Chapter 7

Smartphone: The Ultimate IoT and IoE Device

Mehdia Ajana El Khaddar and
Mohammed Boulmalf

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/intechopen.69734

Abstract

Internet of Things (IoT) and Internet of Everything (IoE) are emerging communication concepts that will interconnect a variety of devices (including smartphones, home appliances, sensors, and other network devices), people, data, and processes and allow them to communicate with each other seamlessly. These new concepts can be applied in many application domains such as healthcare, transportation, and supply chain management (SCM), to name a few, and allow users to get real-time information such as location-based services, disease management, and tracking. The smartphone-enabling technologies such as built-in sensors, Bluetooth, radio-frequency identification (RFID) tracking, and near-field communications (NFC) allow it to be an integral part of IoT and IoE world and the mostly used device in these environments. However, its use imposes severe security and privacy threats, because the smartphone usually contains and communicates sensitive private data. In this chapter, we provide a comprehensive survey on IoT and IoE technologies, their application domains, IoT structure and architecture, the use of smartphones in IoT and IoE, and the difference between IoT networks and mobile cellular networks. We also provide a concise overview of future opportunities and challenges in IoT and IoE environments and focus more on the security and privacy threats of using the smartphone in IoT and IoE networks with a suggestion of some countermeasures.

Keywords: smartphone, Internet of Things, Internet of Everything, ubiquitous, context, sensors, RFID, security, privacy

1. Introduction

The Internet of Things (IoT) is a network of intelligent devices ranging from home appliances to industrial equipment that can become connected to the Internet, monitor themselves, send contextual information such as pressure, location, and temperature, and communicate

somehow, anytime, anywhere on the planet (e.g., a milk carton sending sensor and identification information to a radio-frequency identification (RFID) reader when the temperature is getting higher than a threshold or when the milk carton is moved to a hot place) [1]. IoT means "connecting anyone, anything, anytime, anyplace, any service and any network" [1]. The concept of IoT has been extended by Cisco to Internet of Everything (IoE) to include in addition to things (machine-to-machine (M2M)), people (technology-assisted people-to-people (P2P)) and processes (machine-to-people (M2P)) interactions [2]. Cisco [2] defines Internet of Everything (IoE) as "the intelligent connection of people, process, data and things" [2], englobing interactions and communications generated by users while using a variety of networked devices (e.g., if a person forgot if s/he left the oven on at home, s/he wouldn't have to run back home to check it as s/he could just use a specific application and do it remotely using her/his smartphone) [2]. The proliferation of mobile connectivity and the decreasing prices of sensors and processors are encouraging the rapid growth of the IoT and IoE. Smart devices, for example, smartphones, smartwatches, PDAs, phablets, and tablets, will be the primary interaction tools used by people in a connected environment including cars, homes, and workplaces. Gartner expects in [3] that "the number of connected things and devices to rise to 25 billion by 2020 while other more aggressive estimates put the figure at 50 billion" [3]. "For this to be realized we need to have devices that are not only smart but should be able to access the Internet without being connected to a physical local area network (LAN) or wireless fidelity (Wi-Fi) network, should have an independent power source (e.g. battery), and should have the ability to sense the physical environment and send context information seamlessly" [3]. In today's world of emerging technologies, this could be made a reality: RFID, Bluetooth, 3G, 4G, 5G, wireless sensor networks, etc., along with long-lasting batteries, all bundled in one inexpensive, small, light, and portable device, which is the smartphone.

Equipped with the aforementioned technologies stated above, the smartphone gathers context data about the user (e.g., geolocation, temperature, health conditions, etc.) and interacts seamlessly with various devices using different types of connections such as Bluetooth, near-field communications (NFC), Wi-Fi, etc. Therefore, the smartphone can be considered as the user's ultimate device for IoT and IoE interactions and control. Big data, mobility, and cloud services are the principal parts of IoE concept, and using the smartphones everywhere is helping the IoE movement forward. Many services can be done in real time using the cloud and smartphones, for example, we can use our smartphone to order items online quickly, use an application to see if a specific store has an item in stock, or even better check how big is the queue in this store, order an item, then let customer services know that you are on your way to pick it up.

In this chapter, we will give an overview about the Smartphones' enabling technologies for the Internet of Things (IoT) and Internet of Everything (IoE), such as RFID, NFC, optical tags and quick response codes, Bluetooth, etc. We will also discuss the different application areas of IoT and IoE through the use of smartphones interconnected to other devices and show how the smartphone behaves in a cloud environment using different offered services. Finally, we will state the future opportunities and challenges of IoT and IoE applications. Some of the opportunities that will be discussed include context and ubiquitous services. Challenges will target basically the areas of privacy and security.

http://dx.doi.org/10.5772/intechopen.69734

2. Smartphones

A cell phone is a small device that can be used to make phone calls and send text messages on the go, adding the word "smart" to a phone can be confusing, aren't all phones smart? [4] A smart phone is sometimes called cell phone, because it can make calls but not vice versa [4]. A smartphone can be considered a miniature computer that has a virtual store of many applications such as games, different browsers, maps, emails, image editors, and that help to turn it into a device that is smarter than a regular cell phone [4]. Authors in Ref. [5] define a smartphone as "a next generation, multifunctional cell phone that provides voice communication and text messaging capabilities and facilitates data processing as well as enhanced wireless connectivity" [5]. According to Ref. [5], a smartphone could be considered a combination of "a powerful cell phone" [5] and a "wireless-enabled PDA" [5].

A smartphone has many additional features compared to a regular cell phone such as a color LCD screen, wireless capabilities, that is Wi-Fi, Bluetooth, infrared, etc., a large memory and a specialized operating system (OS) with an offer of many downloadable applications [5]. The emerging new technologies stated above available in smartphones along with the different new applications existing in the market, made of the smartphone a personal device that is not always on, but is always somewhere on us providing a ubiquitous and pervasive computing environment full of seamless services and applications that has most changed our lives [6]. As stated by Romero J. in [6], the smartphone helps users to get the required information whenever needed and to stay connected any time and at any given location [6].

The difference between a smartphone and a cell phone is mainly due to advances in three areas, which are hardware, that is, high-resolution screens, keyboards, cameras, processors, sensors, software, that is, operating systems and various supported applications, and network infrastructure, that is, 3G and 4G networks, and an increasing wireless bandwidth that allows the applications to offload data storage and processing to the cloud [6]. Equipped with different sensors, the smartphone world is considered different: for example, using the smartphone's accelerometers, basic health indicators can be followed, and using the GPS, traffic patterns could be monitored [6]. Many applications for augmented reality were also developed allowing, for example, to point your phone at a restaurant and see customer reviews about it. As stated in Ref. [6], smartphones are considered to become a "sixth sense" for the user, allowing a variety of functionalities.

3. Internet of Things (IoT)

3.1. Definitions

The Internet of Things, also shortly known as IoT, is a term consisting of two words: the first word "Internet," which is "a network of networks and a global system of interconnected computer networks that use TCP/IP as a standard Internet protocol (IP) to connect millions of users and multiple private, public, academic, business, and government networks" [7]. The second word "Things" consists of any real-world object such as home appliances, clothes,

etc. or living things such as plants, animals, and people [7]. The term "Internet of Things" was invented by Kevin Ashton, Executive Director of the Auto-ID Center in MIT, in 1999 and its definition varied among academicians and researchers [7]. The best definition of IoT would be according to Ref. [7]: "An open and comprehensive network of intelligent objects that have the capacity to auto-organize, share information, data and resources, reacting and acting in face of situations and changes in the environment" [7]. IoT aims at providing the vision of "enabling anytime, anywhere connectivity for anything and not only anyone by providing unique identity to each and every object" [7]. In the deployed IoT networks, sensors are attached to physical objects and keep track of their data, to allow their tracking on the Internet [7].

There exist many aliases for the IoT concept; these include "*Internet of Objects,*" "*web of things,*" "*connected devices,*" and "*technology omnipotent,*" "*omniscient,*" "*omnipresent,*" "*web of things,*" and "*embedded intelligence.*" IoT should not be confused with other terms such as ubiquitous computing where "technology becomes virtually invisible in our lives" [7], pervasive computing in which "virtually every object has processing power with wireless or wired connections to a global network" [7], cyber physical systems, which "helps bringing the real and virtual worlds together" [7], machine-to-machine interaction in which "devices are communicating end to end" [7], human–computer interaction, which "concerns the design of interaction between people and computers" [7], and ambient intelligence, which is "a developing technology that will make our lives responsive and environment sensitive" [7].

