1 Introduction to the Internet of Things

Karolina Baras and Lina M. P. L. Brito

CONTENTS

1.1 INTRODUCTION

Back in 1989, there were around 100,000 hosts connected to the Internet (Zakon, 2016), and the World Wide Web (WWW) came to life a year later at CERN with the first and only site at the time.* Ten years after Tom Berners-Lee unleashed the WWW, a whole new world of possibilities started

* http://info.cern.ch/.

to emerge when Kevin Ashton, from the Massachusetts Institute of Technology's (MIT) Auto-ID Labs, coined the term *Internet of Things* (Ashton, 2009). In the same year, Neil Gershenfeld published his work on things that think, where he envisioned the evolution of the WWW as "things start to use the Net so that people don't need to" (Gershenfeld, 1999). Simultaneously, in Xerox PARC Laboratories in Palo Alto, California, the so-called third era of modern computing was dawning, with Mark Weiser introducing the concept of "ubiquitous computing" in his paper published in *Scientific American* (Weiser, 1991). Tabs, pads, and boards were proposed as the essential building blocks for the computing of the future. Wireless networking and seamless access to shared resources would make user experience with technology as enjoyable as "a walk in the woods."

In 1999, the number of hosts exceeded 2 million and the number of sites jumped to 4 million (Zakon, 2016). The Institute of Electrical and Electronics Engineers (IEEE) standard 802.11b (Wi-Fi) had just been published, with transmission rates of 11 Mbits/s. GSM was growing fast, but the phones were not at all smart yet. They (only) allowed for making phone calls and sending short messages. GPS signals for civil usage were still degraded with selective availability, and the receivers were heavy, huge, and expensive. The area of wireless sensor networks (WSNs) also emerged in the 1990s with the concept of smart dust, a big number of tiny devices scattered around an area capable of sensing, recording, and communicating sensed data wirelessly.

In the dawn of the eagerly expected twenty-first century, the technological growth accelerated at an unprecedented pace. Although the reports published 10 and 20 years after Weiser's vision showed that not everything turned out to be just as he had imagined, significant changes were introduced in the way we use technology and live with it. Our habits changed, our interaction with technology changed, and the way we grow, play, study, work, and communicate also changed.

In 2005, the International Telecommunications Union (ITU) published its first report on the Internet of Things (IoT), noting that

> "*Machine-to-machine communications and person-to-computer communications will be extended to things, from everyday household objects to sensors monitoring the movement of the Golden Gate Bridge or detecting earth tremors. Everything from tyres to toothbrushes will fall within communications range, heralding the dawn of a new era, one in which today's internet (of data and people) gives way to tomorrow's Internet of Things*." (ITU-T, 2005)

Three years later, in 2008, the number of devices connected to the Internet outnumbered the world's population for the first time. The introduction of Internet protocol version 6 (IPv6)* resolved the problem of the exhaustion of IP addresses, which was imminent near the end of the twentieth century. The first international conference on IoT† took place in March 2008 to gather industry and academia experts to share their knowledge, experience, and ideas on this emerging concept. In the following years, the number of IoT-related events and conferences grew enormously.

Open-source electronics such as Arduino,‡ which reached the market between 2005 and 2008, gave birth to millions of new ideas and projects for home and office automation, education, and leisure. Other examples of single-board computers (SBCs) followed: Raspberry Pi,§ BeagleBone Black,¶ Intel Edison,** and so on. Today, one can buy a dozen tiny but fairly powerful computers for less than $50 each, connect them to the Internet and to a plethora of sensors and actuators, collect and analyze gigabytes of data, and make interesting home or office automation projects with

* https://tools.ietf.org/html/rfc2460.
† http://www.iot-conference.org/iot2008/.
‡ https://www.arduino.cc/.
§ https://www.raspberrypi.org/.
¶ https://beagleboard.org/black.
** https://software.intel.com/en-us/articles/what-is-the-intel-edison-module.

real-time visualizations of information generated from the data on the go. Alternatively, one can use remote networks of intelligent devices deployed somewhere else, for example, OneLab.*

In 2009, the Commission of the European Communities published a report on the IoT action plan for Europe showing that the IoT had reached a very high level of importance among European politicians, commercial and industry partners, and researchers (Commission of the European Communities, 2009). Several global standard initiatives were created in recent years to discuss and define IoT-related issues and establish global agreement on standard technologies to be deployed in IoT projects. For example, oneM2M† was created in 2012 as a global standard initiative that covers machine-to-machine and IoT technologies, which go from requirements, architecture, and application programming interface (API) specifications, to security solutions and interoperability issues.

In 2015, the European Commission created the Alliance for the Internet of Things (AIOTI)‡ to foster interaction and collaboration between IoT stakeholders. The convergence of cloud computing, the miniaturization and lower cost of sensors and microcontrollers, and the omnipresence of digital connectivity all contributed to making the IoT a reality for years to come.

In fact, some sources consider that the four pillars of digital transformation are cloud, mobility, big data, and social networking, and that IoT is based on these (IDC, 2015; i-SCOOP, 2015).

Gartner forecasts that by 2020 there will be more than 20 billion "things" connected to the Internet (Gartner, Inc., 2013). This number excludes PCs, smartphones, and tablets.

Now that the IoT is finally becoming a reality, there is a need for a global understanding on its definition, a reference architecture (RA), requirements, and standards. In the following sections, an overview of the current IoT landscape will be given and some of the proposals that are on the table for discussion in several groups, alliances, and consortia focused on IoT will be highlighted. There is at least an agreement on some of the requirements that need to be addressed, but still there is space for improvement and even more collaboration among the stakeholders. For example, unique device identification, system modularity, security, privacy, and low cost are some of issues that need further discussion and action.

This chapter covers the fundamentals of IoT, its application domains, and the main challenges that still need to be surpassed. The rest of the chapter is organized as follows: Section 1.2 reviews the main definitions and concepts involved. Some of the proposed architectures and reference models (RMs) are described in Section 1.3. Section 1.4 includes an overview of IoT-enabling technologies and the efforts of several working groups and consortia to create standards for the IoT. Section 1.5 gives an overview of the main IoT application domains, and Section 1.6 highlights main IoT implementation challenges. The last section provides the main conclusions of the chapter and outlines current trends.

1.2 DEFINITION OF IoT

There have been several international organizations and research centers involved in the creation of common standards for the IoT. One of the first steps in this process has been to find a common definition. The first definitions of the IoT were tightly coupled to the radio-frequency identification (RFID)–related context of the Auto-ID Labs at MIT, where the term first emerged. As the concept became universal, the definition started to evolve to more general terms. For Kevin Ashton, the meaning of the IoT and the consequences of its implementation in our environments are the following (Ashton, 2009):

> "*If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste,*

* https://onelab.eu/.
† http://www.onem2m.org/.
‡ http://www.aioti.org/.

loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best. We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves."

Another definition of the IoT is the following (Atzori et al., 2010):

"*The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency IDentification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals.*"

The Study Group 20 (SG 20) was created in 2015 as a result of the 10-year experience period that followed the publication of the first ITU report on IoT in 2005 and the findings of the International Telecommunications Union Telecommunication Standardization Sector (ITU-T) Focus Group on Smart Sustainable Cities, which ceased to exist in 2015. In the SG 20 recommendation document Y.2060 (ITU-T, 2012), the following definition is given:

"*Internet of things (IoT): A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication technologies.*

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.
NOTE 2 – From a broader perspective, the IoT can be perceived as a vision with technological and societal implications."

The ITU-T document goes on to explain that IoT adds a new dimension ("any thing") to the already existing "any time" and "any place" communication provided by the digital connectivity expansion. In this context, "things" are defined as being physical or virtual identified objects capable of communicating. Physical objects are all kinds of everyday objects that are present in our environments and that can contain sensors, actuators, and communication capability. Examples of physical objects are electronic appliances, industrial machinery, and digitally enhanced everyday objects. Virtual objects exist in the information world and can be stored, accessed, and processed. Software is an example of a virtual object.

The European Union (EU) created the IoT European Research Cluster (IERC) as a platform for FP7 (7th Framework Programme for Research and Technological Development) projects on IoT. Currently, the IERC is Working Group 1 (WG 1) of the AIOTI, which was created to establish collaboration and communication between different entities involved in IoT development, standardization, and implementation.

The definition published on the IERC website* states that the IoT is

"*A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the information network*."

International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) Joint Technical Committee 1 (JTC1) was created in 1987 and is responsible for standard development in the information technology (IT) area, having so far published more than 3000 standards.† WG 10 (former SWG 5) is one of JTC1 working groups responsible for IoT-related issues.

* http://www.internet-of-things-research.eu/about_iot.htm.
† https://www.iso.org/committee/45020.html.

In one of the SWG 5 reports published in 2015, the adopted definition for IoT is given in the following terms (ISO/IEC JTC1, 2015):

> "*An infrastructure of interconnected objects, people, systems and information resources together with intelligent services to allow them to process information of the physical and the virtual world and react.*"

In the Request for Comments (RFC) 7452,* which talks about the architectures for networks of smart objects, IoT is defined as follows:

> "*The term 'Internet of Things' (IoT) denotes a trend where a large number of embedded devices employ communication services offered by Internet protocols. Many of these devices, often called 'smart objects,' are not directly operated by humans but exist as components in buildings or vehicles, or are spread out in the environment.*"

The IEEE IoT initiative published a document (IEEE, 2015) with an overview of the IoT applications and a proposal of a definition in order to start a discussion and to give its community members an opportunity to contribute to the definition of the IoT.† The document presents two definitions, one for the small-scale scenarios:

> "*An IoT is a network that connects uniquely identifiable 'Things' to the Internet. The 'Things' have sensing/actuation and potential programmability capabilities. Through the exploitation of unique identification and sensing, information about the 'Thing' can be collected and the state of the 'Thing' can be changed from anywhere, anytime, by anything."*

The other is for the large-scale scenarios:

> "*Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'things' to the Internet through the use of standard communication protocols. The interconnected things have physical or virtual representation in the digital world, sensing/actuation capability, a programmability feature and are uniquely identifiable. The representation contains information including the thing's identity, status, location or any other business, social or privately relevant information. The things offer services, with or without human intervention, through the exploitation of unique identification, data capture and communication, and actuation capability. The service is exploited through the use of intelligent interfaces and is made available anywhere, anytime, and for anything taking security into consideration.*"

A fairly complete collection of IoT definitions can be found in Minoli (2013), in which the definitions are organized into two categories: those that define IoT as a concept and those that define IoT as an infrastructure. The following definition that tries to encompass both the concept and the infrastructure can be found in the above-cited book:

> "*A broadly-deployed aggregate computing/communication application and/or application-consumption system, that is deployed over a local (L-IoT), metropolitan (M-IoT), regional (R-IoT), national (N-IoT), or global (G-IoT) geography, consisting of (i) dispersed instrumented objects ('things') with embedded one- or two-way communications and some (or, at times, no) computing capabilities, (ii) where objects are reachable over a variety of wireless or wired local area and/or wide area networks, and (iii) whose inbound data and/or outbound commands are pipelined to or issued by a(n application) system with a (high) degree of (human or computer-based) intelligence.*"

---

* https://tools.ietf.org/html/rfc7452.

† http://iot.ieee.org/definition.html.

Although the wording may be slightly different, it seems that there are several touching points among the definitions. For example, the IoT is made of (physical and virtual) objects that are uniquely identifiable, that are able to capture their context (sensors), and that are able to transmit and/or receive data over the Internet and, in the case of actuators, are able to change their own state or the state of their surroundings—all of which should ideally be done without or with very little direct human intervention.

1.3 PROPOSED ARCHITECTURES AND REFERENCE MODELS

The end goal of IoT systems is to achieve a synergy between different systems, meaning that they should interoperate and communicate automatically to provide innovative services to the users. Therefore, standardization is needed to ensure that IoT platforms will allow distinct systems to reliably interoperate.

While it is expected that the IoT will positively revolutionize all the different sectors of the economy in society, it will also produce a very large amount of data. This not only brings new challenges regarding the management, processing, and transmission of data, but above all, it also brings new concerns regarding data security. So, on top of standardization for interoperability, security standards are also needed to protect the individuals, businesses, and governments that will use the IoT systems (Dahmen-Lhuissier, 2016; ixia, 2016).

Recently, several attempts were made—and are still being made—to develop RAs, by either standards organizations or industries and universities. However, standardization is difficult to achieve in the real world. RAs are vital for standardization, as they define guidelines that can be used when planning the implementation of an IoT system (Weyrich and Ebert, 2016).

Therefore, with the intention of making interoperability between different IoT systems possible, several attempts have been made in recent years to create reference layered models for IoT (Bassi et al., 2013; Bauer et al., 2013; Gubbi et al., 2013). Several standards development organizations (SDOs) are also engaged in this process, as will be described below.

oneM2M specifications focus on the creation of a framework to support applications and services, such as smart grid, connected car, home automation, public safety, and health. During a workshop organized by the European Telecommunications Standards Institute (ETSI), which took place in November 2016, the European Commission highlighted the need for an open common RA for IoT, enabling the integration of different services, for the specific case of smart cities application. In fact, this is of critical importance not only to smart cities but also to all areas of application of IoT technologies. In addition to oneM2M standardization activities, ETSI has also created a working group on sustainable digital multiservice cities, specifically for the case of smart cities projects (Antipolis, 2016).

The IEEE has produced more than 80 standards* that relate to several areas of IoT systems and has around 60 ongoing projects to develop new standards also related to the IoT. Among all the standards, projects, and events promoted by IEEE, two important initiatives need to be emphasized: the IEEE Standards Association (IEEE-SA) engaged participants in key regions of the world to create the IoT Ecosystem Study, which encompasses three main areas—market, technology, and standards—but also examines the role of academia and research, and the importance of user acceptance; and the IEEE P2413 Working Group is focusing on the creation of a standard architecture for IoT, the "IoT architecture." The resulting draft standard basically defines an architectural framework for the IoT: it describes different IoT domains, gives definitions of IoT domain abstractions, and identifies commonalities between different IoT domains.†

* http://standards.ieee.org/innovate/iot/stds.html.
† http://standards.ieee.org/develop/project/2413.html.

The GSM Association (GSMA)* has gathered nearly 800 mobile operators and 300 companies worldwide to address four areas of the mobile industry: "Personal Data (Enabling trust through digital identity), Connected Living (Bringing the Internet of Things to life), Network 2020 (The future of mobile communications), Digital Commerce (Streamlining interactions and transactions)" (GSMA, 2016). In August 2015, the GSMA established a new project named Mobile IoT Initiative,† supported by a group of 26 of the world's leading mobile operators, equipment manufacturers, and module and infrastructure companies, to address the use of low-power wide area (LPWA) solutions in the licensed spectrum.

The GSMA Connected Living Programme (LP) is working with mobile operators to fasten the delivery of IoT solutions that exploit connectivity in innovative ways. In February 2016, the Connected LP also published new guidelines designed to promote the secure development and deployment of services in the IoT market. The result is the document entitled "GSMA IoT Security Guidelines," developed in conjunction with the mobile industry, which offers IoT service providers practical recommendations on handling common security and data privacy threats associated with IoT services (GSMA, 2016).

