came up with a value proposition that has the potential to elevate the guest experience, create more efficient hotel room design and construction, and contribute to Marriott's global sustainability efforts and goals. Some of the expected benefits of the smart hotel room include customers' integrated experience with access to their own data

Table 1
The use of IoT service business model.

Model component	Architectural requirements
(1) Value proposition: Elevate the guest experience, create a more efficient hotel room, and contribute to Marriott's global sustainability efforts and goals.	Hotel owners would have a seamless, transparent, and flexible end-to-end solution that requires minimal equipment, while customers would enjoy an integrated experience with access to their own data and information, as well as accessible voice and mobile-optimized controls.
(2) Networked activities: Create a partnership with Samsung and Legrand. Samsung develops an end-to-end IoT service from intuitive lighting to voice-activated room controls powered by the ARTIK platform and the SmartThings Cloud. Legrand offers a suite of power, light, and data solutions that bring power and connectivity to previously untapped locations.	HVAC, lighting, drapery, and DND/MUR from the Samsung Smart Hospitality & TV content management solution. Reliable Wi-Fi-enabled devices powered by Samsung's WLAN Solution. Wireless Digital Lighting Management (DLM) solutions. End-to-end security, authentication, and access management. APIs, which allow Amazon's Alexa to "talk to" IoT devices (e.g., thermostats and lights in hotel rooms).
(3) Resources: Marriott capitalizes on the recent extension of VMware's partnership with IBM Cloud. Service-oriented IT model that would securely extend its on-premises data center into the public cloud and enable a variety of new digital experiences. More than 20,000 devices are equipped with enterprise mobility management software to help ensure its mobile workforce can reliably serve customers anytime, anyplace. IP-based infrastructure that enables in-room TVs to communicate with the hotel's property management system (PMS).	A virtualized, software-defined and automated data center environment. A distributed antenna system (DAS) with private LTE solutions, which provide a hotel with its own cellular network machine-to-machine (M2M) communications and 5G cellular fully fiber base. Cloud-based monitoring and remote-management system that enables staff to monitor activity. DLM sensors and switches two-way infrared (IR) communication that enables personal control from handheld remotes.
(4) Sustainability: IoT-enabled building management, guest room management, power management, and lighting control software and hardware reduce the environmental footprint for water/carbon/waste/food waste and contribute to the goal of reducing environmental footprint by: Water: Reduce water intensity by 15% Carbon: Reduce carbon intensity by 30% Waste: Reduce waste to landfill by 45%. Reduce food waste by 50% Renewable energy: Achieve a minimum of 30% renewable electricity use	Mobile and voice-enabled technology to give guests and staff the ability to set up the room to best meet their need and optimize hotel operations. System integration in automation and connectivity for optimal efficiency and comfort.

Sources: https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/customers/vmware-marriott-17q1-casestudy.pdf.
http://serve360.marriott.com/wp-content/uploads/2018/10/2018_Serve_360_Highlights.pdf.

and information, accessible voice and mobile-optimized controls, and improved personalized service. The Lab brings together multiple IoT systems, devices, and applications for device-to-device communications. Samsung develops end-to-end IoT services from intuitive lighting to voice-activated room controls powered by the ARTIK platform and the SmartThings Cloud. Legrand offers a suite of power, light, and data solutions that bring power and connectivity to previously untapped locations. Marriott has well-established private data centers extending into the public cloud and more than 20,000 devices are equipped with enterprise mobility management software to help ensure its mobile workforce can reliably serve customers anytime, anyplace. IoT-enabled building management, guest room management, power management, and lighting control software and hardware reduce the environmental footprint for water/carbon/waste/food waste and contribute to the goal of reducing environmental footprint and sustainability. The management team believes that value creation opportunities of the smart hotel room project is justified in terms of environment and social impacts, profitability, and competitive advantage in the hospitality industry.

6. Conclusion

Because the IoT is such a recent development, there remain a paucity of studies on the enterprise IoT. This makes it very challenging for enterprises to make informed decisions in regard to IoT service development. Our study fills a current gap in the enterprise IoT research and intends to stimulate further interest in this area for anyone interested in the enterprise IoT research and practices.