3.2. IoT structure

The IoT is a global network connecting things through numerous technologies such as RFID and barcodes to name a few [8]. The International Telecommunications Union (ITU) has structured the IoT into the following four dimensions: (1) tagging things, (2) feeling things, (3) shrinking things, and (4) thinking things [8]. In *tagging things*, RFID tags are used to automatically identify and track the attached object. In *feeling things*, sensors are used to collect data from the physical environment such as temperature, pressure, etc. [8]. In *shrinking things*, nanotechnology is used for tiny things: for example, "the use of nanosensors to monitor water quality" [8]. In *thinking things*, the smart things need, in addition to communication, to process information, make self-maintenance, and make independent decisions; this vision changes the way of information communication from human-human to thing-thing [8]. The structure of IoT is better illustrated in the following **Figure 1** [9].

3.3. IoT technologies

3.3.1. Radio-frequency identification (RFID)

RFID is a wireless identification technology that uses radio waves to identify an object or a person [7]. The first use of RFID was during the second world war to identify friend or foe aircrafts in 1948. The technology was later on founded at the Auto-ID center in MIT in 1999 [7]. The RFID systems consist basically of three elements: the *RFID Tag* serves to uniquely identify the attached object and carries data about it, the *RFID Reader* is the equipment used to power

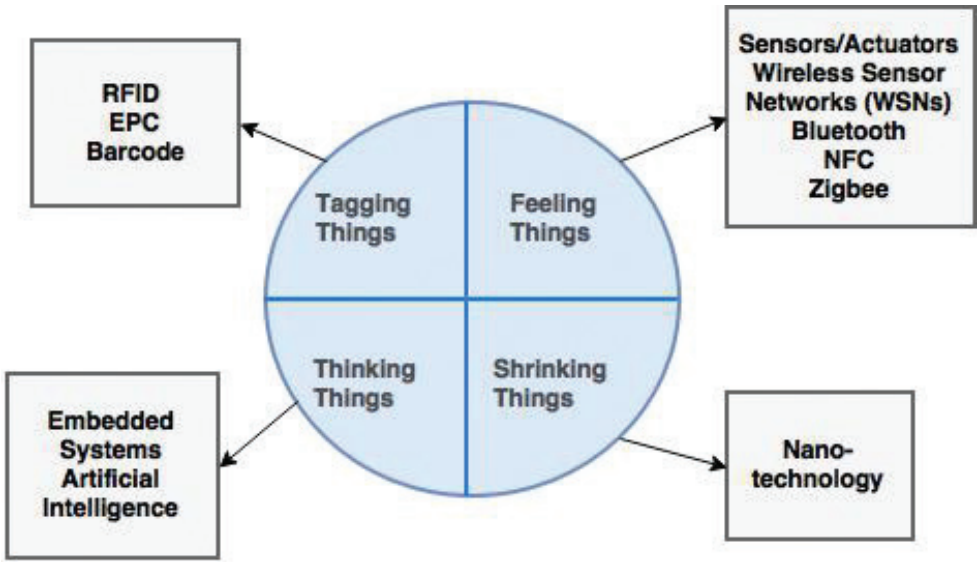

Figure 1. IoT structure in four dimensions and example technologies.

the tag, and read/write data to the tag [7]. The data read by the RFID reader from the RFID tags in its vicinity need to be processed then by a software system, known as the RFID middleware, which is the third component of an RFID system [10]. The *RFID middleware* serves to manage readers, filter, format, and process raw RFID data captured by the tags and send the processed data to the various interested backend applications [10, 11]. There exist three different versions of RFID tags depending on the power supply: *passive tags, active tags*, and *semipassive* [10]. Tags can be also classified based on their type of memory, for example, *read-only, read-write*, or *write-once and read-many*. RFID tags use the ISM (industrial, scientific, or medical) frequency ranges and have three types of frequencies: low frequency (LF), high frequency (HF), ultra high frequency (UHF), and microwave frequency [10]. RFID technology is cost effective, is considered very important in IoT networks for helping with tracking and identification of objects, and is used in a very broad range of application areas [10, 7].

3.3.2. Electronic product code (EPC)

Developed by the AutoID center in 1999 in MIT, the EPC code (64/98 bits) can store information about the unique serial number of a product, its specifications, and manufacturer's details [7]. The EPC has four components which are "object naming service (ONS)," "EPC discovery service (EPCDS)," "EPC information services (EPCIS)," and "EPC security services (EPCSS)" [7]. The EPCglobal Network [7] was created by the EPCglobal Organization to share EPC data and is a framework consisting of the ID System; EPC tags and readers; EPC middleware, which takes care of basic data formatting; EPC Information Services, which enable exchange of information between partners; and Discovery Services, which enable users to get

and search for EPC data [12]. The EPC was basically designed to be stored on an RFID tag to identify a specific item and its associated data such as origination point and date of production [12].

3.3.3. Barcode

The barcode system uses a barcode scanner to interpret the value in the barcode label to obtain a unique code that is used for object identification [7]. Barcodes are "optical machine-readable labels attached to items to record information about them, and they are usually read by laser scanners" [7]. Three types of barcodes exist: *alpha numeric* used for encoding numbers and characters, *numeric* used for encoding pairs of numbers, and *2-dimensional*, which looks like squares or rectangles that contain many small, individual dots [7]. The disadvantage of this system is the line of sight requirement between the barcode and the reader [10, 13].

3.3.4. Internet protocol (IP)

Internet protocol (IP), developed in 1970s, is considered main network protocol used for sending packets in the Internet [7]. There are two different versions of IP addresses: IPv4 (default version) and IPv6. IPv6 was developed to extend the number of available and supported IP addresses [7].

3.3.5. Wireless fidelity (Wi-Fi)

Wi-Fi (wireless fidelity) allows devices to communicate over a wireless signal, and contains any type of wireless local area network (WLAN) device supporting any of the following IEEE 802.11 specification versions: 802.11a, 802.11b, 80.2.11g, and 802.11n [7, 14]. Today, Wi-Fi is delivering the high-speed WLAN in-building connectivity to hotels, homes, airports, and cafes through the use of wireless access points (APs) [14]. Although encryption is considered optional in Wi-Fi, three techniques of encryption have been defined and applied to Wi-Fi to ensure security. These techniques are "wired equivalent privacy (WEP)," "WiFi protected access (WPA)," and "*IEEE 802.11i/WPA2"* [14]. To access a Wi-Fi network, Wi-Fi enabled devices (e.g., laptops) are needed, which can communicate wirelessly in any Wi-Fi equipped location [14].

3.3.6. Bluetooth

Bluetooth is a cheap communication technology, deployed for small distances (10–100 meters), that allows connection between devices, for example, laptops, PDAs, smartphones, printers, cameras, etc. without the need for cabling. Bluetooth is considered the main technology for creating a personal area network (PAN) to share data such as text, images, videos, and sounds, and it uses the IEEE 802.15.1 standard. Bluetooth allows users instantaneous connections between several devices and assures protection against interferences and safety in the sent information [15]. The Bluetooth technology operates in the ISM band, which is 2.45 GHz. Some standard Bluetooth applications include but are not limited to communication between hands-free device and a mobile phone or car radio, and transfer of files between devices [15]. Bluetooth can have some security risks, because it is an open system. Security can be implemented at the level of devices and services [15].

3.3.7. ZigBee

ZigBee technology was created and developed in 2001 by the ZigBee Alliance [7]. As defined in [16], ZigBee is "a low power, low cost, low data rate, and short range (around 100 meters), wireless network protocol based on the IEEE 802.15.4 standard" [16]. ZigBee is widely used in home automation, medical monitoring, industrial controls, and digital architecture [7]. ZigBee was developed to enhance the features of wireless sensor networks (WSNs) and is widely used for wireless home automation systems (WHASs); however, it has many related challenges such as resource constraints, low memory, limited battery, limited processing power, limited range, technological limitations related to the IEEE 802.15.4 standard, interferences with systems operating in the same free band, and internet connectivity, which is needed in WHAS for remote monitoring [16].

3.3.8. Near-field communication (NFC)

NFC is a short-range (theoretically 20 cm, but in most scenarios, typically 4 cm) wireless technology developed by "Philips and Sony companies" that works at the 13.56 MHz frequency and allows customers around the world to easily make transactions, connect electronic devices, and exchange digital content [7]. NFC technology is compatible with existing RFID infrastructure and contactless smart cards and uses the same standards such as ISO/IEC 14443 standard, which is one of its biggest advantages [17]. NFC has an easy and simple connection method, can work also in dirty environment, and does not require a line of sight for reading and executing transactions [7]. Some example applications of NFC include but are not limited to mobile payment such as Google Wallet, and mobile ticketing such as Oyster Card [17].