For 2017, the GSMA Connected LP focuses on four new goals: (1) Mobile IoT, which mainly addresses increasing the market awareness and support for licensed spectrum LPWA solutions; (2) completing the technical specification of the Consumer Remote SIM Provisioning; (3) positioning operators as key partners within the IoT big data market through the delivery of data sets and APIs; and (4) supporting operators in the provision of services that enable smart cities (GSMA, 2016). It is important to be aware of these new goals to get an idea of the directions in which efforts are being made and of what is happening at the moment in the area.

ITU also created the Internet of Things Global Standards Initiative (IoT-GSI),‡ which worked in detailing the requirements for developing the standards that are necessary to enable the deployment of IoT on a global scale, taking into account the work done in other SDOs. In July 2015, this group decided to create the SG 20, which focuses on "IoT and its applications including smart cities and communities." Therefore, all activities conducted by the IoT-GSI were transferred to the SG 20,§ which has produced around 300 related documents so far.

Both Industrial Internet Reference Architecture (IIRA)¶ and Reference Architecture Model for Industrie 4.0 (RAMI 4.0) were developed, focusing on taking advantage of IoT technology to increase the efficiency of the industrial processes, either improving manufacturing itself or making the supply chain from the suppliers to the customers more effective.

Sensor Network Reference Architecture (SNRA),** in turn, provides a general overview of the characteristics of a sensor network and the organization of the entities that comprise such a network. It also describes the general requirements that are identified for sensor networks, which relate to IoT systems since sensor networks are used by IoT systems as a tool for collecting data. A working group created by ISO/IEC,†† involving industry and commerce, academic and research bodies, and government, is working on the development of an RA for IoT (IoT RA—IoT Reference Architecture) that aims to describe the characteristics and aspects of IoT systems, define the IoT domains, describe the RM of IoT systems, and describe the interoperability of IoT entities (ISO/IEC JTC1, 2016). IoT RA intends to become the common reference for all the RAs already proposed by other organizations, including Internet of Things—Architecture (IoT-A) and the standards developed by ITU (Yoo, 2015).

Since there is no universally accepted definition of IoT, different groups have developed different approaches according to the domain in which they are active (ISO/IEC, 2014).

---

* http://www.gsma.com/.

† http://www.gsma.com/connectedliving/mobile-iot-initiative/.

‡ https://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

§ https://www.itu.int/en/ITU-T/studygroups/2017-2020/20/Pages/default.aspx.

¶ http://www.iiconsortium.org/IIRA.htm.

** https://www.iso.org/obp/ui/#iso:std:iso-iec:29182:-1:ed-1:v1:en.

†† https://www.iso.org/standard/65695.html.

Additionally, GS1,* a nonprofit organization working in the area of barcoding standardization, claims that the evolution of standards for IoT has followed a path where no standards existed to a situation where too many standards are available, leading to difficult choices to be made when designing IoT applications (GS1, 2016, 1). These difficulties may be accentuated by manufacturers who try to protect their products and solutions and are not necessarily interested in adopting open standards or ensuring interoperable solutions.

In 2013, a consortium involving industry and university partners, like Alcatel-Lucent, IBM, NEC Siemens, Sapienza University of Rome, and University of Surrey, created an architectural reference model (ARM) for IoT, named IoT-A (Bassi et al., 2013). For the partners, achieving interoperability between solutions across various platforms could only be ensured through interoperability both at the communication level and at the service level. At the end of the project, funded by the EU, the benefits of the developed architecture were demonstrated through the implementation of real-life use cases.

In the following sections, some of the more relevant RAs are briefly described. As they are still being developed, there might be new updates in this field.

1.3.1 IoT-A

Currently, the IoT-A project is no longer active. However, IoT-A is described here since it is being used as a basis for developing other architectures, such as the IoT RA or Reference IoT Layered Architecture (RILA), which are also discussed in the following sections.

The IoT-A ARM was created in order to achieve interoperability between different IoT systems (Bassi et al., 2013). The IoT ARM is defined to be abstract so that it can be used as a reference for generating concrete system architectures. It consists of an RM and an RA.

The RM, presented in Figure 1.1, provides a common understanding of the IoT domain by modeling its concepts and their relationships. Similar to the Open Systems Interconnection (OSI) model, the IoT RM by itself does not specify the technical particularities of an IoT system.

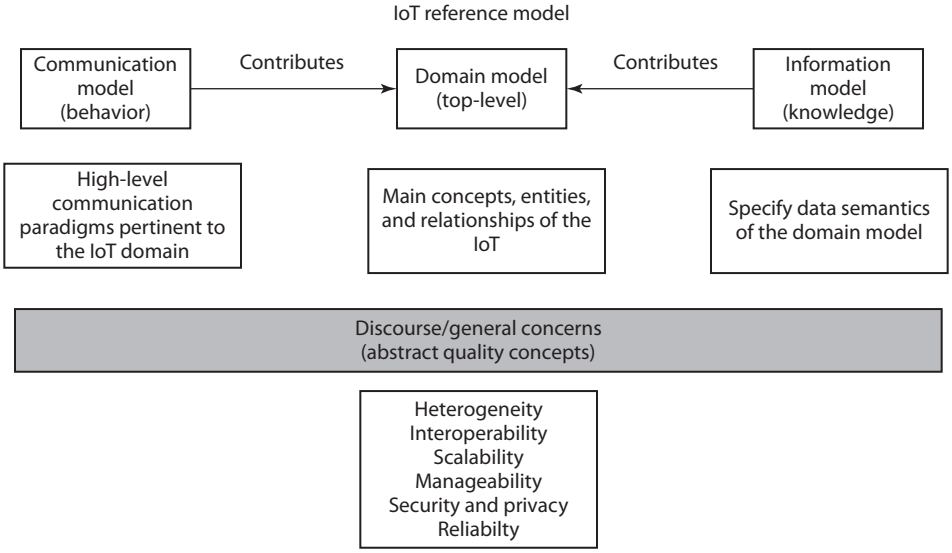

FIGURE 1.1 RM proposed by IoT-A. (Adapted from Bassi, A., et al., *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, Springer, Berlin, 2013, 163–211.)

* http://www.gs1.org.

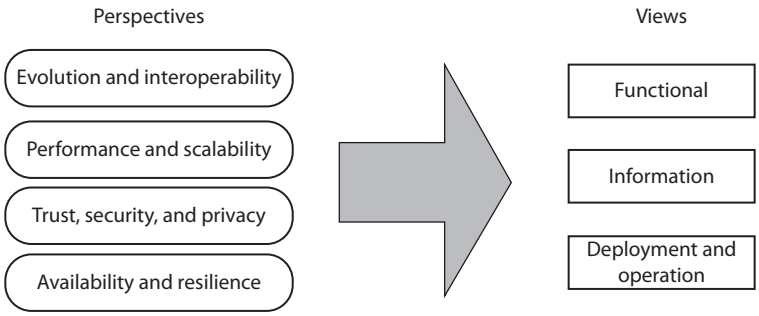

FIGURE 1.2 Perspectives and views of IoT-A. (Adapted from Bassi, A., et al., *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, Springer, Berlin, 2013, 163–211.)

The *domain model* considers a top-level description of the concepts and entities (physical entities, devices, resources, and services) that represent particular aspects of the IoT domain, and defines their relations. Therefore, the domain model can also be used as a taxonomy of the IoT.

The *information model* specifies the data semantics of the domain model; that is, it refers to the knowledge and behavior of the entities considered in the domain model, since they are responsible for either keeping track of certain information or performing specific tasks (it describes which type of information the entities are responsible for).

The *communication model*, in turn, addresses the main communication paradigms necessary for connecting entities, ensuring interoperability between heterogeneous networks. The proposed communication model is structured in a seven-layer stack and describes how communication has to be managed, by each layer, in order to achieve the interoperability features required in the IoT. It also describes the actors (communicating elements) and the channel model for communication in IoT.

The RA of IoT-A mainly consists of "views" and "perspectives," which vary depending on the requirements of each specific application. Figure 1.2 illustrates that the perspectives "evolution and interoperability," "performance and scalability," "trust, security, and privacy," and "availability and resilience" are applied to all the views: the "functional" view, the "information" view, and the "deployment and operation" view, respectively.

While applying perspectives to views, not every view is impacted by the perspectives in the same manner or grade. For example, the perspectives have a high impact when applied to the operation view.

1.3.2 IoT RA

IoT RA, created by the ISO/IEC* (CD 30141), envisions the construction of an IoT system based on a generic IoT conceptual model (CM) that includes the most important characteristics and domains of IoT. Then, it uses the CM as a basis to create a high-level system-based RM. This reference model is, in turn, structured in five architectural views (functional view, system view, user view, information view, and communication view) from different perspectives, which compose the RA itself. Figure 1.3 shows the relation between these three components (CM, RM, and RA).

In essence, the IoT RA provides the basics to create a concrete system architecture. The IoT RA is considered an application-specific architecture or a "target system architecture" since the RA can adapt to the requirements of a specific system, like agricultural system, smart home/building, smart city, and so forth.

* https://www.iso.org/standard/65695.html.

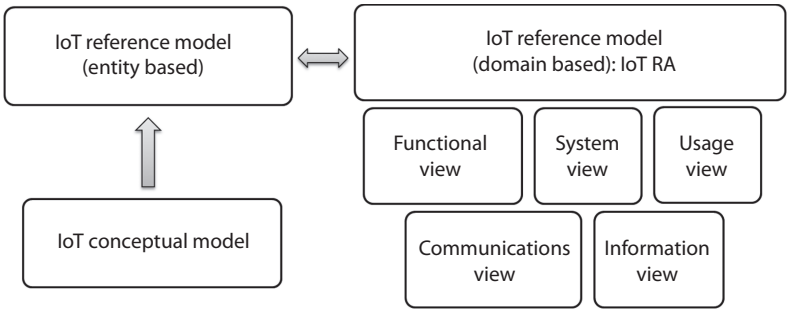

FIGURE 1.3 Relation between CM, RM, and RA. (Adapted from ISO/IEC, Information technology—Data structure—Unique identification for the Internet of things, ISO/IEC 29161:2016, August 2016, https://www.iso.org/obp/ui/#iso:std:iso-iec:29161:ed-1:v1:en.)

1.3.3 IEEE P2413

IEEE P2413 is based on ISO/IEC/IEEE 42010:2011: "Systems and Software Engineering Architecture Description."* The goal is not to create a new standard but to address common aspects of different application domains of the IoT. The IEEE working group is collaborating with ISO, ITU-T, and the Industrial Internet Consortium (IIC), among others, with the common goal of achieving better standards for the IoT in all its areas of application. The focus is on achieving interoperability, together with other quality attributes, such as protection, privacy, security, and safety. Some of these challenges are further discussed in Section 1.6.

1.3.4 Industrial Reference Architectures

The IIRA† is a standard-based open architecture for Industrial Internet Systems (IISs), proposed by the IIC Technology Working Group, whose members are companies like AT&T, Cisco, IBM, General Electric, and Intel. The Industrial Internet is considered an IoT system, enabling intelligent industrial operations and focusing on key characteristics for this type of systems: safety, security, and resilience. IISs cover energy, healthcare, manufacturing, the public sector, transportation, and related industrial systems.

The Industrial Internet Architecture Framework (IIAF) is based on ISO/IEC/IEEE 42010:2011, and as such, it uses the same constructs and common terms, such as viewpoints, concerns, and stakeholders, as well as views and models.‡ The IIRA is the result of applying IIAF to the Industrial IoT systems. Table 1.1 shows an overview of the IIRA. Each viewpoint influences the viewpoints below it. In turn, lower viewpoints validate and sometimes cause revisions in the higher viewpoints. There are some crosscutting concerns, such as security and safety, which are discussed in other reports from the IIC.

Initially designed for German industry, RAMI 4.0, in turn, is a result of cooperation between: Plattform Industrie 4.0 (Industrie 4.0 [I4.0] is considered a specialization within IoT); some German associations, like BITKOM, VDMA, and ZVEI; and several German companies (Adolphs et al., 2015). Their main goal was to achieve a common understanding of what is necessary to evolve from current industries and make I4.0 become a reality. To do that, it was necessary to develop an architecture model to be used as a reference in this migration.

---

* http://grouper.ieee.org/groups/2413/Intro-to-IEEE-P2413.pdf.
† http://www.iiconsortium.org/IIRA.htm.
‡ http://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf.

TABLE 1.1
IIRA Overview: Viewpoints and Their Concerns and Stakeholders

Viewpoints	Concerns	Crosscutting Concerns		Stakeholders
Business	Identification of stakeholders, business vision, values, and objectives of an Industrial IoT system	Safety	Security	Decision makers, product managers, system engineers
Usage	Expected system usage			System engineers, product managers, other users
Functional	Functional components, interfaces and interactions between them			System architects, developers, integrators
Implementation	Technologies needed, communication protocols, life cycle			System architects, developers, integrators, system operators

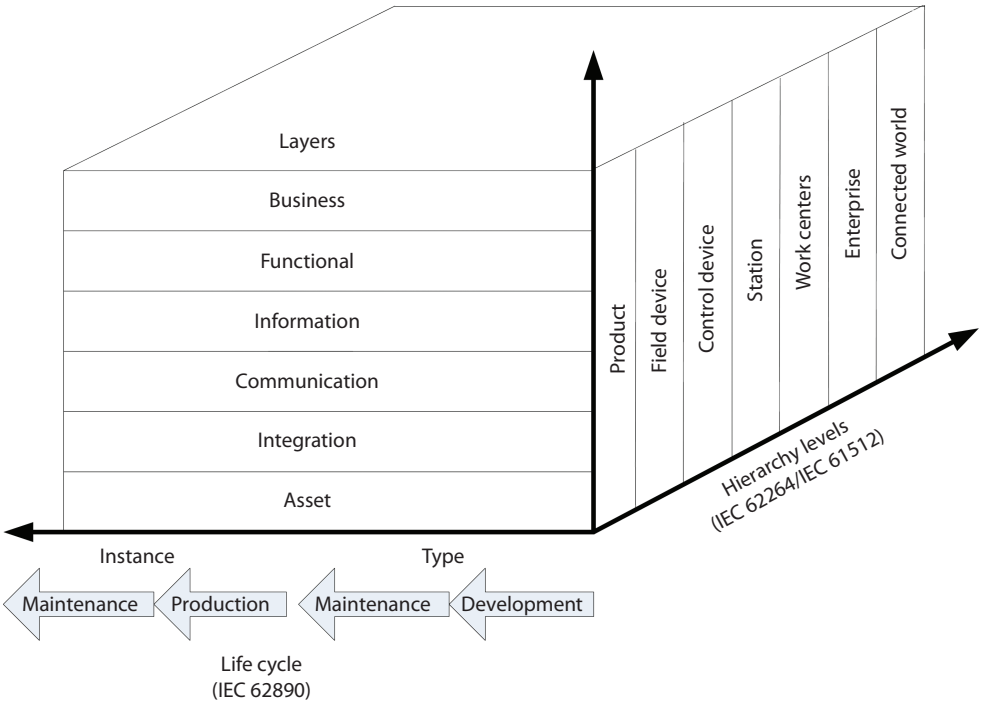

FIGURE 1.4 RAMI 4.0. (Adapted from Adolphs et al., Reference Architecture Model for Industrie 4.0 (RAMI 4.0.), 2015, https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report__Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf.)