This paper discusses an IoT ecosystem, an IoT architecture, and IoT service business model for enterprises essential for deployment of successful IoT-enabled services. The enterprise IoT ecosystem consists of five key players: (1) software platform developers, (2) hardware platform developers, (3) network technology developers, (4) application/solution developers, and (5) users and customers. The architecture of the enterprise IoT consists of perception layer, network layer, processing layer, application layer, and service management layer. This paper presents three categories of IoT applications: operational enterprise IoT, analytical enterprise IoT, and collaborative enterprise IoT. Recognizing that many enterprises invest in a variety of IoT services for their business model innovation, this paper discussed how the IoT services contribute to business model innovation in terms of the four components of the IoT service business model: value proposition, networked

activities, resources, and sustainability. Then this paper illustrates the use of the IoT service business model for a smart hotel room development.

The IoT ecosystem provides a valuable source of insightful data to assess the prospects of the IoT sector. Enterprises need to constantly watch out for newly developed technologies to adapt to the disruptive nature of IoT innovation and offer new and transformative IoT services. Along with innovative IoT technologies and tools 5G cellular technologies and solutions are anticipated to provide substantial opportunities and challenges for enterprise IoT development. A recent Business Insider's survey shows that nearly half of IoT providers plan to introduce support for 5G networks to their solutions within the next two years and companies' plans to invest in IoT solutions will accelerate due to 5G [87]. Furthermore, 5G will accelerate the adoption of fog computing in the IoT ecosystem to meet the need for improved QoS, reduced latency, high mobility, high scalability, and real time execution of applications and services [88]. Fog computing will become a promising solution for the processing of big data and 5G-enabled IoT services such as self-driving cars, segmented reality and virtual reality, and smart cities by moving computing resources to the network edge.

Choosing an IoT platform is an important decision to make and requires leveraging the IoT ecosystem properly for many IoT enterprise applications and service development. Most of the platforms in the IoT ecosystem are built to support a wide variety of applications and service needs but differ in performance, security, customizability, ease of use, and device management. While many applications need standardized, low-performance, and low-power IoT platforms, there is still a significant need for high-performance platforms in order to meet computational needs of data-intensive IoT applications and edge devices [89]. To choose the right IoT platform, application developers need to take into consideration: (1) scalability to handle rapid increases of data and growth of the number of connected devices, (2) edge computing to extend the power of the cloud to mobile and IoT devices, (3) cloud infrastructure to fit in with existing IT systems such as the hybrid cloud to take advantage of the ease of accessibility of the private cloud and scaling capabilities of the public cloud, (4) disaster prevention and recovery such as disaster recovery plans, security measures and data backup plans, and (5) communication protocols and standards with support for upgraded versions of these protocols or newer protocols with ease [90].

In addition to the proper platform choice, enterprises need to decide if they will deploy their own private IoT infrastructure, third party IoT infrastructure, or a hybrid of the private and third party IoT infrastructure. There are also quantitative and qualitative evaluations that an enterprise must consider regarding the IoT infrastructure decision. The quantitative evaluation focuses on the total cost of the infrastructure related to hardware, software, labor, and maintenance, and compares the total costs of alternative infrastructure choices. The qualitative evaluation helps enterprises identify and compare some of the intangible benefits and risks such as the time-to-market of an IoT solution, level of customization required, in-house competencies, compliance and security, and expectations for ongoing support [91].

The next decade will witness the explosion of the IoT applications for enterprises. Since the IoT became a reality beyond hype, managers need to understand the ecosystem, architecture, and business model to become a better problem solver in the IoT-enabled innovations. Our study contributes to the literature in this emerging field by presenting a foundational knowledge for building smart enterprises.

Declaration of interests

None.