3.3.9. Wireless sensor networks (WSNs)

A WSN consists of hundreds to thousands of "sensor nodes" communicating with each other and passing data related to either "physical" or "environmental conditions" such as pressure, temperature, motion, location, sound, etc. [7, 18]. WSNs are used widely in IoT for many types of applications such as agriculture monitoring, patients monitoring, military applications, highway monitoring, civil and environmental engineering applications, forest fire, industrial automation, home control, building automation, etc. [18]. An example of the use of WSNs in healthcare is the use of sensors to monitor medication responses from a patient's body [7]. A key issue faced when designing a WSN network is energy efficiency, that is, designing for a "long network lifetime and limited network maintenance and deployment costs" [10]. A middleware system is needed to provide the multiple services required by WSN applications and allow for scalability, power saving, and quality of service (QoS) while designing WSN applications as suggested in [10].

3.3.10. Actuators

As defined in Ref. [7], an actuator is "a device that actuates or moves something; converting energy into motion or mechanical energy" [19, 7]. Typical applications of actuators are implemented in the industrial and manufacturing fields [7]. There are three types of actuators: *electrical actuators* are "AC and DC motors, stepper motors, and solenoids" [7]; *hydraulic actuators* "use hydraulic fluid to actuate motion" [7]; and *pneumatic actuators* "use compressed air to actuate motion" [7].

3.3.11. Artificial intelligence (AI)

Intelligence has been embedded and hidden in the network connected devices that help people to ease their daily activities [7]. AI refers then to "electronic environments and devices that are sensitive and responsive to people's presence and activities" [7]. AI is considered "*embedded,"* because the devices used are seamlessly embedded within people's environment, "*context-aware"* because these devices are used to know people's situations and context conditions, "*personalized"* because they can be customized to the needs of users, "*adaptive"* because it changes depending on the users' needs, and "*anticipatory"* because it can predict the user needs without conscious mediation [7].

3.4. IoT architecture

A reference model has not yet been suggested for the IoT architecture, although there are an ever-increasing number of proposed architectures for this new trend such as the ones described in [20–24]. Among the most common architectures of IoT we find the 5 layers model described in [25]. The first layer of this model is named the *objects layer/perception layer* and represents the physical objects, for example, sensors, actuators, etc. of the IoT that serve to collect information using standardized plug-and-play mechanisms to serve the heterogeneous devices [25]. The second layer is the *object abstraction layer*, which transfers the collected data from the objects layer to the service management layer using various technologies such as RFID, 3G, 4G, Wi-Fi, Bluetooth, and handles data management processes and cloud computing [25]. The third layer is the *service management layer*, which is the middleware layer that processes the received data, delivers the processed data and services to the interested applications over the network, and makes decisions [25]. The fourth layer is the *application layer* and is the one responsible for providing the requested smart services to the customers or connected applications that meet their needs in the various domains such as healthcare, transportation, and industrial automation [25]. The fifth layer is the *business layer*, which supports decision-making processes based on big data processing and analysis, manages all the underlying four layers of the IoT architecture, and enhances the services provided to the users and maintains their privacy [25].

In Ref. [10] we proposed and developed a flexible middleware solution architecture that has five layers and is compatible with the IoT architecture discussed above. We developed the proposed architecture more and applied it to e-health in [26]. The FlexRFID middleware in [10] serves getting data from the heterogeneous automatic identification devices and sensors, processing them, applying the business rules specified by the connected applications, and disseminating the processed data to the interested applications. Our middleware, that is, FlexRFID was tested with multiple application domains, such as smart library management [27], supply chain management [28], and healthcare scenarios [29].

4. Internet of Everything (IoE)

The Internet of Everything (IoE) concept is a fairly new concept that was developed by Gartner in 2015, and there is still confusion about the difference between IoE and IoT [30]. The IoE as

defined in Ref. [30] is "bringing together people, process, data, and things to make networked connections more relevant and valuable than ever before-turning information into actions that create new capabilities, richer experiences, and unprecedented economic opportunity for businesses, individuals, and countries" [30]. IoE definition means "connecting people in more relevant ways, converting data into intelligence to make better decisions, processing this data and delivering the right information to the right person at the right time, and connecting things which denote any physical devices or objects connected to the Internet or to each other for intelligent decision making" [30]. In other words, IoE describes an environment where many objects are identified, sensed through the use of sensors to detect their status and measure their conditions, and connected over public/private networks using specific standard/proprietary protocols [30]. The IoE is a term describing the intelligence added to every device in order to give it some added functionalities, the device could be any of the following: smartwatches, smart appliances, smart beds, health monitoring devices, smart connected cars, and others [31]. The difference between IoE and IoT is that IoE consists of four parts: "people," "process," "data," and "things" and builds on top of IoT, which consists of one part, which is "things" [30].

As reported by Cisco "IoE is capable of helping organizations achieve many public-policy goals, including increased economic growth and improvements in environmental sustainability, public safety and security, delivery of government services, and productivity" [32]. Also, Cisco reported in [32] the five drivers of IoE value for the public sector which are (1) "*employee productivity"* consisting of "improved labor effectiveness for new and existing services" [32], (2) "*connected militarized defense"* consisting of "improved situational awareness and connected command centers, vehicles, and supplies" [32], (3) "*cost reduction"* consisting of " improved labor efficiency and reduced operational costs" [32], (4) "*citizen experience"* consisting of "shorter search times; improved environment; better health outcomes" [32], and (5) "*increased revenue"* consisting of "improved ability to match supply with demand; improved monitoring and compliance" [32]. Cisco CEO, John Chambers, believes that "IoE will have a dramatic impact on everything from city planning, first responders, military, health, and dozens of other environments" [32].

IoE is believed to "extend the IoT emphasis on machine-to-machine (M2M) communications to describe a more complex system that also encompasses machine-to-people (M2P) and technology-assisted people-to-people (P2P) interactions" [2]. IoT and M2M are often considered synonymous and sometimes used interchangeably; however, IoT refers to "connection of systems and devices to the broader Internet" [2, 33].

5. Application areas of IoT and IoE

5.1. Applications based on the IoT

Information generated and communicated by the enabling objects in IoT can drive many possible applications in many domains such as supply chain management (SCM), transportation, healthcare, and environment and disaster monitoring, etc. [9].

5.1.1. Logistics and supply chain management (SCM)

In IoT society, many logistics applications have been developed to track movements of goods in real time using the different technologies discussed above, such as the systems reported in [34–36]. The data scanned from the RFID tags, barcodes, NFC, and mobile phones were transmitted to the logistics center, and then transmitted through diversified transmission protocols such as WSNs, GSM network, 3G, 4G, or even 5G network to be processed [9]. Some example applications of the IoT in logistics and SCM as reported in [9] include *Supermarket chain management* [34], which tracks goods in real time using WSNs, barcodes, and RFIDs, and controls automatically the stock; *Aspire RFID* [37], which is "a middleware with a range of tools to facilitate RFID deployment, in addition it uses the session initiation protocol (SIP) to detect the location and mobility management of RFID tags" [9], *logistic geographical information detection UIS* [38], and others. The use of sensors in SCM provides rich data about supply chains and also on conditions and location of goods in real time [39]. This helps supporting "circular economy," because tracking a product from manufacture to recycling helps enabling new ways for resource optimization [39]. To guarantee an efficient implementation of IoT, applications in SCM should ensure some basic capabilities such as *autonomous control* by having small decentralized control units [9], *smart logistics entities* by using sensors to track items and protect them from thieves by triggering alarms when a set of conditions is met [9], *unique addressability* by using a set of technologies such as RFID and WSNs to help tracking "the right product, right quantity, at the right time, in the right place, satisfying the right conditions, and having the right price" [9], and *enterprise resource planning* (ERP) interface to help communicate to the customer the right information about the products [9].

5.1.2. Transportation

IoT is considered to have many advantages for solving the numerous challenging transportation problems, and many applications such as the *road condition monitoring and alert system* reported in [40] were developed to communicate the road conditions in real time and alert their users about any congestions or existing problems such as accidents [40]. Other applications such as *license plate identification* as reported in [41] have been implemented to solve the problem of finding parking spaces and securing the vehicles [41]. *Electric vehicles* have also been supported by governments in many countries "to reduce the fuel cost and the impact of global warming"; systems such as the one in [42], that is, remote performance monitoring system and simulation testing, have been designed "to monitor the performance of lithium-ion (Li-on) batteries for electric vehicles" by using WSNs to report the route's status to the drivers and help them save their vehicles' batteries. Using IoT nowadays, many electric vehicles' manufacturers offer applications that can remotely monitor the vehicles' batteries power and schedule their charging [39]. As reported in [39], in the future, fully autonomous vehicles are expected to be integrated in a smart transportation system, and a trial system has been implemented in Newcastle that gives signals to drivers about when to adjust their speed if traffic lights are about to change [39]. Also parking sensors have being tested in Milton Keynes [39]. IoT has been also used at London City Airport to improve customer experience and passenger flow through the use of sensors deployed throughout the airport that send data to passengers'

smartphone applications to help them order from shops and know about queue times [39]. Other systems such as transport vehicle monitoring system based on IoT in [43] uses GPS, RFID, and 3G/4G technologies to monitor and administer the status of goods in real time [43]. IoT is also used nowadays in vehicular ad hoc networks (VANETs) and is driving the evolution of Internet of Vehicles (IoV) paradigm. In conclusion, the IoT-based applications in the transportation field should at least include the following units as suggested by authors in [9]: a *vehicle system* equipped with GPS and wireless communication technologies [9], the *station system*, which is "responsible for receiving data from the monitoring center and displaying real-time transit vehicle information" [9], and the *monitor center*, which is "responsible for comparing the received real-time data with events in the database and integrate the road traffic information for visualization" [9].