RAMI 4.0 focuses on the optimization of central industrial processes, namely, research and development, production, logistics, and service. It describes the structures and functions of the I4.0 components, based on existing and relevant standards.

Figure 1.4 shows the RAMI 4.0 architecture model, which is a three-dimensional model, where the horizontal axis represents the life cycle of systems or products, distinguishing between "type" (life cycle of a product from the idea to the product, going through design, development, and testing)

and "instance" (it represents the manufacturing of a type; its life cycle goes from manufacturing, selling, and delivering to the client, to being installed in a particular system). The vertical axis (six layers), in turn, corresponds to the IT perspective of an I4.0 component, meaning that it breaks complex projects into smaller parts, like business processes, functional descriptions, communications behavior, and hardware/assets. Finally, the third axis represents a functional hierarchy, which does not refer to equipment classes or hierarchical levels of the automation pyramid, but to grouping functionalities and responsibilities within the factories. It contains core aspects of I4.0, such as field device, control device, station, work centers, and enterprise, but expands the hierarchy levels of the IEC 62264 standard by adding "product" and "connected world."

1.3.5 Other Reference Models and Architectures for IoT

So far, there have been several contributions to create RMs for IoT, most of them based on IoT-A. In fact, up to now, several architectures have been proposed, but as they are designed for a specific IoT application, they cannot be used as a reference, since they do not adapt to other applications' requirements (Yin et al., 2015; Pang, 2013; Vlacheas et al., 2013; Domingo, 2012; Yun and Yuxin, 2010). An alternative architectural stack for the "web of things" consists of "levels of functionalities," with each level composed of a set of application protocols and tools (Guinard and Trifa, 2016). The idea is to provide developers with the necessary tools to implement IoT products and applications, and to maximize reuse and interoperability. In this section, only some of the most significant proposals that might be considered as a reference are briefly described.

1.3.5.1 Cisco Reference Model

In 2014, Cisco proposed a seven-layer RM (Cisco, 2014), which is represented in Figure 1.5, giving a more practical point of view. The lowest level includes the physical devices and controllers (the *things*); then there is connectivity and, above that, edge (fog) computing, where some initial

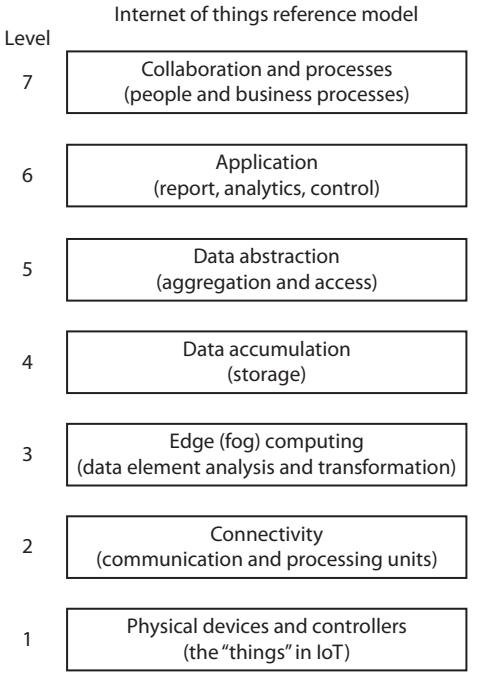

FIGURE 1.5 IoT RM proposed by Cisco. (Adapted from Cisco, The Internet of things reference model, 2014, http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.)

aggregation, elimination of data duplication, and analysis can be carried out. The lower three levels, in turn, are considered operational technology (OT). The top four levels relate to the IT. The lowest level in the IT part of the stack is storage, and this is followed, going toward the top, by data abstraction, applications, and collaboration and (business) processes.

1.3.5.2 Reference IoT Layered Architecture

Every IoT RA must include some essential components, such as interoperability and integration components, context-aware computing techniques, and security guidelines for the whole architecture (Karzel et al., 2016). The resulting proposed architecture is RILA. RILA is a more concrete architecture, intended to be easier to comprehend for customers and industry than the high-level IoT-A. It not only provides guidelines of how to put IoT-A in practice but also demonstrates that this architecture can really be implemented using actual use cases. RILA acts between things, devices, and the user.

RILA consists of six layers, as depicted in Figure 1.6. Besides these layers, there are two cross section layers, "security" and "management," that affect all other layers.

The *device integration layer* includes all the different types of devices, receives their measurements, and communicates actions. This layer can be seen as a translator that speaks many languages (Karzel et al., 2016). The output of the sensors and tags, as well as the input of the actuators, depends on the protocol they implement.

The *device management layer* is responsible for receiving device registrations and sensor measurements from the device integration layer, and for communicating status changes for actuators to the device integration layer. Then, the device integration layer checks if the status change (i.e., the action) conforms with the respective actuator and translates the status change to the actuator. The device management layer controls the devices that are connected to the system; every change to a device's registration, as well as new measurement data, should be communicated from the device integration layer to the device management layer, so the information can be updated and stored.

Normally, the *data management layer* is a central database (but it can also be a data warehouse or even a complete data farm, in the case of larger IoT systems) that stores all data of a thing. Thus,

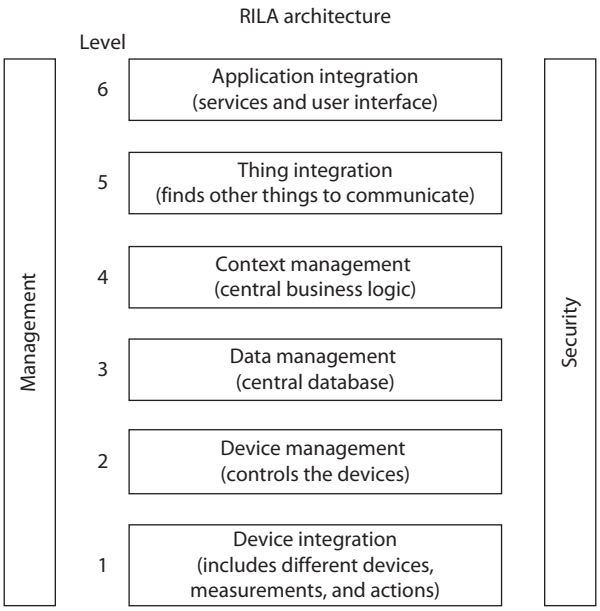

FIGURE 1.6 Reference IoT layered architecture. (Adapted from Karzel, D., et al., A reference architecture for the Internet of things, January 29, 2016, https://www.infoq.com/articles/internet-of-things-reference-architecture.)

the implementation of the data management layer strongly depends on the use case (Karzel et al., 2016).

The *context management layer* defines the central business logic and is responsible for tasks like defining the goals of the thing, consuming and producing the context situations of the things, evaluating the context situation toward the goals, triggering actions that will help to fulfill the goal according to the evaluated rules, and finally, publishing context situations for other things.

The *thing integration layer* is responsible for finding other things to communicate, verifies if communication with the new thing is possible, and is responsible for a registration mechanism.

The *application integration layer* connects the user to the thing, being considered the service layer, or even a simple user interface. The concrete implementation of the layer depends on the use case.

1.4 ENABLING TECHNOLOGIES

In the previous section, a few international organizations that are engaged in defining and developing common standards for the IoT were already mentioned. Many of these are integrated in alliances and consortia that include members from industry, SDOs, manufacturers, network and service providers, academia, and research laboratories.* oneM2M, for example, consists of eight important SDOs from all around the world: ARIB (Japan), ATIS (United States), CCSA (China), ETSI (Europe), TIA (United States), TSDSI (India), TTA (Korea), and TTC (Japan), which have come together with six industry partners and consortia (Broadband Forum, Continua Alliance, GlobalPlatform, HGI, Next Generation M2M Consortium, and OMA) and more than 200 member organizations, including companies (like Alcatel, Nokia, Huawei, Deutsche Telekom, and Qualcomm) and universities.

ISO WG 10 created a very interesting and comprehensive mind map with six IoT-related areas: requirements, technologies, application areas, stakeholders, standards, and other considerations. The map is available on their website as an appendix of their IoT report published in 2015 (ISO, 2017, 1). For technologies, a separate mind map was created due to such a great number of existing and developing technologies that all strive to be key enabling technologies for the IoT. The map is not completely exhaustive due to space limitations, but further details can be added easily to the existing branches, probably originating one or more new separate mind maps for each branch.

This section presents a short overview of some of the technologies that are being used for connected objects identification and discovery, communication, and devices. In the final part of this section, we will see some of the currently available online platforms for IoT project prototyping, development, and testing.

1.4.1 Identification and Discovery

For the things to be identified within a distributed networked system, a unique identifier is needed for each thing. And here a *thing* can be anything ranging from a physical to a virtual object, an event, or a person. Data such as time and location—either geographic (coordinates) or within a network (Uniform Resource Identifier [URI] or IP)—can be used for identification purposes. The Electronic Product Code (EPC) is mostly used for counting and tracking goods in the supply chains without human intervention. While RFID-driven EPCs are attached to the physical objects, URIs and IPs allow the identification and discovery of an object's presence on the web. HyperCat,† for example, is a solution that allows us to expose any number of URIs, together with additional information attached to them in Resource Description Framework (RDF)–like format.

* https://www.postscapes.com/internet-of-things-alliances-roundup/.

† http://www.hypercat.io/.

IP addresses are also used as identifiers for networked objects, together with name labels, which can be used for human readability and resource discovery using a naming service, such as mDNS.* mDNS is an IETF project that aims to adapt the well-established Domain Name System (DNS) programming interfaces and formats to small networks where there are no name servers available.

People, in turn, can be identified through the devices they carry along or through more sophisticated techniques, such as biometric data obtained through face or iris recognition, fingerprints, voice, and so on. The ISO IoT technology mind map includes more identification-related technologies and possible solutions.

In 2016, ISO/IEC published the 29161 standard (ISO/IEC, 2016), which aims to ensure full compatibility among different identification forms.

1.4.2 Communication Patterns and Protocols

RFC 7452† describes four basic communication patterns for IoT environments: device-to-device communication pattern, device-to-cloud communication pattern, device-to-gateway communication pattern, and back-end data sharing pattern.

The device-to-device pattern is applied when two devices communicate directly, normally using a wireless network. There are several protocol stacks available to carry out this type of communication. Depending on the usage scenario, the protocol stack may include, for instance, Bluetooth or IEEE 802.15.4, IPv6, User Datagram Protocol (UDP), and Constrained Application Protocol (CoAP).

The device-to-cloud communication pattern is used when data captured by the device from the environment is uploaded to an application service provider. Communication is based on IP, but when the device manufacturer and the application service provider are the same, the integration of other devices may be difficult. For this not to happen, the protocols used to communicate with the server need to be made available.

The device-to-gateway communication pattern may be used when the system contains non-IP devices, when support for legacy devices is needed, or when additional security functionality must be implemented. Gateways can also be mobile, providing only temporary connections to the Internet. Smartphones are an example of those.

The back-end data sharing pattern is used when there is a need to analyze combined data from several sources. RESTful APIs can be used, although they are not standardized. This pattern may allow users to move their data from one IoT service to another (Rose et al., 2015).

Beyond some well-known communication standards, like Bluetooth, Wi-Fi, or GSM, IoT systems use many more. It is worth pointing out that new communication standards are being developed specifically for some of the IoT scenarios. For example, when the system is composed of devices with constrained resources across wide area networks, low-power wide area network (LPWAN) solutions must be applied.

On the one hand, the last two decades or so registered immense growth in the field of mobile telecommunications, with devices that have more and more resources in terms of processors, memory, sensors, and connectivity. As such, 3GPP and the mobile operators have been making a huge effort toward new standards for mobile communications with even larger bandwidths, higher bit rates, and support for multimedia live streaming.

On the other hand, solutions for the scenarios that will not so much include resource-rich devices, but mostly resource-constrained devices, stayed behind and only appeared recently. In 2016, 3GPP concluded a new standard for the IoT called NB-IoT (3GPP, 2016), which is supported by leading manufacturers and by the world's 20 largest mobile operators (Vodafone Group, 2016). NB-IoT is a technology that allows us to bidirectionally and securely connect multiple sensors and devices with

* http://multicastdns.org/.

† https://tools.ietf.org/html/rfc7452.

low bandwidth requirements. It is a technology that requires low energy consumption (more than 10 years of autonomy) and allows strong penetration of the radio signal in indoor environments.

In the meantime, many other low-power solutions for wide area networks, such as LoRa, NWave, and Sigfox, have been developed and adopted by many IoT deployments. It is predictable that there will be a convergence among these technologies in the near future, and some of them will eventually prevail, while others will disappear or remain in use in legacy deployments. Table 1.2 summarizes some of the communication protocols and standards currently in use.

1.4.3 Devices and Test Beds

A wide range of specialized and multipurpose sensors are available on the market, as well as many SBCs with embedded sensors or with support for several sensors and actuators. Wearable devices are also acquiring more and more enthusiasts, especially in the area of sports and physical activity tracking, sometimes in addition to the already well-equipped smartphones with several embedded sensors.

Sensors enable devices to capture data from their environment. They can be categorized in different ways. Here is a nonexhaustive list of possible categories and some examples:

- *Location*: GPS, GLONASS, Galileo, Wi-Fi, Bluetooth, ultra-wideband (UWB)
- *Biometric*: Fingerprint, iris, face
- *Acoustic*: Microphone
- *Environmental*: Temperature, humidity, pressure
- *Motion*: Accelerometer, gyroscope

Actuators, in turn, allow devices to act on their environment and may be of different types, like hydraulic, pneumatic, electric, mechanical, or piezoelectric.

The SBCs are becoming more and more popular among both hobbyists and researchers. They are low cost (less than $50), provide a reasonable amount of processing power and RAM, sometimes have embedded sensors or support the connection of external sensors, and support wireless connectivity (Wi-Fi, Bluetooth Low Energy [BLE], and ZigBee). Mostly, these are Linux machines. The most popular examples are Arduino, Raspberry Pi, BeagleBone Black, Intel Edison, and Pine 64.* Their characteristics are summarized in Table 1.3.

As an alternative to deploying one's own hardware on site, there are laboratories around the world where the physical devices are located and can be tested remotely, especially for large-scale scenarios testing. Examples are the FIT IoT-lab,† located in France; the III-IoTLab,‡ in Taiwan; and iMinds,§ in Belgium. All of them are parts of OneLab,¶ which offers several test beds giving developers a means to quickly implement and test their projects in controlled environments, being able to evaluate them before the actual deployment takes place.

OneLab is not restricted to the IoT area; it also offers test beds for other areas, like cloud computing or software-defined networks. Regarding test beds for IoT, there is one test bed specifically targeted for *smart cities* applications and another for *connected commerce*, which addresses logistics monitoring (e.g., monitoring the quality of food and its transportation during the whole supply chain).