References

[1] I. Lee, K. Lee, The Internet of Things (IoT): applications, investments and challenges for enterprises, Bus. Horiz. 58 (4) (2015) 431–440.
[2] M. Iansiti, K.R. Lakhani, Digital ubiquity: how connections, sensors, and data are revolutionizing business, Harv. Bus. Rev. 92 (11) (2014) 91–99.
[3] M.E. Porter, J.E. Heppelmann, How smart, connected products are transforming competition, Harv. Bus. Rev. 92 (11) (2014) 64–88.
[4] A. Bosche, D. Crawford, D. Jackson, M. Schallehn, C. Schorling Unlocking opportunities in the Internet of Things, (2018) Available from https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things/
[5] J. Greenough The corporate 'Internet of Things' will encompass more devices than the smartphone and tablet markets combined, (2015) Available from https://www.businessinsider.com/the-enterprise-internet-of-things-market-2014-12
[6] M. Chui, V. Ganesan, M. Patel Taking the pulse of enterprise IoT, (2017) Available from https://www.mckinsey.com/featured-insights/internet-of-things/our-insights/taking-the-pulse-of-enterprise-iot
[7] D. Shin, An exploratory study of innovation strategies of the internet of things SMEs in South Korea, Asia Pac. J. Innov. Entrep. 11 (2) (2017) 171–189.
[8] F. Terroso-Saenz, A. González-Vidal, A.P. Ramallo-González, A.F. Skarmeta, An open IoT platform for the management and analysis of energy data, Future Gener. Comput. Syst. 92 (2019) 1066–1079.
[9] P. Scully Microsoft and PTC named leading IoT platform vendors for cloud and AEP, respectively, as growth in the IoT platforms market accelerates to 39%, (2018) Available from https://iot-analytics.com/report-us22-billion-iot-platforms-market-by-2023/
[10] A. Bhatia, Z. Yusuf, D. Ritter, N. Hunke Who will win the IoT platform wars? (2017) Available from https://www.bcg.com/en-us/publications/2017/technology-industries-technology-digital-who-will-win-the-iot-platform-wars.aspx
[11] J. Moore, Predators and prey: a new ecology of competition, Harv. Bus. Rev. 71 (3) (1993) 75–86.
[12] O. Mazhelis, E. Luoma, H. Warma, Defining an Internet-of-Things ecosystem, in: S. Andreev, S. Balandin, Y. Koucheryavy (Eds.), Internet of Things, Smart Spaces, and Next Generation Networking. ruSMART 2012, NEW2AN 2012, Springer, Berlin, Heidelberg, 2012 Lecture Notes in Computer Science, Vol 7469.
[13] S. Kubler, J. Robert, A. Hefnawy, K. Främling, C. Cherifi, A. Bouras, Open IoT ecosystem for sporting event management, IEEE Access 5 (2017) 7064–7079.
[14] K. Rong, G. Hu, Y. Lin, Y. Shi, L. Guo, Understanding business ecosystem using a 6C framework in Internet-of-Things-based sectors, Int. J. Prod. Econ. 159 (2015) 41–55.
[15] M. Papert, A. Pflaum, Development of an ecosystem model for the realization of Internet of Things (IoT) services in supply chain management, Electron. Mark. 27 (2) (2017) 175–189.
[16] A. Bröring, S. Schmid, C. Schindhelm, A. Khelil, S. Kabisch, D. Kramer, D. Le Phuoc, J. Mitic, D. Anicic, E. Teniente, Enabling IoT ecosystems through platform interoperability, IEEE Softw. 34 (1) (2017) 54–61.