5.1.3. Healthcare

Many IoT solutions were implemented to improve human health and well-being and facilitate access to healthcare in rural areas such as the one described in Ref. [44]. The solution in [44] is based on RFID data communicated by active RFID tags worn by people who register with the rural healthcare center (RHC). The RFID tags are used to continuously monitor and control the patients' healthcare parameters such as temperature, blood pressure, etc., detect any change in them, and communicate them to the RHC doctor. IoT-driven healthcare systems and technologies can be used for prevention and early identification of diseases [39] and are basically used for hospitalized patients whose status requires continuous monitoring and attention, or for monitoring an aging family member at home [47]. Other examples of applications include the integration of a variety of devices in the patient's environment such as the use of smartphones to monitor vital signs and transmit health data directly to the care centers [45]. Some advanced systems such as the one in [46], that is, noncontact health monitoring system (NCHMS) uses classification and recognition-based algorithms and equipment equipped with cameras and microphones to analyze the user's facial expressions and detect any anomalies. In conclusion, the IoT-based applications in the healthcare field should at least include the following units as suggested by authors in [9]: *Tracking and monitoring* using any wearable WSN or RFID devices to generate and communicate health vital signs, *remote service* such as telemedicine and home diagnosis [47], which is necessary to provide emergency help to patients suffering from critical illnesses, *information management* used to manage the large amounts of data produced and captured about a patient such as medical history of medications and allergies, and *cross-organization integration*, which ensures an integration and communication among the hospital information systems, the patients' homes, and other medical care centers [9].

5.1.4. Environment and disaster

IoT technologies are used nowadays to minimize the effects of natural disasters by providing alerts and helping in the disaster recovery process [9]. Many examples of systems exist in the literature for environment monitoring such as "Health Monitoring and Risk Evaluation of Earthen Sites (HMRE2S) model" suggested by Xiao et al [48]; which collects "temperature,

humidity, and light information to evaluate the healthy level of the earthen sites by applying the concept of artificial antibodies to identify unusual environmental factors" [48], and "*Smart heat and electricity management transportation"* suggested by Kyriazis et al. [49] that "uses smart meters for electricity consumption and mobile sensors to assess the effect of real-time electricity usage on the energy consumption of buildings and individual appliances, etc." [9]. In conclusion, the IoT-based applications in the environment and disaster field should at least include the following components as suggested by authors in [9]: *environment sensors*, which help gathering and processing information such as humidity, temperature, and pressure from the environment, *WSN and mobile communication* (3G and 4G) helping to communicate the sensed information to other users or systems and trigger the necessary alerts, and *participatory sensing applications*, which, by the use of multiple sensors and devices to capture the environment data and sense the physical world, and to help making the right decisions when facing a disaster, for example [9].

5.1.5. Smart home and smart buildings

Home automation can be made possible using IoT technologies to allow us to remotely control our home's appliances based on our needs [50]. Example applications include but are not limited to monitoring of utility meters, energy, and water supply to avoid overloading or leaks, and gardening sensors, which could be used to water plants according to their needs and measure their vitals such as light, humidity, and moisture [50]. Connected to the IoT, smart buildings' energy and maintenance could be optimized and predicted, along with increased comfort, security, and safety for the building users [39].

5.1.6. Smart agriculture

The IoT technologies, such as field-based sensors, can be used to monitor soil humidity, moisture, and nutrition, automatically adjust the temperature to maximize agricultural production, and communicate with weather stations to get the latest forecasts [50, 39]. They can also help for an accurate fertilization and watering [50]. Sensors used for animal tracking help in monitoring livestock for disease and accidents, and providing better opportunities for husbandry [39]. "Smart farms" may also share data with other farms, consumers, and regulators [39]. The major opportunities provided by IoT for agriculture are maximizing yields by automatically identifying damaging weeds and reporting their location to farm owners or autonomous weeding machines, improving food traceability by tracking food and informing consumers about their provenance, origin, and production methods, and tackling environmental challenges such as the use of 3D accelerometers to detect injuries in cows and monitor them within the livestock, which allows for an early adoption of preventive measures [39].

5.2. Applications based on the IoE

The IoE has been used to help "automated and people-based processes" by extracting and analyzing real-time data from the millions of connected sensors [51]. IoE has been also used for environment sustainability, public policy goals, and economic goals [51]. The use of IoE

has been facilitated by the expansion of cloud computing, which helps connecting everything online [51]. "Smart cities" will benefit from IoE to address city-specific concerns along with big data processing, for example, using sensors in monitoring highways and traffic, education, healthcare, agriculture, and environment [51]. These cities will most likely enhance the living conditions of citizens in the future by forming "Smart + connected communities" [51]. IoE will be considered a critical element in implementing new features of the future cities such as *smart grid* and traffic control [51, 52]. According to Cisco, "cities stand to benefit the most from IoE related projects, implementations and platforms," which helps providing real-time, context-specific intelligence and analytics to serve the city's specific needs [53]. Many examples of how Cisco was involved in developing new models for cities have been included in [53]; however, there exist many challenges for the IoE-enabled cities such as the need for new operating models, coherent IoE deployment plans, new ways to preserve the cities assets such as data, new governance models, and the need to face societal challenges such as pollution, and CO2 emissions [53]. IoE technology architecture for cities is suggested in [53], which is a multilayered architecture that provides handling millions of devices and sensors, processing and streaming of big data and decisions, storage and analytics of data, and APIs for adding new services or applications [53].

IoE is also expected to ensure safety in the mining industry of fossil fuels [53]. Another use of IoE is in the educational sector where it facilitates access of students to E-learning and M-Learning, and provides more feedback and progress monitoring [51]. As reported by Zielinski [52], "The IoE provides a new business model for companies, which ultimately implies lowering the cost of energy distribution, automate billing and service calls as well as providing proactive response to environmental condition" [52].

In an IoE world, we can find multiple applications integrated in multiple ways: for example, public and private organizations usually integrate IoE applications with their existing solutions such as ERP, SCM, CRM, human resources, etc. [54]. This high level integration allows for better service guarantee and higher security [54]. IoE solutions are also expected to access data from a single-purpose device initially, an example of this is connected automobiles running multiple applications such as location detection, emergency calls, etc. [54].

6. The use of smartphones in IoT and IoE

The technology necessary for all the example applications of IoT and IoE, stated in the previous sections, to succeed is available today. RFID, Bluetooth, NFC, 3G, 4G, 5G, etc. can transfer data over the Internet, also batteries' technologies have evolved; for example, wireless and solar power batteries and long-lasting batteries are available in today's market [3]. In addition, different types and sizes of sensors exist and can be used to monitor various industrial processes [3]. The challenge is to include all the aforementioned technologies into one light, inexpensive, user-friendly, multipurpose, and portable device that can be easily used by people in their daily lives [3]. Such a device is today an existing reality which is the smartphone. The Smartphone is equipped with a range of built-in sensors such as accelerometers, motion

sensors, position sensors, and environmental sensors, that is, barometers, thermometers, and photometers measuring pressure, humidity, ambient temperature and illumination levels, etc. Some other kinds of special sensors measuring health vital signs, such as body temperature, ECG value, blood glucose level, stress level, body fat percentage, heart rate, etc., can be integrated into the smartphone [3]. All these sensors produce large volumes of data in structured form such as GPS or acceleration data and unstructured form such as pictures or videos [55]. The smartphone's cameras and microphones are also used to detect and record images in many smart applications used in IoT [3]. The smartphone is also equipped with a variety of connectivity technologies such as NFC, Bluetooth, Wi-Fi, and cellular, which allow it to connect and interact with other devices and sensors and be the brain of the IoT world [56]. An example of the use of IoT-enabled smartphones given in [3] is "traffic congestion control on specific roads using Google Maps; data are automatically being collected from users' smartphones moving along a specific road at a specific time, processed and sent to all connected users to Google Maps interested in getting this information" [3]. Another example is the use of smartphone to open a smart door of a hotel room in some parts of the world, once you approach it. This could be extended to office access control or garage access door opening [56].