* https://www.pine64.org/.
† https://www.iot-lab.info/.
‡ https://iot.snsi.iii.org.tw/.
§ http://ilabt.iminds.be/.
¶ https://onelab.eu/.

TABLE 1.2
Overview of Communication Technologies and Standards for IoT

Name	Frequency	Range	Examples	Standards
BLE	2.4 GHz	1–100 m >100 m	Headsets, wearables, sports and fitness, healthcare, proximity, automotive	IEEE 802.15.1 Bluetooth SIG
EnOcean	315, 868, 902 MHz	300 m outdoor 30 m indoors	Monitoring and control systems, building automation, transportation, logistics	ISO/IEC 14543-3-10
GSM LTE	Europe: 900 MHz and 1.8 GHz United States: 1.9 GHz and 850 MHz		Mobile phones, asset tracking, smart meter, M2M	3GPP
LoRa	Sub-1 GHz ISM band	2–5 km urban 15 km suburban 45 rural	Smart city, long range, M2M	LoRaWAN
NB-IoT	700–900 MHz	10–15 km rural deep indoor penetration	Smart meters, event detectors, smart city, smart home, industrial monitoring	3GPP LTE Release 13
NFC	13.56 MHz	Under 0.2 m	Smart wallets, smart cards, action tags, access control	ISO/IEC 18092 ISO/IEC 14443-2, -3, -4 JIS X6319-4
NWave	Sub-1 GHz ISM band	Up to 10 km	Agriculture, smart city, smart meter, logistics, environmental	Weightless
RFID DASH7	120–150 kHz (LF), 13.56 MHz (HF), 2450–5800 MHz (microwave), 3.1–10 GHz (microwave), 433 MHz (UHF), 865–868 MHz (Europe), 902–928 MHz (North America) (UHF)	10 cm–200 m 0–5 km	Road tolls, building access, inventory, goods tracking, building automation, smart energy, smart city logistics	ISO 18000
Sigfox	900 MHz	3–10 km urban 30–50 km rural	Smart meters, remote monitoring, security	
Weightless	470–790 MHz	Up to 10 km	Smart meters, traffic sensors, industrial monitoring	Weightless
Wi-Fi	2.4 GHz, 3.6 GHz, 4.9/5 GHz	Up to 100 m	Routers, tablets, smartphones, laptops	IEEE 802.11
Z-Wave	ISM band 865–926 MHz	100 m	Monitoring and control for home and light commercial environments	Z-Wave Recommendation ITU G.9959
ZigBee	2.4 GHz; 784 MHz in China, 868 MHz in Europe, and 915 MHz in the United States and Australia	10–20 m	Home and building automation, WSN, industrial control	IEEE 802.15.4

Source: Data from Postscapes, IoT technology guidebook, IoT Technology | 2017 Overview Guide on Protocols, Software, Hardware and Network Trends, 2017, https://www.postscapes.com//internet-of-things-technologies/; Opensensors, How to choose the best connectivity network for your Project, 2017, https://publisher.opensensors.io/connectivity; ETSI (European Telecommunications Standards Institute), SmartM2M; IoT standards landscape and future evolutions, ETSI TR 103 375 V1.1.1 (2016-10), 2016, http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf.

Note: M2M, machine-to-machine; LF, low frequency; HF, high frequency; UHF, ultra-high frequency.

TABLE 1.3
Characteristics of Some of the Currently Available Single-Board Computers for IoT

	Models	CPU	RAM	Operating System	Price ($)	Connectivity	Embedded Sensors
Arduino	20+ models	ATmega, ATSAM, AR9331, etc.	0.5 kB–16 MB	Linux	30	Ethernet, Wi-Fi, extension boards	Extensions
Beagle board	BeagleBone Black	AM335x, 1 GHz; ARM Cortex A8	512 MB–1 GB	Linux	50	Ethernet	Extensions
Intel	Edison, Joule, Galileo	Intel Atom, Intel Quark	256 MB–4 GB	Linux	20–60	Wi-Fi, Bluetooth	
Pine 64	Pine A64, Pine A64+	ARM Cortex A53, 1.2 GHz	512 MB–2 GB	Linux, Android, Windows IoT	15–29	Ethernet	
Raspberry Pi	Zero, RPi 1 A+, RPi 2 B+, RPi 3 B	ARM1176, 1 GHz; ARM1176; ARM Cortex A7; ARMv8, 1.2 GHz	512 MB–1 GB	Linux, Windows IoT	20–40	Wi-Fi, BLE, Ethernet, extensions	SenseHAT, other

1.5 APPLICATION AREAS: AN OVERVIEW

A symbiosis between platforms, applications, devices, and services gives the ability to improve citizens' well-being and quality of life. The great potentialities offered by the IoT make the development of a huge number of applications possible, while it also plays a crucial role in the so-called fourth Industrial Revolution (I4.0). The IIC* was created with the goal of transforming industry through intelligent, interconnected objects that may improve performance, lower costs, and increase reliability. This consortium considers that industry involves the areas of energy, healthcare, manufacturing, smart cities, and transportation.

Nevertheless, the areas of application cover various sectors of society and are grouped in diverse ways in the literature. There are at least two (Atzori et al., 2010; AIOTI, 2015) fairly complete and interesting classification schemes of the application domains. Considering the most relevant research made on applications, but essentially these two sources, an overview of the main application domains is shown in Figure 1.7.

As the figure depicts, the main areas of application are smart cities, healthcare, smart homes and buildings, mobility and transportation, energy, industry, agriculture, and the environment/planet. Note that some applications, like environmental monitoring, can fit into different groups, like smart city, smart buildings, the environment, and industry. It is worth mentioning that in the context of IoT, it is not possible to develop a "one-size-fits-all" solution. For example, a solution for home environmental monitoring may not be adequate for industrial ambient monitoring due to different types of physical conditions and relevant parameters. An industrial setting requires different levels of accuracy, security, and robustness for the deployed sensors and software, while a home environment usually does not impose such restrictions. Some examples of these applications are briefly introduced below.

1.5.1 Smart Cities

Finding ways to use technology to improve the quality of life in a city has become one of the most popular research topics in the area of IoT applications (Yin et al., 2015; Zanella et al., 2014; Vlacheas et al., 2013; AT&T, 2017). Smart city solutions include several areas, ranging from water and waste management (like smart dumpsters) (Hong et al., 2014; Phithakkitnukoon et al., 2013; Smartup Cities, 2017), lighting control (Castro et al., 2013), energy (Kyriazis et al., 2013), transportation, traffic, and parking management, to building efficiency, services, and safety (Perera et al., 2014).

Even though smart buildings, transportation and mobility, and energy are sometimes included under the smart cities umbrella, Figure 1.5 dedicates a separate branch to each, due to the importance that these areas are receiving.

Some examples of real-life implementations occur in the cities of London† and Greenwich in the United Kingdom; Santander (Sanchez et al., 2011), Barcelona, and Murcia in Spain; Amsterdam in Holland; Aarhus in Denmark; Oulu (Gil-Castineira et al., 2011) in Finland; several towns in Korea; and Bordeaux in France. AT&T is helping cities to deploy integrated smart city solutions and will deliver solutions in some cities in the United States. The CITYkeys‡ project, funded by the European Commission's Horizon 2020 program, aims at developing an evaluation framework to compare smart city solutions across European cities.

1.5.2 Healthcare

IoT technologies may bring significant benefits to the healthcare domain, namely, in two areas: clinical care and remote monitoring. Basically, the use of small-sized, low-cost, and low-power wearable

* http://www.iiconsortium.org/about-industrial-internet.htm.
† http://www.organicity.eu.
‡ http://www.citykeys-project.eu.

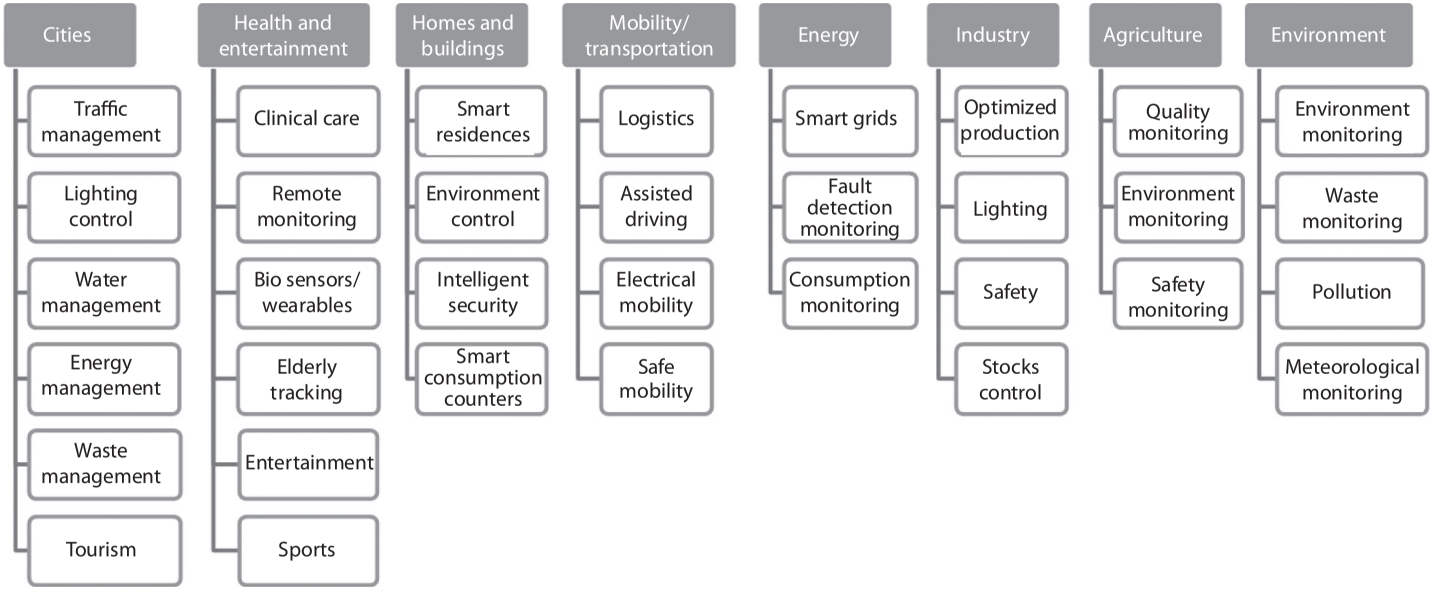

FIGURE 1.7 Applications grouped in domains. (Based on Atzori, L., et al., *Computer Networks*, 54 (15), 2787–2805, 2010; AIOTI, Internet of things applications, 2015, https://aioti.eu/aioti-wg01-report-on-internet-of-things-applications/.)

biosensors can enhance the quality of life of people suffering from chronic diseases or even during emergencies, either inside (Domingo, 2012; Doukas and Maglogiannis, 2012; Yang et al., 2014; Bui and Zorzi, 2011; Dohr et al., 2010; X. Li et al., 2011) or outside their homes (Domingo, 2012; Doukas and Maglogiannis, 2012). Elderly tracking or ambient assisted living (AAL) encompasses technical systems to support elderly people in their daily routine to allow an independent and safe lifestyle as long as possible. This is a special case of healthcare that has gained increased importance due to the problem of population aging (Yang et al., 2014; Dohr et al., 2010). Another interesting example is using IoT in noninvasive glucose-level sensing for diabetes management (Istepanian et al., 2011) or using an IoT platform to improve the life of people with disabilities (Domingo, 2012).

1.5.3 Smart Homes and Smart Buildings

Smart home applications can range from elderly monitoring (Yang et al., 2014) and home automation, in either air conditioning control and monitoring or lighting control, to consumption monitoring and energy saving (Wei and Li, 2011; Kelly et al., 2013), or even solar greenhouse production (Wang et al., 2004).

The focal point of IoT applications for "smart buildings" or "intelligent buildings" is essentially cost savings, providing the building with some intelligence, through building automation. These applications mainly focus on air conditioning and lighting monitoring and control, and on consumption monitoring and energy saving (Wei and Li, 2011; Moreno et al., 2014; Brad and Murar, 2014; Ji et al., 2014). Security is also an important issue; therefore, fire and intrusion monitoring are also crucial (Ryu, 2015; Li et al. 2013; Li, 2013). Intel, Telit, IBM, and many others have several solutions for smart building implementations (Zhong and Dong, 2011).

1.5.4 Mobility and Transportation

All types of vehicles in a city (cars, trains, buses, and bicycles) are becoming more equipped with sensors and/or actuators, resulting in a network composed of a set of mobile sensors. Both roads and rails, as well as transported goods, are also equipped with tags and sensors that send important information to traffic control sites. This not only allows monitoring of the status of the transported goods, but also allows the creation of innovative solutions, allowing transportation vehicles to better route the traffic or providing the tourist with appropriate transportation information.

Moreover, modern cars are also equipped with several sensors, forming a kind of in-vehicle network, which provides kinematics information, automotive diagnostic services, and so forth. Cars can be further equipped with external sensing devices to monitor specific physical parameters, such as pollution, humidity, and temperature. Thus, the concept of "smart vehicles" emerges.

If properly collected and delivered, such data can contribute to make the road transport greener, smarter, and safer (Campolo et al., 2012; Zouganeli and Svinnset, 2009). For example, driving recommendations that aim at eco-efficiency for public transportation and reducing fuel consumption and emission can be provided (Tielert et al., 2010; Kyriazis et al., 2013). Mobile applications, such as Google Traffic or Waze,* rely on user-contributed data to monitor traffic conditions. Smart traffic light infrastructures can be used to improve the life of drivers or make cycling or driving in cities safer and smoother. For example, combining data from smartphones carried by cyclists and traffic data gathered from different kinds of sensors deployed in the traffic light infrastructure of a city may allow for an intelligent traffic light orchestration, letting cyclists drive smoothly without unnecessary stopping at each crossroad (Anagnostopoulos et al., 2016). Another specific area of application is modern logistics, which refers to monitoring the whole process of the physical movement of goods from suppliers to demanders, in order to ensure their quality (Zhengxia and Laisheng, 2010; Zhang et al., 2011).

* https://www.waze.com/.

1.5.5 Energy

The smart grid is a recent kind of intelligent power system that can improve energy efficiency, reduce environmental impact, improve the safety and reliability of the electricity supply, and reduce the electricity transmission of the grid. The integration of IoT technology in smart grids can help to implement fault detection and monitoring, as well as consumption monitoring, through the installation of energy sensors (Yun and Yuxin, 2010; L. Li et al. 2011; Liu et al., 2006; Bui et al., 2012; Ou et al., 2012).

Other groups of related solutions envision the heat and energy management in homes and buildings to accomplish an energy savings purpose (Kyriazis et al., 2013; Sundramoorthy et al., 2010). Using IoT technology to collect data on energy consumption can also help to improve the energy efficiency and competitiveness of manufacturing companies at the energy production level (Shrouf and Miragliotta, 2015).