[17] F. Berkers, M. Roelands, F. Bomhof, T. Bachet, M. Van Rijn, W. Koers, in: Constructing a multi-sided business model for a smart horizontal IoT service platformProceedings of the Seventeenth International Conference on Intelligence in Next Generation Networks (ICIN), Venice, Italy, 2013, pp. 126–132.
[18] T. Degrande, F. Vannieuwenborg, S. Verbrugge, D. Colle, Multi-sided platforms for the Internet of Things, in: B. Shishkov (Ed.), Business Modeling and Software Design. BMSD, Springer, Cham, Switzerland, 2018 Lecture Notes in Business Information Processing, Vol 319.
[19] C. Perera, A.V. Vasilakos, G. Calikli, Q.Z. Sheng, K.-C. Li, Guest editorial special section on engineering industrial big data analytics platforms for Internet of Things, IEEE Trans. Ind. Inform. 14 (2) (2018) 744–747.
[20] Y. Sun, H. Yan, C. Lu, R. Bie, P. Thomas, A holistic approach to visualizing business models for the Internet of Things, Commun. Mob. Comput. 1 (1) (2012) 1–7.
[21] A. Botta, W. de Donato, V. Persico, A. Pescapé, Integration of cloud computing and Internet of Things: A survey, Future Gener. Comput. Syst. 56 (2016) 684–700.
[22] T. James IoT cross-platform by the deutsche telekom also known as “House of Clouds” (2018) Available from https://medium.com/nworld-publications/iot-cross-platform-by-the-deutsche-telekom-also-known-as-house-of-clouds-44c115451d7
[23] D. Bruneo, S. Distefano, M. Giacobbe, A.L. Minnolo, F. Longo, G. Merlino, D. Mulfari, A. Panarello, G. Patanè, A. Puliafito, C. Puliafito, N. Tapas, An IoT service ecosystem for smart cities: the #SmartME project, Internet Things 5 (2019) 12–33.
[24] G. Gardašević, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović, The IoT architectural framework, design issues and application domains, Wirel. Person. Commun. 92 (1) (2017) 127–148.
[25] K.J. Singh, D.S. Kapoor, Create your own Internet of Things: a survey of IoT platforms, IEEE Consum. Electron. Mag. 6 (2) (2017) 57–68.
[26] H. Lee, D. Sin, E. Park, I. Hwang, G. Hong, D. Shin, Open software platform for companion IoT devices, in: Proceedings of the IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2017, pp. 391–392.
[27] J. Yun, I.-Y. Ahn, N.-M. Sung, K. Kim, A device software platform for consumer electronics based on the Internet of Things, IEEE Trans. Consum. Electron. 61 (4) (2015) 564–571.
[28] J. Santa, R. Sanchez-Iborra, P. Rodriguez-Rey, L. Bernal-Escobedo, A.F. Skarmeta, LPWAN-based vehicular monitoring platform with a generic IP network interface, Sensor 19 (2) (2019) 264, doi:10.3390/s19020264.
[29] D. Chen, J. Cong, S. Gurumani, W. Hwu, K. Rupnow, Z. Zhang, Platform choices and design demands for IoT platforms: cost, power, and performance tradeoffs IET cyber-physical systems, Theory Appl. 1 (1) (2016) 70–77.
[30] M. Gusev, S. Dustdar, Going back to the roots-the evolution of edge computing, an IoT perspective, IEEE Internet Comput. 22 (2) (2018) 5–15.
[31] F. Wu, C. Rüdiger, M.R. Yuce, Real-time performance of a self-powered environmental IoT sensor network system, Sensors 17 (2) (2017) 282, doi:10.3390/s17020282.
[32] J. Lee, G.-I. Park, J.-H. Shin, J.-H. Lee, C.J. Sreenan, S.-E. Yoo, SoEasy: a software framework for easy hardware control programming for diverse IoT platforms, Sensors 18 (7) (2018) 2162, doi:10.3390/s18072162.
[33] O. Bello, S. Zeadally, M. Badra, Network layer inter-operation of device-to-device communication technologies in Internet of things (IoT), Ad Hoc Netw. 57 (2017) 52–62.
[34] R.S. Sinha, Y. Wei, S.-H. Hwang, A survey on LPWA technology: LoRa and NB-IoT, ICT Express 3 (1) (2017) 14–21.
[35] S. Li, L.D. Xu, S. Zhao, 5G Internet of Things: a survey, J. Ind. Inf. Integr. 10 (2018) 1–9.
[36] I.F. Akyildiz, S. Nie, S.-C. Lin, M. Chandrasekaran, 5G roadmap: 10 key enabling technologies, Comput. Netw. 106 (2016) 17–48.
[37] G. Brown Service-oriented core networks Huawei White Paper, (2017). Available from http://carrier.huawei.com/~/media/CNBG/Downloads/track/HeavyReadingWhitepaperServiceOriented5GCoreNetworks.pdf