Smartphones along with other IoT devices will play a main role in the expansion and use of this new terrain of Internet of Things [55]. The smartphone is considered to be "at the heart of a growing universe of connected devices and sensors" [55], also the rise of the smart wearables such as Apple Watch and Android Wear plays an additional role in creating an intelligent body area network (BAN) for the user where he stays connected most of the time [55]. The NFC technology integrated to the smartphones allows them also to act not only as sensors but as actuators triggering many actions such as payments, TV control, cars control, and home automation [55].

As reported in Ref. [55], smartphones can be used in an IoT setup along with four application categories: (1) *Personal IoT* where we find an increasing number of applications targeting health and fitness, and helping to solve everyday problems for users; (2) *group IoT* where smartphones can be used in the context of connected cars to check the system status, or in smart homes; (3) *community IoT* where crowd-sourcing applications could be used by citizens to contribute to a smart city; and (4) *industrial IoT* where smartphones are used for business to consumer (B2C) purposes such as sending customized services and vouchers in real time [55]. Future applications of the use of IoT through the smartphone include viewing data and controlling sensors anywhere; for example, at home or in a workplace, the smartphone could be used to "control a smart air conditioning or an alarm system at home from an application, or technicians may be alerted on their smartphones when a factory machine at a customer site is overheating and probably needs attention" [56]. In a smart city context, a smartphone application could be used to check the queue in a local store and see whether an item is in stock in real time, reserve the item, and call the client service for delivery. Other applications could be used in the smartphone to get data about noise and traffic congestion in the city to improve the residents' living experience in the controlled area.

Authors in [58] propose a four layers model named "*k-Healthcare*," which is considered a comprehensive platform for accessing patients' health data using the smartphones' sensors and applications. The model in [58] is composed of the following layers: (1) the *sensor layer*; which consists of sensors used to detect the patients' vital signs such as blood oxygen and pulse and the smartphone

built-in sensors such as barometers, temperature, and humidity sensors, along with RFID tags used to for objects identification. All of these IoT devices are used by the k-Health platform to get data and send them to the other layers for further processing [58]. (2) The *network layer* is "the communication layer that connects the IoT devices with WAN using different protocols such as 802.16 for 3G, IEEE 802.16m for 4G, IEEE 802.20, ZigBee, etc." [58] (3) The *internet layer* is responsible for data management and storage using cloud storage or physical storage. Finally (4) the *services layer* "provides direct access of data to patients and professionals such as doctors, hospitals, and medicine supply chains using various protocols such as HTTP, HTTPS, web services, etc." [58]

Using our FlexRFID middleware discussed in the IoT architecture section, **Figure 2** shows the use of smartphones at the different layers of the IoT architecture.

From **Figure 2**, it is clear that the smartphone could be used as an automatic identification and sensing device at the level of the *sensing/auto-tracking layer* and as a backend device at the level of the *application layer* where different users accessing different applications could get the needed services.

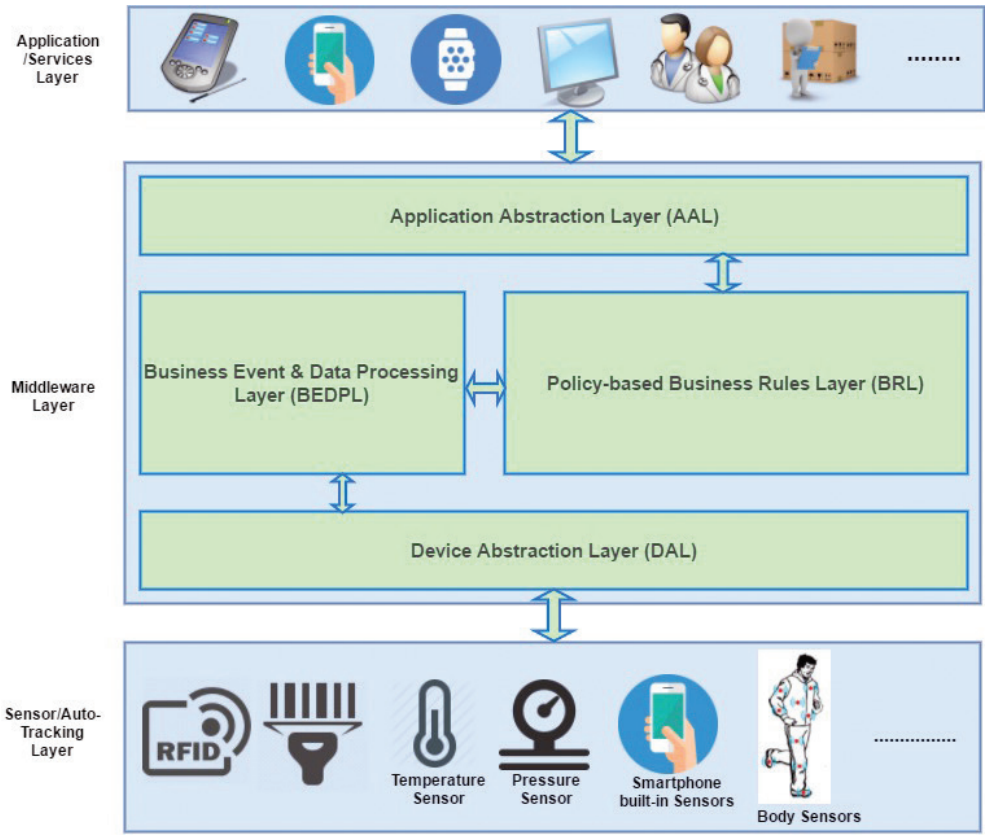

Figure 2. The use of smartphone in FlexRFID middleware.

7. IoT networks versus mobile cellular networks

Regular cell phone networks fall short for IoT requirements, basically for battery life, cost, and wireless coverage. That is why many wireless carriers around the world are building new cellular networks to work with current and upcoming IoT devices and solving one or all of the three new IoT requirements [59]. For example, Orange and SoftBank are building nationwide IoT networks, Vodafone is upgrading its networks, and Cisco and Samsung are inventing and selling new devices to expand the IoT concept [59]. A comparison between cellular networks and IoT networks concerning these perspectives is given below.

7.1. Long battery life

Mobile cellular networks were designed to coordinate moving from one cell to another, called "hand-off" mechanism, without interrupting a phone call by using sophisticated algorithms [59]. To ensure this, mobile cell phones should communicate multiple times per second with the cell tower, which is very expensive in terms of battery consumption. In order to save the battery power for years, the IoT new cell networks' devices should spend most of their time in sleep mode using low power radio chips and optimized to minimize the power cost of data transmission and reception, for example, to read sensors' data or activate a control such as an alarm system [59]. Achieving years of battery is important for IoT devices, because it eliminates installation costs and that is why new networks need to be built to save the battery power consumption [59].

7.2. Support for a massive number of devices, network scalability, and diversity

The IoT network should handle the increasing number of simultaneous connected devices, which may not be uniform and therefore could not be handled by the cellular network, because some cells may have a very high number of connected devices compared to others [60].

IoT networks need to scale efficiently to handle thousands or millions of connected devices, and should support diverse applications' requirements from simple sensors to tracking services to more advanced smart applications requiring higher throughput and lower latency [61].

7.3. Low device and deployment cost

The opportunity cost of supporting IoT devices in cellular networks is very high, because as reported in [59], "IoT devices that pay less than a dollar per month will never get network access priority over cell phones with $100 voice and data plans" [59]. IoT connectivity can be implemented and deployed over existing cellular networks using software upgrade in order to avoid additional costs of acquiring any new hardware [60]. The IoT networks are designed to be robust to interference, because they basically use the unlicensed bands or unused "guard bands" between the channels of licensed cellular spectrum, which are cheap compared to the licensed bands [59].

7.4. Extended coverage

IoT networks should also handle coverage concerns that are not covered by cellular networks in places such as basements of buildings, underground parking lots, and rural fields [60]. This extended coverage is required by many IoT applications to get the necessary data from the deployed sensors and send them in real time to the interested applications [60]. The IoT networks handle this by maximizing deep indoor penetration rather than bandwidth, and through the use of self-deployable gateways that could be installed like Wi-Fi routers [59].