1.5.6 Smart Manufacturing

The design and operation of a manufacturing system needs numerous types of decision making at various levels of its activities. Therefore, IoT can be applied to develop modern manufacturing enterprises characterized by dynamic and distributed environments (Da Xu et al., 2014). In these environments, IoT technology can be used to serve a variety of purposes (Fantana et al., 2013; Tao et al., 2014; Bi et al., 2014): from environment control, lighting control, and safety, to production optimization, error detection and correction, and automatic control of stocks.

1.5.7 Smart Agriculture

Modern agriculture has a different set of requirements than traditional agriculture. It must be high yield, high quality, efficient, safe, and ecological (Shifeng et al., 2011). IoT technology has contributed to agriculture modernization and improvement (Shifeng et al., 2011; Bo and Wang, 2011). WSNs, for example, have been successfully deployed for irrigation control, fertilization, pest control, and animal monitoring, as well as for greenhouse monitoring, viticulture, and horticulture (Rehman et al., 2014; Zhang et al., 2018).

1.5.8 Environment/Smart Planet

IoT can be used to allow for the development and management of sustainable cities, covering issues like environmental monitoring (Fang et al., 2014), pollution control (Du et al., 2013; Fang et al., 2014), meteorological monitoring (Du et al., 2013), disaster monitoring, or waste management (Hong et al., 2014).

IoT technology can be used to tackle rapid urbanization and related environmental problems, allowing us to study the environment, planning, and construction issues, in order to increase understanding of how to integrate urban development and ecological processes for sustainable city construction.

1.6 CHALLENGES

Currently, IoT is one of the main accelerators of technological innovation, being one of the areas with greater potential of the transformation of society and the economy. As such, all the involved stakeholders, ranging from technologists to developers, companies, and users, face several challenges that remain to be tackled. Experience from areas such as distributed systems, networks, mobile and ubiquitous computing, context awareness, and WSN could be considered a good starting point for seeking appropriate solutions for issues such as interoperability, openness, security, scalability, and failure handling in the scope of the IoT systems.

TABLE 1.4
Overview of IoT Challenges

Challenges	References
Heterogeneity and interoperability	Ortiz et al. (2014), Serbanati et al. (2011), Al-Fuqaha et al. (2015), Rose et al. (2015), Borgia (2014), Miorandi et al. (2012), Atzori et al. (2010), Alur et al. (2016)
Openness	Perera et al. (2014), Alur et al. (2016)
Security, privacy, and trust	Perera et al. (2014), Serbanati et al. (2011), Ortiz et al. (2014), Al-Fuqaha et al. (2015), Borgia (2014), Rose et al. (2015), Miorandi et al. (2012), Whitmore et al. (2014), Atzori et al. (2010), Taivalsaari and Mikkonen (2017), Alur et al. (2016)
Scalability	Alur et al. (2016), Al-Fuqaha et al. (2015), Borgia (2014), Miorandi et al. (2012)
Failure handling	Alur et al. (2016), Ortiz et al. (2014), Taivalsaari and Mikkonen (2017), and Miorandi et al. (2012)

Based on a nonexhaustive literature survey, a set of challenges is shortly discussed in the next sections. Researched publications were grouped into the five previously mentioned categories, as shown in Table 1.4.

1.6.1 Interoperability

Heterogeneity has been a great challenge in distributed systems, as a variety of networks, hardware, different operating systems, and programming languages started to coexist within the same system. IoT systems of the future will be composed of humans, machines, things, and groups of them. To accomplish the functioning of such a network, seamless communication and cooperation among all the components is crucial (Ortiz et al., 2014). Developers and programmers also need to be prepared to cope with multidevice, always-on, highly dynamic, and distributed systems and adapt and update their programming skills to this new paradigm (Taivalsaari and Mikkonen, 2017).

Even though there are other challenges for the IoT, interoperability remains one of the most challenging goals for IoT systems, unless an RA and a set of standards are developed (Atzori et al., 2010; Rose et al., 2015; Serbanati et al., 2011). There has been an effort by the ISO/IEC to create an RA, IoT RA, which is currently under development. This architecture gathers consensus from several organizations (Yoo, 2015).

Furthermore, to interoperate, IoT components must be identifiable and discoverable by other components (Atzori et al., 2010; Borgia, 2014; Miorandi et al., 2012; Ortiz et al., 2014; Serbanati et al., 2011), as discussed in Section 1.1. After the discovery and identification process, components must be able to somehow communicate (Al-Fuqaha et al., 2015; Alur et al., 2016; Borgia, 2014; Miorandi et al., 2012; Ortiz et al., 2014). Section 1.2 gave an overview of the communication protocols and patterns that are currently being used and developed. It is imperative that in the near future, existing and new wireless technologies, such as NB-IoT, LoRaWAN, and Sigfox, be thoroughly tested and further developed, to achieve steps in the direction of having standards for connectivity among IoT devices.*

1.6.2 Openness

The openness of a system is the degree to which it can be extended and reimplemented in new ways. IoT systems must be prepared to share their data and resources with other systems in sometimes unpredictable ways (Alur et al., 2016; Perera et al., 2014). In order to make sustainable IoT systems,

* https://datafloq.com/read/7-trends-of-internet-of-things-in-2017/2530.

"openness must provide a correct balance between access to functionality, human interaction, and privacy and security" (Alur et al., 2016).

1.6.3 Security, Privacy, and Trust

In addition to the current already complex security and privacy landscape, IoT introduces considerably more data security and privacy issues. Often, IoT systems rely on wireless communications that intrinsically pose security problems. Additionally, the large amount of data generated raises new concerns not only about managing, processing, and analyzing such an amount of data, but also in how to ensure data confidentiality. IoT systems, especially those that collect sensitive data (e.g., healthcare systems), need to be secured at all layers, from the physical to the application layer (Perera et al., 2014; Rose et al., 2015). Existing IoT-enabled devices and deployed systems have been shown to be particularly vulnerable to denial of service attacks.* Only with adequate security and data protection mechanisms in place can the IoT systems expect to gain trust from the users (Ortiz et al., 2014; Rose et al., 2015). Security and privacy issues should be considered from the very beginning of the system design (Miorandi et al., 2012).

Caution is advised in the way data is processed, particularly taking care to keep it anonymous, until official data protection authorities make formal recommendations (Serbanati et al., 2011). In fact, this is an area of ongoing work and more research is needed to be able to overcome these issues. Many end-user companies and customers point to security as the main reason not to have embraced the IoT concept yet (ixia, 2016), while others find that data protection and privacy are the greatest barriers to the development of the IoT (Foster, 2017). An assessment of the extent to which existing data protection regulations fully address the IoT needs to be carried out, in order to establish what actions still need to be taken (Foster, 2017). The key legal issues that might delay the IoT also need to be discussed, as well as the ways that might help to overcome these issues. Recently, the EU published a revised version of the regulations and directives† regarding personal data processing, which becomes effective in 2018 in all member states.

Nevertheless, so far, some security frameworks have been proposed to provide confidentiality, integrity, and authentication (Serbanati et al., 2011). However, these frameworks add some communication and processing overhead to achieve their goal. Security requirements for IoT systems may be grouped into four sets (Borgia, 2014): secure authentication and authorization, secure configuration and data transmission, secure data storage, and secure access to data. For all these requirements, it is necessary to keep in mind that many IoT devices are low power and resource constrained. As such, some of the conventional techniques may not be adequate and new ones must be developed (e.g., lightweight cryptography).‡

1.6.4 Scalability

A scalable system continues to work effectively even when the amount of resources and the number of users are increased significantly. For the IoT, it is predicted that 20 billion devices will be connected to the Internet by 2020. Many of these devices will be mobile and will have low power and an unstable connection. As such, the current solutions may not be enough to guarantee proper functioning of the networks (Alur et al., 2016). At least two levels of scalability may be considered in the scope of IoT: network scalability and data scalability (Borgia, 2014). As the network of interconnected objects grows, interoperability must be guaranteed, as well as data security and privacy. Issues related to energy consumption also need to be tackled (Miorandi et al., 2012).

---

* https://datafloq.com/read/7-trends-of-internet-of-things-in-2017/2530.

† http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1493140462765&uri=CELEX:32016R0679.

‡ http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8114.pdf.

The volume and diversity of data that can and will potentially be generated by IoT is overwhelming (Cisco, 2014). Additionally, with so many different types of devices generating data, there are many reasons why this data may be stored in disparate data storage: there might be too much data to put in one place; transferring data into a database might consume too much processing power, so it is recommended that data is retrieved separately from the data generation process; devices might be geographically separated, and it is advisable to process data locally in order to obtain some processing optimization; there might be the need to separate raw data from data that represents an event; and finally, different kinds of data processing might be required. For these reasons, the data abstraction level must process many different things, which include integrating multiple data formats from different sources, for which purpose ensuring consistent semantics of data across various sources is of extreme relevance. Finally, confirming that data is complete to the higher-level application is also important (Cisco, 2014).

1.6.5 Failure Handling

Failure handling includes detecting, masking, and tolerating failures; recovering from failures; and redundancy. In such a complex, dynamic, and heterogeneous environment as IoT is expected to be, systems are required to be able to self-configure, self-diagnose, and autorepair (Alur et al., 2016). Gateways, as more resourceful components of the IoT systems, may be the right place to implement self-management fault, configuration, accounting, performance, and security (FCAPS) features (Al-Fuqaha et al., 2015).

Systems that successfully meet failure handling requirements are going to gain trust more rapidly among their users (Ortiz et al., 2014). However, this will make the task of the developers far more difficult, as they will have to find the right balance between application logic and error handling (Taivalsaari and Mikkonen, 2017).

1.7 CONCLUSION

By 2020, there will be more than 20 billion interconnected IoT devices, and its market size may reach $1.5 trillion (IDC, 2017). According to ETSI (Antipolis, 2016), each person is expected to have an average of four connected devices. Despite its growth, the IoT ecosystem is a complex market, with multiple layers and hundreds of players, including device vendors, communications and IT service providers, platform providers, and software vendors.

This chapter introduced the main topics on IoT, namely, definitions, RMs and RAs, enabling technologies, standards, main application domains, and challenges. As explained previously, international bodies, enterprises, academia, and industry are working together on a common definition and an RA for the IoT, as well as on standards that will enable interoperability among systems. Solutions to tackle other challenges, such as security and privacy, openness, scalability, and failure handling, are also being explored. Many are already on the table, and new ones are still emerging. It is expected that of around 300 IoT software platforms that are available on the market today, in the long term, only 5–7 of them will be consolidated (Skerrett, 2016).

As a network of devices that communicate autonomously, without human intervention, continuously connected to the Internet, the IoT has several social, individual, economic, and environmental implications. It is expected that IoT technologies will have a positive impact on several areas of society, as discussed in Section 1.5, where an overview of application areas was given. The development of smart cities, for example, in terms of infrastructure, transport, and buildings, has had a significant societal impact by improving the efficiency and sustainability of a whole range of urban services. IoT also plays a crucial role in I4.0, in which industrial sites are being transformed through intelligent, interconnected objects that may improve performance, lower costs, and increase reliability.

According to Tech Republic, artificial intelligence, augmented reality, virtual reality, healthcare IoT, Industrial IoT, and wearables are some of the currently emerging trends for the IoT

(Maddox, 2017). The potential of the area of IoT associated with these trends points toward a promising future. Soon, the results of the collaborative work that has been done by the different groups composed by industry, academia, and SDO representatives are expected to become evident.

REFERENCES

GPP. 2016. Standardization of NB-IOT completed. June 22. http://www.3gpp.org/news-events/3gpp-news/1785-nb_iot_complete.

Adolphs, P., H. Bedenbender, M. Ehlich, U. Epple, M. Hankel, R. Heidel, M. Hoffmeister, et al. 2015. Reference Architecture Model for Industrie 4.0 (RAMI 4.0). https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2016/januar/GMA_Status_Report__Reference_Archtitecture_Model_Industrie_4.0__RAMI_4.0_/GMA-Status-Report-RAMI-40-July-2015.pdf.

AIOTI (Alliance for the Internet of Things). 2015. Internet of things applications. https://aioti.eu/aioti-wg01-report-on-internet-of-things-applications/.

Al-Fuqaha, A., M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. 2015. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials* 17 (4): 2347–76. doi:10.1109/COMST.2015.2444095.

Alur, R., E. Berger, A. W. Drobnis, L. Fix, K. Fu, G. D. Hager, D. Lopresti, et al. 2016. Systems computing challenges in the Internet of things. ArXiv Preprint ArXiv:1604.02980. http://arxiv.org/abs/1604.02980.

Anagnostopoulos, T., D. Ferreira, A. Samodelkin, M. Ahmed, and V. Kostakos. 2016. Cyclist-aware traffic lights through distributed smartphone sensing. *Pervasive and Mobile Computing* 31 (C): 22–36. doi:10.1016/j.pmcj.2016.01.012.

Antipolis, S. 2016. ETSI IoT-M2M Workshop: Approaching a smarter world. November 25. http://www.etsi.org/index.php/news-events/news/1144-2016-11-news-etsi-iot-m2m-workshop-approaching-a-smarter-world.

Aqeel-ur-Rehman, A. Z. A., N. Islam, and Z. Ahmed Shaikh. 2014. A review of wireless sensors and networks' applications in agriculture. *Computer Standards and Interfaces* 36 (2): 263–270.

Ashton, K. 2009. That 'Internet of things' thing. *RFiD Journal* 22 (7): 97–114.

AT&T. 2017. Smart cities. Smart Cities—Internet of Things Newsroom|AT&T. Accessed January 13. http://about.att.com/sites/internet-of-things/smart_cities.

Atzori, L., A. Iera, and G. Morabito. 2010. The Internet of things: A survey. *Computer Networks* 54 (15): 2787–2805.

Bassi, A., M. Bauer, M. Fiedler, T. Kramp, R. Van Kranenburg, S. Lange, and S. Meissner. 2013. *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, 163–211. Berlin: Springer.

Bauer, M., N. Bui, J. De Loof, C. Magerkurth, A. Nettsträter, J. Stefa, and J. W. Walewski. 2013. IoT reference model. In *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*, edited by A. Bassi et al., 113–162. Berlin: Springer.

Bi, Z., L. Da Xu, and C. Wang. 2014. Internet of things for enterprise systems of modern manufacturing. *IEEE Transactions on Industrial Informatics* 10 (2): 1537–1546.

Bo, Y. and H. Wang. 2011. The application of cloud computing and the Internet of things in agriculture and forestry. In 2011 *International Joint Conference on Service Sciences (IJCSS)*, Taipei, Taiwan, 168–172.

Borgia, E. 2014. The Internet of things vision: Key features, applications and open issues. *Computer Communications* 54: 1–31.

Brad, S. and M. Murar. 2014. Smart buildings using IoT technologies. *Construction of Unique Buildings and Structures* 5 (20): 15–27.

Bui, N., A. P. Castellani, P. Casari, and M. Zorzi. 2012. The Internet of energy: A web-enabled smart grid system. *IEEE Network* 26 (4): 39–45.