[38] J. Ni, X. Lin, X.S. Shen, Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT, IEEE J. Sel. Areas Commun. 36 (3) (2018) 644–657 (2018).
[39] E. Fleury, N. Mitton, T. Noel, C. Adjih FIT IoT-LAB: The Largest IoT Open Experimental Testbed ERCIM News, (2016). Available from https://hal.inria.fr/hal-01138038/document.
[40] F. Corno, L. De Russis, J.P. Sáenz, Easing IoT development for novice programmers through code recipes ICSE-SEET, in: Proceedings of the Fortieth International Conference on Software Engineering: Software Engineering Education and Training, Gothenburg, Sweden, 2018, pp. 13–16. (2018).
[41] ABI Research system integrators quickly becoming the IoT gatekeepers (2017). Available from https://www.abiresearch.com/press/system-integrators-quickly-becoming-iot-gatekeeper/
[42] C. Bardaki, P. Kourouthanassis, K. Pramatari, Deploying RFID-enabled services in the retail supply chain: lessons learned toward the Internet of Things, Inform. Syst. Manag. 29 (3) (2012) 233–245.
[43] S.H. Choi, Y.X. Yang, B. Yang, H.H. Cheung, Item-level RFID for enhancement of customer shopping experience in apparel retail, Comput. Ind. 71 (2015) 10–23.
[44] H. Evanschitzky, G.R. Iyer, K.G. Pillai, P. Kenning, R. Schütte, Consumer trial, continuous use, and economic benefits of a retail service innovation: the case of the personal shopping assistant, J. Prod. Innov. Manag. 32 (3) (2015) 459–475.
[45] C.-L. Hsu, J.C.-C. Lin, Exploring factors affecting the adoption of Internet of Things services, J. Comput. Inform. Syst. 58 (1) (2018) 49–57.
[46] B. Di Martino, M. Rak, M. Ficco, A. Esposito, S.A. Maisto, S. Nacchia, Internet of Things reference architectures, security and interoperability: a survey, Internet Things 1-2 (2018) 99–112.
[47] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, D. Aharon, The Internet of Things: Mapping the Value Beyond the Hype, McKinsey Global Institute, 2015.
[48] H. Park, H. Kim, H. Joo, J. Song, Recent advancements in the Internet-of-Things related standards: a oneM2M perspective, ICT Express 2 (3) (2016) 126–129.
[49] J. Swetina, G. Lu, P. Jacobs, F. Ennesser, J. Song, Toward a standardized common M2M service layer platform: introduction to oneM2M, IEEE Wirel. Commun. 21 (3) (2014) 20–26.
[50] M. Noura, M. Atiquzzaman, M. Gaedke, Interoperability in Internet of Things: taxonomies and open challenges, Mob. Netw. Appl. (2018), doi:10.1007/s11036-018-1089-9.
[51] D. Mocrii, Y. Chen, P. Musilek, IoT-based smart homes: a review of system architecture, software, communications, privacy and security, Internet Things 1–2 (2018) 81–98.
[52] S. Sicari, A. Rizzardi, L.A. Grieco, A. Coen-Porisini, Security, privacy and trust in Internet of Things: the road ahead, Comput. Netw. 76 (15) (2015) 146–164.
[53] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for IoT security and privacy: the case study of a smart home, in: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017.
[54] D. Minoli, B. Occhiogrosso, Blockchain mechanisms for IoT security, Internet Things 1–2 (2018) 1–13.
[55] G.B. Barney The Internet of Things: are government regulation efforts too little, too late? (2018). Available from https://www.law.com/thelegalintelligencer/2018/07/20/the-internet-of-things-are-government-regulation-efforts-too-little-too-late/
[56] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Futture Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[57] B. Karakostas, Towards autonomous IoT logistics objects, in: I. Lee (Ed.), The Internet of Things in the Modern Business Environment, IGI Global, Hershey, USA, 2017, pp. 210–222.
[58] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, Internet of Things: a survey on enabling technologies, protocols, and applications, IEEE Commun. Surv. Tutor. 17 (4) (2015) 2347–2376.
[59] I. Mashal, O. Alsaryrah, T.Y. Chung, C.Z. Yang, W.H. Kuo, D.P. Agrawal Choices for interaction with things on internet and underlying issues ad hoc networks, 28 (2015), pp. 68–90