8. Future opportunities and challenges of IoT and IoE applications

8.1. Future opportunities

People are getting more connected and devices are becoming smarter, and new network architectures are adapting to this: such as big data, cloud infrastructure, and mobility, which are important parts of the Internet of Everything movement. In the future, every device is considered to be communicating to some extent and this will have an impact on the growth of cloud services [57]. The IoE will reinvent industries at three levels in the future; the first level is *business processes and services* will be improved by the new trends in digital technology [30], the second level is *business model*, which will be changed as new ways of doing business industries will emerge and companies will tend to digitalize more its products and processes, an example stated in [30] is that of Nike with its connected sporting clothes in the healthcare domain [30], the third level is *business moment*, which is the need to compete with other businesses [30]. Also the IoE will generate large volumes of data in real time, and therefore, businesses will need big data, storage, and analysis tools to manage these data; generate high-level information and services; and turn them into money. As millions of objects, sensors, devices, and people get more connected and collect more data; a critical task for companies will be to tackle the issues of privacy and security that arise through the use of IoE technology [30].

8.2. Challenges

IoT and IoE offer numerous revolutionary benefits to consumers in many areas such as healthcare and supply chain management (SCM), to name a few. The use of connected medical devices, for example, can engage patients in their own care and allow doctors to respond in real time and better manage the patients' diseases. Despite these opportunities in many application fields, security and privacy risks arise due to the increased connectivity among devices, people, and the Internet. According to Ref. [62] IoT technology presents a higher potential of security risks at different levels such as enabling unauthorized access to personal information and identity theft, creating safety risks and allowing attacks to other connected systems; for example "security vulnerabilities in an IoT device could be used to launch a denial of service attack on the consumer's network to which it is connected, this device could also be used to send malicious emails and messages to other devices" [62]. Unauthorized persons might also create physical safety risks by exploiting the security vulnerabilities of IoT devices: for

example, a hacker can change the settings of an insulin pump to no longer deliver insulin to the concerned patient, which creates health problems and crisis [62].

Companies experiencing the IoT technology may not have enough experience in dealing with the security issues stated above and therefore find securing IoT devices and communications a challenging task [62]. Also the structure of some IoT devices is sophisticated and the manufacturers find it difficult or expensive to apply a security patch in them if a specific vulnerability is discovered [62]. In addition, some IoT devices are made disposable after purchase and therefore, the consumers are often left with vulnerable devices shortly after their purchase in most cases [62].

In addition to security risks, there are many privacy risks involved with IoT such as the collection of sensitive personal daily information such as health information, geolocation, and account numbers and sending data through the cloud [62]. The collection of this information over time could be misused and can help intruders infer future values. Privacy principles state that users should control their personal data and choose the smart environment and technology that protects their private lives [63]. Users usually have difficulty knowing about the existence of IoT devices in their environment, what information is being disclosed and sent in the network, and which parties benefit from this information. Also manufacturers are interested in building services around the collected data rather than selling the devices themselves [63]. According to Ref. [62], researchers state that the smartphones could be used to disclose the user's personality type, demographics, stress level and mood, happiness, etc. [62]. Another privacy risk is that an intruder could intercept unencrypted IoT data remotely while sent in the IoT network, combine, analyze, and act upon them [63]. The above security and privacy challenges may result in an undermined consumer confidence and a decrease in the IoT technology widespread adoption, which will surely affect the overall societal acceptance of IoT services [62].

Our proposed middleware architecture called FlexRFID tackles the security and privacy issues in the IoT environment at the application level by using policies as described in [29]. These policies allow the applications to specify the security, access control and privacy rules that should be applied on data before getting them, and therefore minimize the possibilities of compromising user's sensitive data. At devices level, new security models other than strong encryption are required in IoT because of the devices' limited capabilities such as limited size, computing, and processing power [63].

Authors in [1] define features of IoT security and privacy in the healthcare field, including security requirements of medical data, which are "confidentiality, integrity, authentication, availability, data freshness, non-repudiation, authorization, resiliency, fault-tolerance, and self-healing" [1]. In addition, the authors in [1] identify challenges for providing secure IoT services, which include (1) the computational, memory, and energy limitations of IoT healthcare devices, (2) multiplicity of IoT devices in healthcare, (3) mobility of IoT devices through different networks having different security configurations, which requires a challenging task of developing a mobility-compliant security algorithm, (4) scalability of IoT devices and their connection to the global information network, (5) IoT devices are connected to multiprotocol networks using a wide range of communication media and a dynamic network topology,

(6) designing a mechanism for dynamic security updates for the various IoT devices, and (7) designing tamper-resistant packages for IoT healthcare devices to avoid extracting cryptographic secrets, modifying programs, or replacing these devices. In addition to the challenges stated above, there are many other issues that need to be addressed concerning IoT services and devices. According to authors in [1], the most important issues are: the need for a unified standardization effort, the need for special IoT platforms and frameworks, targeting cost analysis of IoT-based services, the need to develop new IoT applications as the technology evolves and new devices emerge, the need for a "business model," and the need for "quality of service" guarantees for most IoT services [1].

9. Security and privacy challenges concerning the use of smartphones in IoT and IoE networks

Security and privacy of smartphones in IoT and IoE should be guaranteed to the maximum, because the smartphone is considered the major personal device used in IoT. Threats and attacks on the smartphone and IoT devices can be divided into the following categories as reported in [64]:

- **Resources**: such as GPS, camera, NFC, and other sensors.
- **Data**: such as messages, calls, contacts' list that could be compromised by malicious apps available for free in the app stores.
- **System information** about the smartphone such as identity, location, and Wi-Fi MAC address that could be disclosed without the user permission.
- **Worms**, which are programs that copy themselves to the various devices of a network and can compromise the security of the smartphone.
- **Spyware and malware applications**, which can monitor the users' data without his/her knowledge and send the data to the attacker.

Other smartphones attacks discussed in [64] include "financial malware attacks, network spoofing attacks, phishing attacks, surveillance attacks and network congestion attacks" [64].

Authors in [64] divide security violation into five categories, which are the following: (1) "*breach of confidentiality*" when "an unauthorized person reads and gets access to the data" [64], (2) "*breach of integrity*" when "the attacker reads and modifies the data" [64], (3) "*breach of availability*" when "the attacker destroys and deletes the data" [64], (4) "*denial of service*" when "the attacker attacks the limited resources of the smartphone like filling its memory, draining its battery, etc. and therefore makes it unable to communicate with other IoT devices" [64], and (5) "*theft of services*" when "the resources are used by an unauthorized person" [64]. The five categories of attacks stated above have different effects on the smartphones as major IoT devices, for example, a Denial of Service attack of a smartphone will affect the IoT and the cellular network, a data leakage attack of a smartphone will disclose private data such as online transactions, and a spamming attack will send messages to other smartphones and IoT devices [64].

The study in [64] compares IoT devices and smartphones in terms of many features such as "computation capacity, storage, external storage, authentication, end-to-end communication, expansibility, battery exhaustion, etc." [64]. The study shows that the smartphone has a lot of functionalities and has built-in sensors that allow it to perform most of IoT devices functions [64]. The study also shows the behavior of smartphones in the IoT environment concerning data sharing with other IoT machines, communication with IoT devices and the cloud, supporting more computation in IoT than in the web, and the possibility of sending malicious data to other IoT machines [64].

A survey of more than 5000 consumers from the USA, UK, Canada, Austria, and Japan conducted by Norton in 2016 revealed that some people understand that smartphones and IoT devices present risks and the rest do not care about their information being hacked [65]. As stated in [65] few research studies have focused on the risk of controlling IoT devices by the use of mobile apps installed in a user's smartphone. An intruder can control or get access to the smartphone and therefore control the IoT devices from mobile applications such as control of home appliances and healthcare-sensitive sensors [65]. Mobile applications can send unencrypted sensitive information from a user's phone such as location, call logs, browser history, and account details. Examples of vulnerabilities could be adding browser favorites, downloading and changing call logs, etc. Authors in [65] state the most important best practices that a user can adopt while using IoT devices, smartphones, and mobile apps, which are the following: (1) *using a reputable mobile security app* that identifies potential vulnerabilities before downloading an app, (2) *downloading apps from an official app store*, (3) *being mindful of the app settings* such as apps asking the user to disable security setting that protects installing apps from an unknown source, (4) *keeping the IoT devices current* by installing the latest updates, (5) *protecting the device by choosing a strong and unique password*, and (6) *being stingy with the device* such as protecting the communication between the device and network using an encrypted Wi-Fi connection or a hard-coded LAN connection if available [65].