Bui, N. and M. Zorzi. 2011. Health care applications: A solution based on the Internet of things. In *Proceedings of the 4th International Symposium on Applied Sciences in Biomedical and Communication Technologies*, Barcelona, 131.

Campolo, C., A. Iera, A. Molinaro, S. Yuri Paratore, and G. Ruggeri. 2012. SMeaRTCaR: An integrated smartphone-based platform to support traffic management applications. In 2012 *First International Workshop on Vehicular Traffic Management for Smart Cities (VTM)*, Dublin, 1–6.

Castro, M., A. J. Jara, and A. F.G. Skarmeta. 2013. Smart lighting solutions for smart cities. In 2013 *27th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Barcelona, 1374–1379.

Cisco. 2014. The Internet of things reference model. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf.

Commission of the European Communities. 2009. Internet of things—An action plan for Europe. COM (2009) 278 final. Brussels: European Union. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0278:FIN:EN:PDF.

Dahmen-Lhuissier, S. 2016. Internet of things. Valbonne, France: ETSI. Accessed October 18. http://www.etsi.org/technologies-clusters/technologies/internet-of-things.

Da Xu, L., W. He, and S. Li. 2014. Internet of things in industries: A survey. *IEEE Transactions on Industrial Informatics* 10 (4): 2233–2243.

Dohr, A., R. Modre-Osprian, M. Drobics, D. Hayn, and G. Schreier. 2010. The Internet of things for ambient assisted living. *ITNG* 10: 804–809.

Domingo, M. C. 2012. An overview of the Internet of things for people with disabilities. *Journal of Network and Computer Applications* 35 (2): 584–596.

Doukas, C. and I. Maglogiannis. 2012. Bringing IoT and cloud computing towards pervasive healthcare. In *2012 Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS)*, Palermo, Italy, 922–926.

Du, K., C. Mu, J. Deng, and F. Yuan. 2013. Study on atmospheric visibility variations and the impacts of meteorological parameters using high temporal resolution data: An application of environmental Internet of things in China. *International Journal of Sustainable Development & World Ecology* 20 (3): 238–247.

ETSI (European Telecommunications Standards Institute). 2016. SmartM2M; IoT standards landscape and future evolutions. ETSI TR 103 375 V1.1.1 (2016-10). http://www.etsi.org/deliver/etsi_tr/103300_103399/103375/01.01.01_60/tr_103375v010101p.pdf.

Fang, S., L. Da Xu, Y. Zhu, J. Ahati, H. Pei, J. Yan, and Z. Liu. 2014. An integrated system for regional environmental monitoring and management based on Internet of things. *IEEE Transactions on Industrial Informatics* 10 (2): 1596–1605.

Fantana, N., T. Riedel, J. Schlick, S. Ferber, J. Hupp, S. Miles, F. Michahelles, and S. Svensson. 2013. IoT Applications—Value Creation for Industry, 153. River Publishers Series in Communications. Aalborg, Denmark: River Publishers.

Foster, T. 2017. Regulation of the Internet of things. Accessed January 17. http://www.scl.org/site.aspx?i=ed47967.

Gartner, Inc. 2013. Gartener says the Internet of things installed base will grow to 26 billion units by 2020. December 12. http://www.gartner.com/newsroom/id/2636073.

Gershenfeld, N. 1999. *When Things Start to Think*. New York: Henry Holt and Co.

Gil-Castineira, F., E. Costa-Montenegro, F. J. Gonzalez-Castano, C. López-Bravo, T. Ojala, and R. Bose. 2011. Experiences inside the ubiquitous Oulu smart city. *Computer* 44 (6): 48–55.

GS1. 2016. GS1 and the Internet of things. Final. http://www.gs1.org/sites/default/files/images/standards/internet-of-things/gs1-and-the-internet-of-things-iot.pdf.

GSMA (GSM Association). 2016. Annual report 2016. http://www.gsma.com/aboutus/wp-content/uploads/2016/09/GSMA_AnnualReport_2016_FINAL.pdf.

Gubbi, J., R. Buyya, S. Marusic, and M. Palaniswami. 2013. Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems* 29 (7): 1645–1660.

Guinard, D. and V. Trifa. 2016. *Building the Web of Things*. Shelter Island, NY: Manning Publications.

Hong, I., S. Park, B. Lee, J. Lee, D. Jeong, and S. Park. 2014. IoT-based smart garbage system for efficient food waste management. *Scientific World Journal* 2014 (2014): 646953.

IDC. 2015. IDC predicts the emergence of 'the DX economy' in a critical period of widespread digital transformation and massive scale up of 3rd platform technologies in every industry. November 4. http://www.businesswire.com/news/home/20151104005180/en/IDC-Predicts-Emergence-DX-Economy-Critical-Period.

IDC. 2017. Internet of things ecosystem and trends. Accessed January 18. http://www.idc.com/getdoc.jsp?containerId=IDC_P24793.

IEEE (Institute of Electrical and Electronics Engineers). 2015. Towards a definition of the Internet of things (IoT). http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

i-SCOOP. 2015. Digital transformation: Online guide to digital transformation. February 1. http://www.i-scoop.eu/digital-transformation/.

ISO (International Organization for Standardization). 2017. ISO/IEC JTC 1—Information technology. Accessed January 15. http://www.iso.org/iso/home/standards_development/list_of_iso_technical_committees/jtc1_home.htm.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2014. Study report on IoT reference architectures/frameworks. https://www.itu.int/md/T13-SG17-150408-TD-PLEN-1688/_page.print.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission). 2016. Information technology—Data structure—Unique identification for the Internet of things. ISO/IEC 29161:2016. August. https://www.iso.org/obp/ui/#iso:std:iso-iec:29161:ed-1:v1:en.

ISO/IEC JTC1. 2015. Internet of things (IoT) preliminary report 2014. ISO/IEC. http://www.iso.org/iso/internet_of_things_report-jtc1.pdf.

ISO/IEC JTC1. 2016. Information technology—Internet of Things Reference Architecture (IoT RA). ISO/IEC CD 30141:20160910 (E). https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf.

Istepanian, R. S. H., S. Hu, N. Y. Philip, and A. Sungoor. 2011. The potential of Internet of M-health things 'm-IoT' for non-invasive glucose level sensing. In *2011 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, Boston, MA, 5264–5266.

ITU-T (International Telecommunications Union Telecommunication Standardization Sector). 2005. ITU Internet reports, the Internet of things. Geneva: ITU-T.

ITU-T (International Telecommunications Union Telecommunication Standardization Sector). 2012. Overview of the Internet of things. Y.2060. https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-Y.2060-201206-I!!PDF-E&type=items.

ixia. 2016. Key building blocks of Internet of things (IOT). https://www.ixiacom.com/resources/key-building-blocks-internet-things-iot.

Ji, S. W., H. Yun Teng, and J. Feng Su. 2014. The application and development of the Internet of things in intelligent buildings. *Advanced Materials Research* 834: 1854–1857.

Karzel, D., H. Marginean, and T-S. Tran. 2016. A reference architecture for the Internet of things. January 29. https://www.infoq.com/articles/internet-of-things-reference-architecture.

Kelly, S. D. T., N. Kumar Suryadevara, and S. Chandra Mukhopadhyay. 2013. Towards the implementation of IoT for environmental condition monitoring in homes. *IEEE Sensors Journal* 13 (10): 3846–3853.

Kyriazis, D., T. Varvarigou, D. White, A. Rossi, and J. Cooper. 2013. Sustainable smart city IoT applications: Heat and electricity management & eco-conscious cruise control for public transportation. In *2013 IEEE 14th International Symposium and Workshops on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Madrid, 1–5.

Li, L., H. Xiaoguang, C. Ke, and H. Ketai. 2011. The applications of Wifi-based wireless sensor network in Internet of things and smart grid. In 2011 *6th IEEE Conference on Industrial Electronics and Applications*, Beijing, 789–793.

Li, X., R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin. 2011. Smart community: An Internet of things application. *IEEE Communications Magazine* 49 (11): 68–75.

Li, X. 2013. Multi-day and multi-stay travel planning using geo-tagged photos. In *Proceedings of the Second ACM SIGSPATIAL International Workshop on Crowdsourced and Volunteered Geographic Information* (GEOCROWD '13), Orlando, FL, 1–8.

Li, Z., T. Wang, Z. Gong, and N. Li. 2013. Forewarning technology and application for monitoring low temperature disaster in solar greenhouses based on Internet of things. *Transactions of the Chinese Society of Agricultural Engineering* 29 (4): 229–236.

Liu, X., M. D. Ceorner, and P. Shenoy. 2006. Ferret: RFID localization for pervasive multimedia. In *UbiComp 2006: Ubiquitous Computing*, Orange County, CA, 422–440.

Maddox, T. 2017. 9 IoT Global Trends for 2017. *TechRepublic*. January 2. http://www.techrepublic.com/article/9-iot-global-trends-for-2017/.

Minoli, D. 2013. *Building the Internet of things with IPv6 and MIPv6: The Evolving World of M2M Communications*. Hoboken, NJ: Wiley.

Miorandi, D., S. Sicari, F. De Pellegrini, and I. Chlamtac. 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks* 10 (7): 1497–1516.

Moreno, M. V., M. A. Zamora, and A. F. Skarmeta. 2014. User-centric smart buildings for energy sustainable smart cities. *Transactions on Emerging Telecommunications Technologies* 25 (1): 41–55.

Opensensors. 2017. How to choose the best connectivity network for your project. Accessed January 15. https://publisher.opensensors.io/connectivity.

Ortiz, A. M., D. Hussein, S. Park, S. N. Han, and N. Crespi. 2014. The cluster between Internet of things and social networks: Review and research challenges. *IEEE Internet of Things Journal* 1 (3): 206–215.

Ou, Q., Y. Zhen, X. Li, Y. Zhang, and L. Zeng. 2012. Application of Internet of things in smart grid power transmission. In 2012 *Third FTRA International Conference on Mobile, Ubiquitous, and Intelligent Computing (MUSIC)*, Vancouver, BC, 96–100.

Pang, Z. 2013. Technologies and architectures of the Internet-of-Things (IoT) for health and well-being. Doctoral thesis, KTH, School of Information and Communication Technology (ICT), Electronic Systems, Kista, Sweden.

Perera, C., A. Zaslavsky, P. Christen, and D. Georgakopoulos. 2014. Context aware computing for the Internet of things: A survey. *IEEE Communications Surveys and Tutorials* 16 (1): 414–454.

Phithakkitnukoon, S., M. I. Wolf, D. Offenhuber, D. Lee, A. Biderman, and C. Ratti. 2013. Tracking trash. *IEEE Pervasive Computing* 12 (2): 38–48.

Postscapes. 2017. IoT technology guidebook. IoT Technology|2017 Overview Guide on Protocols, Software, Hardware and Network Trends. Accessed January 13. https://www.postscapes.com//internet-of-things-technologies.

Rose, K., S. Eldridge, and L. Chapin. 2015. The Internet of things: An overview. Reston, VA: Internet Society. https://pdfs.semanticscholar.org/6d12/bda69e8fcbbf1e9a10471b54e57b15cb07f6.pdf.

Ryu, C-S. 2015. IoT-based intelligent for fire emergency response systems. *International Journal of Smart Home* 9 (3): 161–168.

Sanchez, L., J. Antonio Galache, V. Gutierrez, J. Manuel Hernandez, J. Bernat, A. Gluhak, and T. Garcia. 2011. Smartsantander: The meeting point between future Internet research and experimentation and the smart cities. In *Future Network and Mobile Summit (FutureNetw)*, 2011, Warsaw, 1–8.

Serbanati, A., C. Maria Medaglia, and U. Biader Ceipidor. 2011. *Building Blocks of the Internet of Things: State of the Art and Beyond*. Rijeka, Croatia: INTECH Open Access Publisher. http://cdn.intechweb.org/pdfs/17872.pdf.

Shifeng, Y., F. Chungui, H. Yuanyuan, and Z. Shiping. 2011. Application of IOT in agriculture. *Journal of Agricultural Mechanization Research* 7: 190–193.

Shrouf, F. and G. Miragliotta. 2015. Energy management based on Internet of things: Practices and framework for adoption in production management. *Journal of Cleaner Production* 100: 235–246.

Skerrett, I. 2016. IoT trends to watch in 2017. December 19. https://ianskerrett.wordpress.com/2016/12/19/iot-trends-to-watch-in-2017/.

Smartup Cities. 2017. Smart waste containers with ultrasonic fill-level sensors. SmartUp Cities Smart City IoT Solutions for the Future Cities. Accessed January 17. http://www.smartupcities.com/smart-waste-containers/.

Sundramoorthy, V., Q. Liu, G. Cooper, N. Linge, and J. Cooper. 2010. DEHEMS: A user-driven domestic energy monitoring seystem. In *Internet of Things (IOT)*, *2010*, Tokyo, 1–8.

Taivalsaari, A. and T. Mikkonen. 2017. A roadmap to the programmable world: Software challenges in the IoT era. *IEEE Software* 34 (1): 72–80.

Tao, F., Y. Zuo, L. Da Xu, and L. Zhang. 2014. IoT-based intelligent perception and access of manufacturing resource toward cloud manufacturing. *IEEE Transactions on Industrial Informatics* 10 (2): 1547–1557.

Tielert, T., M. Killat, H. Hartenstein, R. Luz, S. Hausberger, and T. Benz. 2010. The impact of traffic-light-to-vehicle communication on fuel consumption and emissions. In *Interenet of Things (IOT)*, *2010*, Tokyo, 1–8.

Vlacheas, P., R. Giaffreda, V. Stavroulaki, D. Kelaidonis, V. Foteinos, G. Poulios, P. Demestichas, A. Somov, A. Rahim Biswas, and K. Moessner. 2013. Enabling smart cities through a cognitive management framework for the Internet of Things. *IEEE Communications Magazine* 51 (6): 102–111.

Vodafone Group. 2016. Vodafone completes the world's first trial of standardised NB-IoT on a live commercial network. September 20. https://www.vodafone.com/content/index/what/technology-blog/nbiot-commercial.html#.

Wang, X., J. Song Dong, C. Chin, S. Ravipriya Hettiarachchi, and D. Zhang. 2004. Semantic space: An infrastructure for smart apaces. *IEEE Pervasive Computing* 3 (3): 32–39.

Wei, C. and Y. Li. 2011. Design of energy consumption monitoring and energy-saving management system of intelligent building based on the Internet of things. In *2011 International Conference on Electronics, Communications and Control (ICECC)*, Ningbo, China, 3650–3652.

Weiser, M. 1991. The computer for the 21st century. *Scientific American* 265 (3): 94–104.

Weyrich, M. and C. Ebert. 2016. Reference architectures for the Internet of things. *IEEE Software* 33 (1): 112–16.

Whitmore, A., A. Agarwal, and L. Da Xu. 2014. The Internet of things—A survey of topics and trends. *Information Systems Frontiers* 17 (2): 261–274.

Yang, G., L. Xie, M. Mäntysalo, X. Zhou, Z. Pang, L. Da Xu, S. Kao-Walter, Q. Chen, and L-R. Zheng. 2014. A health-IoT platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. *IEEE Transactions on Industrial Informatics* 10 (4): 2180–2191.