[60] Y. Chen, J. Guo, X. Hu, The research of Internet of Things' supporting technologies which face the logistics industry, in: Proceedings of the International Conference on Computational Intelligence and Security (CIS), Nanning, China, 2010, pp. 59–63.
[61] D. Darwish, Improved layered architecture for Internet of Things, Int. J. Comput. Acad. Res. 4 (4) (2015) 214–223.
[62] S. Madakam, R. Ramaswamy, S. Tripathi, Internet of Things (IoT): a literature review, J. Comput. Commun. 3 (5) (2015) 164–173.
[63] P. Sethi, S.R. Sarangi, Internet of Things: architectures, protocols, and applications, J. Electr. Comput. Eng. 2017 (2017) 9324035 Article ID.
[64] R. Mahmoud, T. Yousuf, F. Aloul, I. Zualkernan, Internet of Things (IoT) security: current status, challenges and prospective measures, in: Proceedings of the Tenth International Conference for Internet Technology and Secured Transactions (ICITST), London, UK, 2015.
[65] S. Li, T. Tryfonas, H. Li, The Internet of Things: a security point of view, Internet Res. 26 (2) (2016) 337–359.
[66] A. Alqahtani, Y. Li, P. Patel, E. Solaiman, R. Ranjan, End-to-End service level agreement specification for IoT applications, in: Proceedings of the International Conference on High Performance Computing & Simulation (HPCS), Orleans, France, 2018, pp. 926–935.
[67] K. Incki, I. Ari, A novel runtime verification solution for IoT systems, IEEE Access 6 (2018) 13501–13512.
[68] A. Larmo, A. Ratilainen, J. Saarinen, Impact of CoAP and MQTT on NB-IoT system performance, Sensors 19 (1) (2019) 7, doi:10.3390/s19010007.
[69] A.J. Jara, M.A. Zamora-Izquierdo, A.F. Skarmeta, Interconnection framework for mHealth and remote monitoring based on the Internet of Things, IEEE J. Sel. Areas Commun. 31 (9) (2013) 47–65.
[70] G. Yang, L. Xie, M. Mäntysalo, X. Zhou, Zhibo Pang, LD. Xu, S. Kao-Walter, Q. Chen, L.-R. Zheng, A health-IoT platform based on the integration of intelligent packaging unobtrusive bio-sensor and intelligent medicine box, IEEE Trans. Ind. Inf. 10 (4) (2014) 2180–2191.
[71] G. Miragliotta, F. Shrouf, Using Internet of Things to improve eco-efficiency in manufacturing: a review on available knowledge and a framework for IoT adoption, in: C. Emmanouilidis, M. Taisch, D. Kiritsis (Eds.), Advances in Production Management Systems. Competitive Manufacturing For Innovative Products and Services. APMS 2012. IFIP Advances in Information and Communication Technology, Vol 397, Springer, Berlin, Heidelberg, 2013, pp. 96–102.
[72] J. Bughin, M. Chui, The Internet of Things: assessing its potential and identifying the enablers needed to capture the opportunity, in: I. Lee (Ed.), The Internet of Things in the Modern Business Environment, IGI Global, Hershey, USA, 2017, pp. 111–125.
[73] M. Swan, Sensor mania! the Internet of Things, wearable computing, objective metrics, and the quantified self 2.0, J. Sens. Actuat. Netw. 1 (3) (2012) 217–253.
[74] E. Bucherer, D. Uckelmann, Business models for the Internet of Things, in: D. Uckelmann, M. Harrison, F. Michahelles (Eds.), Architecting the Internet of Things, Springer, Berlin Heidelberg, 2011, pp. 253–277.