10. Conclusion

The Internet of Things (IoT) and Internet of Everything (IoE) are rapidly finding their paths in our modern lives, allowing connecting and automating everything around us. This chapter gave an overview about these new trends, their enabling technologies, architecture, and application fields such as smart homes and healthcare. In this chapter, we also talked about the different IoT and IoE enabling technologies available in the smartphone and examples of its use in IoT and IoE scenarios. We proposed a model for IoT implementation that uses the smartphone sensors to sense and transmit data to multiple backend applications using a middleware layer. The applications could be running on a smartphone, which receive the data and present it to the end user, that is, the patient, hospital administration, or physician in the case of healthcare. These data could be stored in special databases or in the cloud and retrieved by the user later on upon need, using the smartphone dedicated application. We also covered the differences between IoT networks and mobile cellular networks in terms of requirements such as the need in IoT networks for long battery life, support for a massive number of devices, network scalability, low device and deployment costs, and extended coverage. Finally, future

opportunities and challenges of IoT and IoE have been addressed especially the security and privacy risks of using the smartphone in these networks and possible countermeasures. By addressing the extensive use of the smartphone in IoT and IoE applications in this chapter, we consider that the smartphone is the ultimate IoT and IoE device.

Author details

Mehdia Ajana El Khaddar[1]* and Mohammed Boulmalf[2]

*Address all correspondence to: mehdia.ajana@gmail.com

1 Ecole Nationale Supérieure de L'informatique et d'Analyse des Systèmes (ENSIAS), Rabat, Morocco

2 International University in Rabat (UIR), Rabat, Morocco

References

[1] Islam SMR, Kwak D, Kabir MDH, Hossain M, Kwak KS. The Internet of Things for health care: A comprehensive survey. IEEE Access. 2015;**3**:678-708. DOI: 10.1109/ACCESS.2015.2437951

[2] Rouse M. Internet of Everything (IoE) [Internet]. Available from: http://internetofthingsagenda.techtarget.com/definition/Internet-of-Everything-IoE [Accessed: 7 March 2017]

[3] Mukherjee P. The Smartphone and the Internet of Things [Internet]. 2015. Available from: http://praxis.ac.in/the-smartphone-and-the-internet-of-things/ [Accessed: 7 March 2017]

[4] Fendelman A. How are Cell Phones Different From Smartphones? Is a Cell Phone the Same As a Smartphone? [Internet]. 2017. Available from: https://www.lifewire.com/cell-phones-vs-smartphones-577507 [Accessed: 7 March 2017]

[5] Zheng P, Ni LM. Spotlight: The rise of the smart phone. IEEE Computer Society. 2006;**7**(3). DOI: 10.1109/MDSO.2006.22

[6] Romero J. Smartphones: The Pocketable PC: Is Your Phone Smarter Than a Fifth Grader? [Internet]. 2010. Available from: http://spectrum.ieee.org/telecom/wireless/smartphones-the-pocketable-pc [Accessed: 7 March 2017]

[7] Madakam S, Ramaswamy R, Tripathi S. Internet of Things (IoT): A literature review. Journal of Computer and Communications. 2015;**3**:164-173. DOI: 10.4236/jcc.2015.35021

[8] Vongsingthong S, Smanchat S. Internet of things: A review of applications & technologies. Suranaree Journal of Science & Technology. 2014;**21**(4): 359-374

[9] Vongsingthong S, Smanchat S. Internet of Things: A Review of Applications & Technologies [Internet]. 2014. Available from: http://www.thaiscience.info/journals/Article/SJST/10966646.pdf [Accessed: 7 March 2017]

[10] Ajana M E, Boulmalf M, Harroud H, Elkoutbi M. RFID Middleware Design and Architecture. In: Dr. Cristina Turcu, editor. Designing and Deploying RFID Applications. Rijeka, Croatia: InTech; 2011. DOI: 10.5772/16917

[11] Floerkemeier C, Lampe M. RFID middleware design: Addressing application requirements and RFID constraints. In: Proceedings of Smart Objects Conference; October; Grenoble, France. 2005. pp. 219-224

[12] ZIH Corp. Electronic Product Code (EPC) RFID Technology [Internet]. 2017. Available from: https://www.zebra.com/us/en/resource-library/getting-started/rfid-printing-encoding/epc-rfid-technology.html [Accessed: 7 March 2017]

[13] Ishikawa T, Yumoto Y, Kurata M, Endo M, Kinoshita S, Hoshino F, Yagi S, Nomachi M. Applying Auto-ID to the Japanese Publication Business to Deliver Advanced Supply Chain Management, Innovative Retail Applications, and Convenient and Safe Reader Services [Internet]. 2003. Available from: http://cocoa.ethz.ch/downloads/2014/06/None_KEI-AUTOID-WH004.pdf [Accessed: 7 March 2017]

[14] Tutorials Point. Wi-Fi Wireless Communication [Internet]. 2015. Available from: https://www.tutorialspoint.com/wi-fi/wifi_tutorial.pdf [Accessed: 7 March 2017]

[15] Puy I. Bluetooth [Internet]. 2008. Available from: http://webuser.hs-furtwangen.de/~heindl/ebte-08ss-bluetooth-Ingo-Puy-Crespo.pdf [Accessed: 7 March 2017]

[16] Obaid T, Rashed H, Abou-Elnour A, Rehan M, Muhammad-Saleh M, Tarique M. Zigbee technology and its application in wireless home automation systems: A survey. International Journal of Computer Networks & Communications. 2014;**6**(4). DOI: 10.5121/ijcnc.2014.6411

[17] Burkard S. Near Field Communication in Smartphones [Internet]. Available from: https://www.snet.tu-berlin.de/fileadmin/fg220/courses/WS1112/snet-project/nfc-in-smartphones_burkard.pdf [Accessed: 7 March 2017]

[18] Sohraby K, Minoli D, Znati T. Wireless Sensor Networks: Technology, Protocols, and Applications. 1st ed. Hoboken, NJ: John Wiley & Sons; 2007. pp. 38-69

[19] Southwest Center for Microsystems Education (SCME) University of New Mexico. Introduction to Transducers, Sensors and Actuators [Internet]. 2011. Available from: http://engtech.weebly.com/uploads/5/1/0/6/5106995/more_on_transducers_sensors_actuators.pdf [Accessed: 7 March 2017]

[20] Khan R, Khan SU, Zaheer R, Khan S. Future internet: The Internet of Things architecture, possible applications and key challenges. In: Proceedings of 10th International Conference on Frontiers of Information Technology (FIT); 17-19 December; Islamabad, Pakistan. 2012. DOI: 10.1109/FIT.2012.53

[21] Yang Z, Peng Y, Yue Y, Wang X, Yang Y, Liu W. Study and application on the architecture and key technologies for IOT. In: Proceedings of the International Conference on Multimedia Technology (ICMT); 26-28 July 2011. pp.747-751

[22] Wu M, Lu T, Ling F, Sun J, Du H. Research on the architecture of Internet of Things. In: Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), August 2010

[23] Atzori L, Iera A, Morabito G. The Internet of Things: A survey. Computer Networks. 2010;**54**:2787-2805

[24] Chaqfeh MA, Mohamed N. Challenges in middleware solutions for the Internet of Things. In: Proceedings of the International Conference on Collaboration Technologies and Systems (CTS); Denver. 2012. pp. 21-26

[25] Al-Fuqaha A, Guizani M, Mohammadi M, Aledhari M, Ayyash M. Internet of Things: A survey on enabling technologies, protocols, and applications. IEEE Communication Surveys & Tutorials. 2015;**17**(4):2347-2376. DOI: 10.1109/COMST.2015.2444095

[26] Ajana ME, Harroud H, Boulmalf M, Elkoutbi M, Habbani A. Emerging wireless technologies in e-health trends, challenges, and framework design issues. In: Proceedings of the International Conference on Multimedia Computing and Systems (ICMCS), 10-12 October 2012. pp. 440-445

[27] Ajana ME, Harroud H, Boulmalf M, Hamam H. FlexRFID: A flexible middleware for RFID applications development. In: Proceedings of the 6th International Wireless and Optical Networks Communications (WOCN) Conference; April; Cairo, Egypt. 2009.