Yin, C. T., Z. Xiong, H. Chen, J. Yuan Wang, D. Cooper, and B. David. 2015. A literature survey on smart cities. *Science China Information Sciences* 58 (10): 1–18.

Yoo, S. 2015. ISO/IEC JTC1/WG 10 Working Group on Internet of Things. June 16. http://iot-week.eu/wp-content/uploads/2015/06/07-JTC-1-WG-10-Introduction.pdf.

Yun, M., and B. Yuxin. 2010. Research on the architecture and key technology of Internet of things (IoT) applied on smart grid. In *2010 International Conference on Advances in Energy Engineering (ICAEE)*, Beijing, 69–72.

Zakon, R. H. 2016. Hobbes' Internet Timeline 23. The Definitive ARPAnet & Internet History. https://www.zakon.org/robert/internet/timeline/#Growth.

Zanella, A., N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. 2014. Internet of things for smart cities. *IEEE Internet of Things Journal* 1 (1): 22–32.

Zhang, Y., B. Chen, and X. Lu. 2011. Intelligent monitoring system on refrigerator trucks based on the Internet of things. In *International Conference on Wireless Communications and Applications*, Sanya, China, 201–206.

Zhang, L., K. Ibibia, W. Dabipi, and L. Brown. 2018. Internet of Things Applications in Agriculture. In *Internet of Things A to Z*, edited by Q. F. Hassan. John Wiley and Sons Inc.

Zhengxia, W. and X. Laisheng. 2010. Modern logistics monitoring platform based on the Internet of things. In *2010 International Conference on Intelligent Computation Technology and Automation (ICICTA)*, Changsha, China, 2: 726–731.

Zhong, Y. and Y-T Dong. 2011. Application of the Internet of things to security automation system for intelligent buildings. *Internet of Things Technologies* 4: 041.

Zouganeli, E. and I. Einar Svinnset. 2009. Connected objects and the Internet of things—A paradigm shift. In *2009 International Conference on Photonics in Switching*, Pisa, 1–4.

2 Organizational Implementation and Management Challenges in the Internet of Things

Marta Vos

CONTENTS

2.1 INTRODUCTION

The Internet of Things (IoT) is becoming one of the most heavily researched and hyped computing concepts today. At the most basic level, the IoT concept describes how "things" can be connected to the Internet, and each other, giving them the potential to act without the mediation of humans. This connection allows for the creation of new and novel applications with interconnected devices, organizations, and users. Theoretically, any real or virtual thing could be included in the IoT, with the limits to what IoT networks can do being bounded only by the imagination of developers and users. In reality, however, there is no one seamless IoT in which devices communicate with each other and their users. Instead, almost all "IoT" networks exist within single organizations, or limited organizational collaborations, which could be considered to be "intranets of things" (Santucci, 2010). These siloed networks and the devices they include are capable of connecting to both the Internet and each other, as well as other organizational IoT networks, but currently only connect within their silos to the Internet. Thus, these individual networks powered by radio-frequency identification (RFID), wireless sensors, or mobile technology are IoT capable, but not actually networked together. It can therefore be seen that the IoT is conceptual rather than being current reality. This is recognized in the term *Future Internet of Things* (FIoT) (Tsai et al., 2014), which acknowledges the gap between the IoT concept and reality, and looks to integrate today's intranets of things to form one IoT (Zorzi et al., 2010).

While IoT systems still exist in silos or intranets, the organizational implications of joining up these systems, within or between organizations, are not as well explored as the technical aspects of IoT systems operation. From 2010 to 2015, a sample of research literature across three commonly used databases yielded more than 8000 publications in the IoT field. Of these, the majority were concerned with technology-related questions, such as solving problems with networks, wireless technologies (e.g., RFID, wireless sensor network [WSN], and wireless body area network [WBAN]), the cloud, and security issues. Publications with respect to the management of IoT systems were relatively lacking, as was qualitative or social research (Vos, 2016). The fragmentary research, the disparate nature of IoT devices, and the complexity and size of the networks they form mean that many organizations, researchers, and users do not grasp its full potential or scale.

The IoT will likely reach into all corners of our existence, from home security systems to organizational supply chains and healthcare. Users often perceive their devices to be connected to the Internet, and therefore the IoT, but many technological, organizational, and social issues lie behind this apparent integration. Organizations themselves often do not consider issues beyond the boundaries of their own IoT implementations, and are unsure about how to deal with challenges that arise when they attempt to join with other organizational IoT networks (Vos, 2014). Because of the scale of the IoT, it is not possible to present an overview of its technology, organizational, and social issues in a single chapter. This chapter therefore focuses on the issues faced by organizations considering integrating their own IoT systems (or intranets of things) into the wider IoT environment. The term *organizations* is used broadly in this chapter to apply to the full range of organizational types and sizes. The issues discussed here would also apply in the home environment to individuals who wanted to participate more fully in the IoT experience, but the literature in this field is sparse, so IoT in the home environment is not considered in detail. Initially, the chapter discusses the IoT in an organizational context, and then the need for integration and technology standards is discussed. Following this, the chapter considers the application and adoption of the IoT in organizations. Challenges specific to the organizational management of IoT systems are then considered, including privacy, security, data management, trust, legislation, and governance. The chapter concludes with an overview of how the building blocks of the IoT might be integrated into one uniform network and a discussion of the current state of IoT research, with some suggestions for future research.

2.2 IoT IN ORGANIZATIONS

While there is an enormous amount of research dedicated to developing new technologies, and solving issues related to the IoT, organizational and social research has somewhat lagged (Vos, 2016). Partly, this is due to the difficulty of studying IoT systems, as huge distributed systems make it difficult and time-consuming for research to be undertaken, and the methods for studying such systems are not well developed (Vos, 2014). Most organizational research with respect to IoT systems deals with RFID technology, as this technology formed the initial basis of IoT implementations, while applications research and case studies focus on the most common applications, particularly in the smart city, healthcare, defense, and supply chain sectors. Potential uses for IoT systems are limited only by the imagination, but recorded implementations range from animal tracking (Vlad et al., 2012) to preventing cheating in Mahjong (Tang, 2013). One of the most heavily studied areas of IoT and WSN implementation is the healthcare sector. Healthcare organizations have been found to benefit from IoT technology in a number of ways, ranging from inventory management and time savings (Wamba and Ngai, 2011) through to improvements in healthcare practices as basic as handwashing (Shi et al., 2012).

The IoT market is predicted to continue growing, possibly reaching a potential value of $11 trillion per year by 2025 (Manyika et al., n.d.). A number of factors are driving this growth, including the reduction in costs for tags and sensors, increasing efforts in standardization assisting with the interoperability of systems, improving IoT infrastructure, and competitive pressures (Wyld, 2005). However, there are also inhibitors to adoption. Ongoing difficulties with privacy, security,

and standardization (Hossain and Quaddus, 2011) are hindering systems adoption, as are problems with cost, benefits realization, and technology complexity (Bose et al., 2009; Hossain and Quaddus, 2011; Ilie-Zudor et al., 2011). From the management side, trust between organizations (Spekman and Sweeney, 2006), accountability issues (Ilie-Zudor et al., 2011), organizational readiness (Hossain and Quaddus, 2011), training (Kopalchick and Monk, 2005), satisfaction with current technology solutions (Kros et al., 2011), change resistance (Carr et al., 2010), organizational size (Matta et al., 2012), and health concerns (Curtin et al., 2007) are inhibiting the adoption of IoT technologies.

The adoption and implementation of IoT systems has received some research interest, as well as the barriers to implementation and adoption, along with research based on specific applications of IoT technology. From an organizational management perspective, the amount of knowledge an organization has about the technology, along with the presence of a knowledgeable technology champion, is a predictor of IoT adoption (C.-P. Lee and Shim, 2007). Similarly, in systems shared between public and private sectors, the amount of knowledge an organization has about technology systems is important in the management of such systems, along with the expected mediators of privacy, security, cost, data management, and benefits realization (Vos et al., 2012). The extent to which organizations are transformed by systems adoption can be predicted to some extent by the benefit derived from such systems (Wamba and Chatfield, 2010). However, the degree to which organizations achieve the benefits they thought they would from their IoT implementations has also been questioned, with benefits derived not always being those expected (Vos et al., 2012). Technology reliability, placement, and data management and interpretation also continue to be ongoing challenges in systems design and implementation (Bardaki et al., 2012).

2.3 MANAGING IoT SYSTEMS

Many of the technical issues faced with implementing and operating an IoT system are also mirrored within the management of these systems. While the technical side of interoperability, privacy, and security management, for example, is subject to ongoing technical research, the organizational issues with respect to these topics are less discussed, but not less complex. Between organizations, seven closely related issues are highlighted from a business perspective as being essential to the organizational integration of IoT systems: interoperability, standards, privacy, security, trust, data management, and legislation and governance (Vos, 2014). Privacy and security are often considered to be elements of trust, as they contribute to ensuring that the members of the trusted relationship understand exactly how they should act, and how the other partners will act (Rousseau et al., 1998). In other instances, they can be considered separately, where issues of trust might not arise, for example, where security is compromised by a malicious attack. For ease of discussion, each of these will be considered separately, with organizational and technology perspectives.

2.3.1 Interoperability

There are many technical and organizational considerations when implementing IoT-based systems, including reliability, scalability, heterogeneity, and data use, not to mention how technical solutions might be used to solve privacy or security problems. However, when considering the issue of how organizations might implement their IoT-based systems in such a way that they might join the IoT either immediately or in the future, issues around ensuring that systems can be integrated with other IoT systems rise to the fore.

The ever-increasing range of devices that can be connected to the IoT presents enormous challenges to IoT systems, as each different device must be able to connect with the IoT architecture, transmit its data, and be understood. Each system or even device may have a different hardware manufacturer, along with different circuits, data formats, legacy systems, and carrier demands (Vermesan et al., 2011). Even the selection of radio frequency for the transmission of data presents difficulties, with different countries having different frequency ranges available for the transmission

of IoT data, which cannot be readily changed (European Commission, 2013). A great deal of research effort, and expense, is being aimed at developing middleware and systems architectures to allow for integration and interoperability of IoT systems. Interoperability of IoT hardware and software allows for information to flow between different devices, networks, and IoT systems. This ability to share information between systems is a crucial component of a seamlessly integrated IoT, with standardization of infrastructure, data formats, and communications protocols being a cornerstone of interoperability (Kopalchick and Monk, 2005).

At the most basic level, there is still no agreement as to what interoperability actually means, and to what degree it is required (European Commission, 2013). For example, would it be enough for users to be happy with their devices being interoperable, and thus unaware of any delay between their devices and the services they require, or does everything need to communicate with everything else? The benefits of IoT interoperability have yet to be fully explored, but apart from seamless communication, benefits could include such things as the ability for users and organizations to create unique combinations of devices and applications in "mashups."

2.3.2 Standards

Central to the effort to ensure interoperability in IoT systems is the issue of standardization. Standards allow devices to communicate with each other as the devices would all "speak the same language." They also allow new devices to be introduced to established IoT systems with the guarantee that those devices will work seamlessly. Standards are required across the full range of IoT architecture, from naming standards for device identification through to data standards ensuring that data can be processed and interpreted without difficulties in integrating different data formats.

Hardware naming standards are generally specific to the hardware type; for example, RFID standards apply to RFID tags, and WSN standards to WSN nodes. A number of standards exist for naming (numbering) RFID tags in a way that is unique and allows the tag to be identified. The IP for Smart Objects Alliance and the Ubiquitous ID Center (Zorzi et al., 2010) develop RFID naming standards, and proprietary naming schemes are developed by some organizations for their own RFID implementations. However, the most common and widely implemented RFID naming standards center on the Electronic Product Code (EPC). EPCglobal drives development of these identification standards, along with standards for RFID architecture and hardware, in an effort to allow seamless integration of RFID-enabled devices into RFID systems (EPCglobal, 2010). The EPC Information Service (EPCIS) is a permission-based service allowing information to be shared between applications, and between applications and users, through mapping RFID identification codes to the relevant information (Glover and Bhatt, 2006). These standards are RFID specific and do not include other IoT devices. Other IoT devices also have some naming standards, although these are not as well developed as those relating to RFID. Mobile devices are identified by their Media Access Control Identification (MAC-ID), the conventions for which are managed by the Institute of Electrical and Electronics Engineers (IEEE), while Sensor Web Enablement (SWE) standards identify sensors to the Internet.

A number of organizations, including the Internet Engineering Task Force (IETF) and IEEE, are developing standards with respect to how the various IoT devices communicate with the Internet, including Internet protocol version 6 (IPv6) and the Constrained Application Protocol (CoAP). For devices with low power resources, the IETF is promoting the 6LoWPAN standard. Other communications standards, particularly for WSN, include those developed by the IEEE, ZigBee, and WirelessHART. At the architecture level GS1, the IEEE, the European Union (EU), and the Internet of Things Architecture (IoT-A) Project, among others, are working toward a standardized architectural model for the IoT (Bertot and Choi, 2013). There are few data standards that have been developed particularly for the IoT, and as the number of connected devices increases, the need for an ontology-based semantic standard is becoming more urgent to ensure that data can be exchanged effectively between different devices (Vermesan et al., 2011).

Standards are the driving force behind IoT interoperability, ensuring that devices can connect with each other, if necessary, and allowing users to achieve the seamless IoT experience promised (Bertot and Choi, 2013). However, caution needs to be exercised to ensure that any standards developed do not constrain innovation by forcing a particular standard architecture, communications protocol, or hardware on the IoT, a situation that would inhibit innovation and growth.

2.3.3 Privacy

Privacy in the IoT context is difficult to define. Separate from the need to secure IoT infrastructure, privacy refers to the need to ensure that data relating to individuals remains confidential. IoT systems gather a great deal of data, and at times are invisible to individuals who may not even be aware they are carrying digitalized devices, or RFID tags. Data collected from these devices could be used to track movements or gather other information, without the knowledge of the owner. Similarly, data collected from WSN in the home environment could reveal a lot about the personal habits of the user, from his or her preferred air temperature to how many times he or she exercises (Peppet, 2014). Anonymization of data is difficult, and de-anonymizing is also possible, leading to ongoing concerns about how IoT databases are used and secured (Peppet, 2014). In the ubiquitous IoT environment, theoretically anything could reveal everything.