[75] L. Ping, Q. Liu, Z. Zhou, H. Wang, Agile supply chain management over the Internet of Things, in: Proceedings of the International Conference on Management and Service Science, Wuhan, China, 2011, pp. 1–4.
[76] M.S. Balaji, S.K. Roy, A. Sengupta, A. Chong, User acceptance of IoT applications in retail industry, in: I. Lee (Ed.), The Internet of Things in the Modern Business Environment, IGI Global, Hershey, USA, 2017, pp. 28–49.
[77] B. Afzal, M. Umair, G.A. Shah, E. Ahmed, Enabling IoT platforms for social IoT applications: vision, feature mapping, and challenges, Future Gener. Comput. Syst. 92 (2019) 718–731.
[78] A. Osterwalder, Y. Pigneur, Business Model Generation: A Handbook For Visionaries, Game Changers, and Challengers, John Wiley & Sons, Hoboken, NJ, 2010.
[79] R.M. Dijkman, B. Sprenkels, T. Peeters, A. Janssen, Business models for the Internet of Things, Int. J. Inf. Manag. 35 (6) (2015) 672–678.
[80] H. Li, Z.Z. Xu, Research on business model of Internet of Things based on MOP, in: E. Qi, J. Shen, R. Dou (Eds.), Proceedings of the International Asia Conference on Industrial Engineering and Management Innovation (IEMI2012), Berlin, Heidelberg, Germany, Springer, 2013, pp. 1131–1138.
[81] L. Liu, W. Jia, Business model for drug supply chain based on the Internet of Things, in: Proceedings of the Second IEEE International Conference on Network Infrastructure and Digital Content, Beijing, China, IEEE, 2010, pp. 982–986.
[82] G. Sun, V. Chang, S. Guan, M. Ramachandran, J. Li, D. Liao, Big data and Internet of Things-fusion for different services and its impacts, Future Gener. Comput. Syst. 86 (2018) 1368–1370.
[83] M. Dubosson-Torbay, A. Osterwalder, Y. Pigneur, E-business model design, classification, and measurements, Thunderbird Int. Bus. Rev. 44 (1) (2002) 5–23.
[84] J. Peppard, A. Rylander, From value chain to value network: insights for mobile operators, Eur. Manag. J. 24 (2–3) (2006) 128–141.
[85] B. Wernerfelt, A resource-based view of the firm, Strateg. Manag. J. 5 (2) (1984) 170–180.
[86] Marriott.com. (2017). Marriott International Teams with Samsung and Legrand to Unveil Hospitality Industry's IoT Hotel Room of the Future, Enabling the Company to Deepen Personalized Guest Experience. http://news.marriott.com/2017/11/marriott-international-teams-samsung-legrand-unveil-hospitality-industrys-iot-hotel-room-future-enabling-company-deepen-personalized-guest-experience/
[87] Business Insider IoT Report: how Internet of Things technology growth is reaching mainstream companies and consumers (2019). Available from https://www.businessinsider.com/internet-of-things-report
[88] J. Kitanov, T. Janevski, State of the art: fog computing for 5G networks, in: Proceedings of the Twenty Fourth Telecommunications Forum (TELFOR), Belgrade, Serbia, 2016, pp. 1–4.
[89] D. Chen, J. Cong, S. Gurumani, W.-m. Hwu, K. Rupnow, Z. Zhang, Platform choices and design demands for IoT platforms: cost, power, and performance tradeoffs IET, Cyber-Phys. Syst. Theory Appl. 1 (1) (2016) 70–77.
[90] R. Savjani 5 things to consider before choosing an IoT platform company (2017). Available from https://www.softwebsolutions.com/resources/IoT-platform-company.html
[91] Telit IoT platform build versus buy decision guide (2019). Available from https://www.telit.com/iot-build-vs-buy/