[28] Ajana ME, Harroud H, Boulmalf M, Elkoutbi M. FlexRFID middleware in the supply chain: Strategic values and challenges. International Journal of Mobile Computing and Multimedia Communications. 2011;**3**(2):19-32. DOI: 10.4018/jmcmc.2011040102

[29] Ajana EM, Chraibi M, Harroud H, Boulmalf M, Elkoutbi M, Maach A. FlexRFID: A security and service control policy-based middleware for context-aware pervasive computing. International Journal of Advanced Research in Artificial Intelligence (IJARAI). 2014;**3**(10). DOI: 10.14569/IJARAI.2014.031004

[30] Banafa A. The Internet of Everything (IoE) [Internet]. 2016. Available from: https://www.bbvaopenmind.com/en/the-internet-of-everything-ioe/ [Accessed: 7 March 2017]

[31] Bajarin T. The Next Big Thing for Tech: The Internet of Everything [Internet]. 2014. Available from: http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/ [Accessed: 7 March 2017]

[32] Bradley J, Loucks J, Macaulay J, Noronha A. Internet of Everything (IoE) Value Index: How Much Value Are Private-Sector Firms Capturing from IoE in 2013? [Internet]. 2013. Available from: http://internetofeverything.cisco.com/sites/default/files/docs/en/ioe-value-index_Whitepaper.pdf [Accessed: 7 March 2017]

[33] Holler J, Tsiatsis V, Mulligan C, Avesand S, Karnouskos S, Boyle D. From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. 1st ed. Cambridge, Massachusetts, United States: Academic Press; 2014. 352 p

[34] Li R, Luo H. Based on the Internet of Things the supermarket chain management information system development and safety stock research. In: Proceedings of the 2nd International Conference on Education Technology and Computer (ICETC); 22-24 June; Shanghai, China. 2010. pp. 368-371

[35] Wei Y. Design and realization of mobile information collection module in logistic Internet of Things unified information system. In: Proceedings of IEEE 3rd International Conference on Communication Software and Networks (ICCSN); 27-29 May; Xian, China. 2011. pp. 263-266

[36] El-Baz D, Bourgeois J, Saadi T, Bassi A. ALMA, a logistic mobile application based on Internet of Things. In: Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; 20-23 August; Beijing, China. 2013. pp. 355-358

[37] Soldatos J, Kefalakis N, Leontiadis N, Konstantinou N, Mitton N, Schmidt L, Dagher R, David M, Anggorojati B, Frattasi S, Prasad N, Donsez D, Pedraza G, Gama K. D-3.4b: Core aspire middleware infrastructure. 2010. Technical Report, Aspire FP7 Contract: ICT-215417-CP, 89 p

[38] Lin X. Logistic geographical information detecting unified information system based on Internet of Things. In: Proceedings of the 3rd International Conference on Communication Software and Networks (ICCSN); 27-29 May; Xian, China. 2011. pp. 303-307

[39] Government Office for Science. The Internet of Things: Making the Most of the Second Digital Revolution [Internet]. Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf [Accessed: 7 March 2017]

[40] Ghose A, Biswas P, Bhaumik C, Sharma M, Pal A, Jha A. Road condition monitoring and alert application: Using in-vehicle Smartphone as internet-connected sensor. In: Proceedings of the IEEE 10th International Conference on Pervasive Computing and Communications (PERCOM Workshops); 19-23 March; Lugano, Switzerland. 2012. pp. 489-491

[41] Ren X, Jiang H, Wu Y, Yang X, Liu K. The Internet of Things in the license plate recognition technology application and design. In: Proceedings of the Second International Conference on Business Computing and Global Informatization (BCGIN); 12-14 October; Shanghai, China. 2012. pp. 969-972

[42] Haiying W, Long H, Xin Q, Hongbo W, Gechen L, Xianqing D. Simulation system of the performance of power battery for electrical vehicle based on Internet of Things. In: Proceedings of the 2012 International Conference on Measurement, Information and Control (MIC); 18-20 May; Harbin, China. 2012. pp. 681-684

[43] Shengguang L, Lin T, Yuanshuo Z, Rucai Z. Internet of Things for special materials transportation vehicles. In: Proceedings of the IEEE International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; 20-23 August; Beijing, China. 2013. pp. 1891-1894

[44] Rohokale VM, Prasad NR, Prasad R. A cooperative Internet of Things (IoT) for rural healthcare monitoring and control. In: Proceedings of the 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE); 28 February–3 March; Chennai, India. 2011. pp. 1-6

[45] Jara AJ, Zamora MA, Skarmeta AF. Knowledge acquisition and management architecture for mobile and personal health environments based on the Internet of Things. In: Proceedings of the IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom); 25-27 June; Liverpool, UK. 2012. pp. 1811-1818

[46] Yang N, Zhao X, Zhang H. A noncontact health monitoring model based on the Internet of Things. In: Proceedings of the 8th International Conference on Natural Computation; 29-31 May; Chongqing, China. 2012. pp. 506-510

[47] Kulkarni A, Sathe S. Healthcare applications of the Internet of Things: A review. International Journal of Computer Science and Information Technologies (IJCSIT). 2014;**5**(5):6229-6232. DOI: 10.1.1.659.5696

[48] Xiao Y, Li W, Chen X-J, Liu B-Y, Wang L, Fang D-Y. An immune theory based health monitoring and risk evaluation of earthen sites with Internet of Things. In: Proceedings of the International Conference on Green Computing and Communications (GreenCom) and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing; 20-23 August; Beijing, China. 2013. pp. 378-382

[49] Kyriazis D, Varvarigou T, Rossi A, White D, Cooper J. Sustainable smart city IoT applications: Heat and electricity management & eco-conscious cruise control for public transportation. In: Proceedings of the14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)); 4-7 June; Madrid, Spain. 2013. pp. 1-5

[50] Farooq MU, Waseem M, Mazhar S, Khairi A, Kamal T. A review on Internet of Things (IoT). International Journal of Computer Applications. 2015;**113**(1). DOI: 10.5120/19787-1571

[51] Miraz MH, Ali M. A review on Internet of Things (loT), Internet of Everything (IoE) and Internet of Nano Things (IoNT). In: Proceedings of the ITA 2015; 8-11 September; Wrexham. 2015. pp. 219-224

[52] Zielinski JS. Internet of Everything (IoE) in Smart Grid [Internet]. 2015. Available from: https://www.researchgate.net/publication/275956622_Internet_of_Everything_IoE_in_Smart_Grid [Accessed: 7 March 2017]

[53] Mitchell S, Villa N, Stewart-Weeks M, Lange A. The Internet of Everything for Cities: Connecting People, Process, Data, and Things to Improve the 'Livability' of Cities and Communities [Internet]. 2013. Available from: http://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/everything-for-cities.pdf [Accessed: 7 March 2017]

[54] Machination. The Development of the Internet of Everything [Internet]. 2014. Available from: https://www.machnation.com/wp-content/uploads/2014/06/MachNation-Development-of-the-IoE.pdf

[55] Hausenblas M. Smart Phones and the Internet of Things [Internet]. 2014. Available from: https://www.mapr.com/blog/smart-phones-and-internet-things [Accessed: 7 March 2017]

[56] Wittmann E. The Internet of Things Is Here, and It Will Revolve Around the Smartphone [Internet]. 2015. Available from: http://memeburn.com/2015/12/the-internet-of-things-is-here-and-it-will-revolve-around-the-smartphone/ [Accessed: 7 March 2017]

[57] Tempest A. The Internet of Everything [Internet]. 2014. Available from: http://www.rymote.com/general/internet-everything/ [Accessed: 7 March 2017]

[58] Ullah K, Shah MA, Zhang S. Effective ways to use Internet of Things in the field of medical and smart health care. In: Proceedings of the Intelligent Systems Engineering (ICISE) Conference; 15-17 January; Islamabad, Pakistan. 2016. DOI: 10.1109/INTELSE.2016.7475151

[59] Conrad D. Three Reasons Carriers Are Building New Cell Networks for the Internet of Things [Internet]. 2016. Available from: https://techcrunch.com/2016/10/28/three-reasons-carriers-are-building-new-cell-networks-for-the-internet-of-things/ [Accessed: 7 March 2017]

[60] Nokia. LTE Evolution for IoT Connectivity [Internet]. 2017. Available from: http://resources.alcatel-lucent.com/asset/200178 [Accessed: 7 March 2017]

[61] Ericsson. Cellular Networks for Massive IoT [Internet]. 2016. Available from: https://www.ericsson.com/res/docs/whitepapers/wp_iot.pdf [Accessed: 7 March 2017]

[62] FTC Staff Report. Internet of Things: Privacy & Security in a Connected World [Internet]. 2015. Available from: https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf [Accessed: 7 March 2017]

[63] The Internet of Things: An Introduction to Privacy Issues with a Focus on the Retail and Home Environments [Internet]. 2016. Available from: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/iot_201602/

[64] Khan MH, Shah MA. Survey on security threats of smartphones in Internet of Things. In: Proceedings of the International Conference on Automation and Computing (ICAC); 7-8 September; University of Essex Wivenhoe Park Colchester, UK. 2016. DOI: 10.1109/IConAC.2016.7604979

[65] Haley K. Mobile Apps and IoT Devices Are an Overlooked Security Risk by Consumers—And that's a Problem [Internet]. 2016. Available from: https://uk.norton.com/norton-blog/2016/02/mobile_apps_and_iot.html [Accessed: 7 March 2017]