It is important to note that there are at least three types of information available from IoT systems:

1. Information relating to individual humans, which is considered *private*, especially when it is individually identifiable
2. Information relating to organizations, which is considered *confidential* and secured against unauthorized access
3. Information that is neither *private* nor *confidential*, but could be shared without causing individuals to be identified or businesses to be disadvantaged

Some of the data related to IoT-related systems can be shared; for example, sensor information related to weather conditions is commonly made public. However, the nature of data generated by IoT systems must be understood by organizations, and secured appropriately. The Organisation for Economic Co-operation and Development (OECD) updated its guidelines with respect to data transmitted across national borders in 2013, in part to take account of the increasing amounts of cross-border data transmission caused by the proliferation of IoT devices. In response, many OECD member states have implemented or updated legislation and privacy guidelines to ensure that cross-border data flows respect the need for the privacy and confidentiality of individuals and organizations, while still allowing for these data flows to continue (OECD, 2013). Further, jurisdictional issues are of concern in the IoT environment, as cloud servers are not always located in the country of origin of the data. Even where organizations share IoT systems, they may be spread across different countries with different privacy requirements. The European Commission on Internet of Things Governance recommends that organizations take a "privacy by design" approach to IoT systems, advising organizations to ensure that they consider privacy from the earliest development phase, and that the data collected, and its possible impact on people, is well understood (European Commission, 2013). The European Commission has also recommended that individuals have the capability to "be invisible" to IoT systems, something that is difficult to ensure with the increasing ubiquity of IoT technologies (Krotov, 2008). However, not all IoT systems require high levels of privacy protection. There is a substantial difference between data that could identify individuals and data that, for example, deals with the movement of inventory items (Vos, 2014). The EU and OECD regulations are concerned with data that can be identified to individuals, but much less concerned with organizational information.

The nature of IoT hardware also presents difficulties in ensuring both privacy and security. Passive tags by their nature are seldom secured, and the heterogeneity of devices connected to the

IoT makes one single privacy or security solution impossible (Miorandi et al., 2012). Solutions such as "kill tags," where tags are deactivated at the point of sale, have been proposed. But these solutions disable a number of the attractive features of IoT-based items, including product support and ease of item return (Ohkubo et al., 2005). Other possible solutions, such as physical shielding of tags, is only possible in limited applications, such as passports, where the individual can both identify the tag and take action to shield it. A range of technical solutions are being explored to assist in improving privacy in the IoT (Sicari et al., 2015), including tagging IoT data with privacy properties (Evans and Eyers, 2012), anonymous authentication protocols (Alcaide et al., 2013), encryption (Wang et al., 2014), and privacy protective Domain Name Systems (DNSs) that would recognize the user's identity (Wang and Wen, 2011), among other approaches.

Identity management is another area of research with respect to improving IoT privacy for individuals. Using an identity management approach, individuals could manage how they interact with various IoT devices. Such strategies could include the use of pseudonyms to obscure the identity of an individual, and in a theoretical future, individuals could entirely dictate how they interacted with computing devices (De Hert, 2008). For example, an individual could chose to suppress his or her identity when moving through a building, and any IoT devices he or she were carrying would not be identified to the owners of the building (Cas, 2005). This is the type of privacy-preserving technology recommended by the European Commission (2013).

2.3.4 Security

Without securing the IoT environment, privacy is not possible. The IoT environment presents many security challenges, including

- The heterogeneous nature of IoT devices
- The large attack surface offered by numerous IoT devices
- The fact that the simpler building blocks of the IoT, such as passive RFID tags, are not easily secured

Security solutions, such as the Trusted Platform Module (TPM), are expensive and thus limited to high-end devices, with the energy and processing power to accommodate such units. From the data protection point of view, the gold standard for data protection is the use of public key encryption, but as with TPM, the obvious drawback of encryption is the high cost involved, making it economic only in limited applications (Mykletun et al., 2006).

The most basic devices are generally secured through software-based methods that leave the devices themselves unprotected (Abera et al., 2016). Further, engineering of security into cheap consumer goods is seldom a priority for their manufacturers (Peppet, 2014). Thousands of identical modules sold to consumers, who seldom bother with updates or secure passwords, can all be attacked in exactly the same way, leading to the kind of Distributed Denial of Service (DDoS) attacks seen in recent years (Ackerman et al., 2012). With billions of online IoT devices predicted for 2020 (Nordrum, 2016) (although more generous predictions go as high as 1 trillion devices [Iwata, 2012]), the security of these devices is a major concern. Security protection for the IoT will need to consider the nature of the infrastructure, communications, and data, as well as align with social and legal expectations of privacy.

Security issues in the IoT environment have two perspectives. One is securing the IoT devices and infrastructure against attacks directed at the organization or owner; the other perspective is securing against unauthorized use of the device itself. In 2016, IoT-capable devices were used in a DDoS attack against the Dyn domain name servers, which shut down Twitter, Netflix, and Spotify, among other popular websites (Ingraham, 2016). The attack used the Mirai malware, which exploits a weakness in IoT-capable devices where factory default passwords are not reset by the users, and could not have been reset in many cases because the passwords were hardwired into the devices. In this

particular case, DVRs and IP cameras were the primary devices affected (Walker, 2016). This is not the first time a large-scale attack of this type has been carried out. In 2013, more than 100,000 IoT devices were involved in a spam and phishing attack; the services were compromised in the same way as in the 2016 attack, through factory-set passwords not being reset (Proofprint, 2014).

Other types of attack are also possible; for example, home NEST thermostats can be hacked, using ransomware to demand that the thermostat be reset (Mayer, 2016). Researchers have demonstrated how simple it is to locate vulnerable IoT devices, with an October 6, 2016, Internet scan locating more than 515,000 nonsecured IoT devices (Wikholm, 2016).

The obvious vulnerability of IoT devices has led to the European Commission commencing the development of cybersecurity requirements for IoT devices, including those used in the October 2016 attack, as part of a general overhaul of EU telecommunications law (Stupp, 2016). Similarly, the U.S. Federal Trade Commission has released best practice security guidelines for IoT devices, and has prosecuted at least 50 companies for not having sufficiently secured networks or products (Mayer, 2016).

The heterogeneous nature of the IoT, as well as the complexity and lack of standardization of IoT architecture, makes securing infrastructure difficult. Security (and privacy) is frequently cited as an inhibitor of IoT adoption, and with recent highly publicized attacks, the need to secure IoT devices is becoming urgent.

2.3.5 Trust

Trust is a concept supported by a vast amount of literature in the psychological and business fields, but one that is not always considered in technology implementations. Two features are common within trust definitions: the first recognizes that a risk must be present that gives rise to the need for trust; the other is that the different parties must be interdependent or have cause to rely on each other (Rousseau et al., 1998). In technology systems, such as supply chains or the IoT, trust is seen to be an essential part of the infrastructure of systems where credentials are exchanged between infrastructure elements before services are provided (Mahinderjit-Singh and Li, 2010). The exchange of data also needs a level of trust, as organizations sharing information need to be reassured that the information will be used in appropriate ways (Eurich et al., 2010). Contracts between organizations play a role in mitigating this risk and ensuring a trusted relationship, as organizations can be sure of the behavior of their partners (Blomqvist et al., 2008). Similarly, the presence of regulations and legislation is considered one of the most effective ways of increasing trust, most likely related to the consequences of violating legislation (Luhmann, 1979). In some cases, the mitigation of risk through sufficient knowledge of partner organizations (Laeequddin et al., 2012) and consistent policies between organizations (Treglia and Park, 2009) is considered to be a possible replacement for a trusted relationship, which could then develop over time.

Trust can also emerge or be strengthened as a result of the successful implementation and use of technology systems, and where organizations have been involved in intense collaboration, it can emerge quite quickly (Blomqvist et al., 2008). However, in a ubiquitous technology environment, such as that of the IoT, trust is complicated by the large number of different participants and stakeholders, their differing needs and perspectives, and the speed with which the technology itself changes. Consumer trust is especially important in this type of environment, as consumers tend to distrust new technologies. The presence of consistent and strong privacy policies in particular has been found to assist with consumer acceptance of such technologies (Lee et al., 2007). The associated use of entity authentication and appropriate controls on access also assists users in trusting technology systems (Grandison and Sloman, 2000).

Between organizations, trust models are many and varied. Some include the characteristics of individuals, logical economic elements, and institutional trust, which includes regulation (Laeequddin et al., 2012). Other models consider trust elements, including the anticipation of certain responses, expectations of particular behaviors based on shared goals, and the knowledge

of consequences for noncompliance (Tejpal et al., 2013). Across national boundaries, different national policies, the number of agencies involved in collaborative efforts, and national culture (including attitudes toward technology) add extra challenges to trusted relationships (Navarrete et al., 2009).

When considering technology systems, security and privacy are often considered to be dimensions of trust. But the situation is more complicated than simply ensuring systems security or data privacy. The nature of trust is such that the technology itself must also be trusted. Users must trust that the technology will operate without interruption, that it will be available when wanted, and that it will not transmit incorrect or malicious data (Roman et al., 2013). Similarly, each element of the IoT network is built with the assumption (or trust) that needed components will be available when they are required, even if those components are owned by other organizations in other jurisdictions (Yan et al., 2014).

From the technological standpoint, we can also observe the necessity for trust in the IoT context. Each architectural layer relies on the other layers operating as expected, and these layers rely on the overall operation of the whole system (Yan et al., 2014). The extensive nature of IoT systems also raises challenges that may not be seen in less widespread technology systems. The nature of the IoT itself is to collect vast amounts of data; therefore, data collection trust needs to be considered. If data collected is not trustworthy, through either collection error, technical problems, or outside interference, then the integrity of the whole system is compromised. Similarly, the quality of the data collected reflects directly on the services that can be provided, with poor quality or inaccurate data producing poor-quality and nontrustworthy services. Users are also expected to disclose or share data through the IoT devices. If they do not trust IoT services, they will not want to disclose data (Yan et al., 2014).

Technology-based trust management has not been extensively studied in IoT systems, while the elements of trust, such as data handling and access rights (Sicari et al., 2015) privacy, security, data perception and transmission, quality of service, identity, and systems reliability (Yan et al., 2014), are generally considered separately from the technology basis of the IoT. However, some research has taken a broader approach considering trust management in the IoT. Recent work considers building trusted networks of devices where nodes and devices can rate each other, and also exchange information with respect to other devices in a recommendation-type system (Bao and Chen, 2012). A similar approach is taken in Social IoT (SIoT) systems where reputation-based trust systems can repel some types of attacks through denying entry to nontrusted nodes, with services and information being obtained only from trusted sources (Nitti et al., 2012). Each node or device can calculate how trustworthy its associates and other nodes are, based on the ratings of its "friends" and on its own experience, choosing the most trustworthy node to transact with, similar to a trust-based model proposed for peer-to-peer (P2P) networks (Sicari et al., 2015). Beyond such trust-based calculations, trusted communities of nodes and devices can be formed using P2P principles. Each node or device, and each community, has its own identity within the IoT network, and is trusted within the network according to its behavior. This forms a trust chain within the community with parameters such as past history, proximity, consistency, availability, common warrants and goals, place within the hierarchy, and fulfillment of requests considered. Figure 2.1 summarizes this process, illustrating how a device could come to be trusted based on its behavior within the IoT network.

Security is established by considering the nodes crossed when users access this network, while initial trust is established either by the user or, where there is no user, by the manufacturer or organization controlling the device (Lacuesta et al., 2012). These trusted chains can form communities with unique identities that allow members to access services. Such distributed trust-based models go some way toward answering concerns around the difficulties traditional access control models have in securing highly dynamic and decentralized IoT networks (Mahalle et al., 2013).

Fuzzy methods can also be used to calculate trust scores, which are used to control access through sets of permissions and credentials. This fuzzy trust-based access control (FTBAC) method

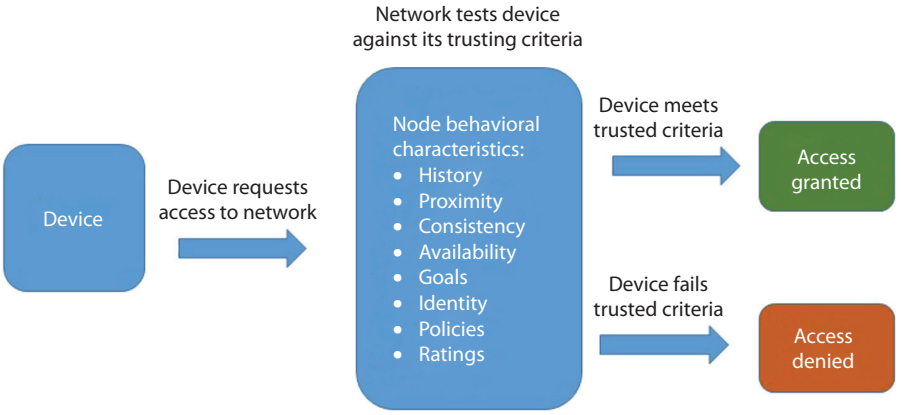

FIGURE 2.1 Demonstration of how devices come to be trusted in a trusted network.

considers three layers, a device (or sensor) layer, a request layer (which collects the trust values of knowledge, experience, and recommendations), and an access control layer. In such models, a device can access the IoT system only if its credentials meet preset policies related to the device's trust value (Wang et al., 2014). The FTBAC method has been shown to be scalable and flexible, as well as energy efficient (Bao and Chen, 2012; Mahalle et al., 2013). Other trust management mechanisms involve assessing the behavior of various nodes and calculating trust values based on prior behavior (Saied et al., 2013), and identity-based key negotiation in WSNs that recognizes suspicious nodes and reduces involvement with them (Liu et al., 2014).

Owner-defined policies are also used to verify nodes attempting to join the trusted network (Lize et al., 2014), and to control access to nonpublic information (Martinez-Julia and Skarmeta, 2013), although the lack of a common semantic language to verify differing policies still hinders this type of development. Other difficulties with policy-based management currently include determining how to manage negotiation between inconsistent and difficult-to-understand policies, and the presence of errors in security policies (Wu and Wang, 2011). Despite the difficulties with policy management, if it works correctly, it carries the advantage of allowing device owners to dictate how they interact with the IoT, and this type of trust management is preferred by the EU and similar regulatory bodies (European Union, 2009).

2.3.6 Data Management

As already discussed, IoT systems produce huge databases, up to zettabytes in size (Chen et al., 2015), which can be of considerable value to organizations (Thiesse et al., 2009). The heterogeneous nature of the data collected, along with its volume and complexity, presents challenges to effective IoT data usage (Zhou et al., 2016). NoSQL data query languages and cloud (or fog) storage are helping to reduce costs of managing big databases, and assisting in data utilization. Because of its volume, IoT data is inevitably stored in cloud databases, thus leading to problems with bandwidth, and delays in data processing and provision, or data latency (Botta et al., 2014). Fog computing (or edge computing) is an attempt to address these problems by storing data on local devices, thus removing the need for distributed data centers and improving speed of access, as well as allowing for greater mobility and real-time interaction (Marr, 2016).

From the management perspective, the ability to share information within and between organizations is enhanced by common data standards, as well as trusted networks and interoperable technical infrastructure (Yang and Pardo, 2011). Clear policies and regulations also aid data sharing within organizations or in systems where such polices were negotiated (Treglia and Park, 2009), while between jurisdictions with different regulatory structures or expectations, regulations can

hinder data sharing as organizations struggle to meet disparate regulatory requirements (Ilie-Zudor et al., 2011). Further, the impact of questions about data ownership and data storage in a cloud environment, where jurisdiction is not always clear, has not been well explored, and will only become an increasing problem as the amount of data generated by IoT systems continues to grow (Chow et al., 2009).

The quantities of data generated by IoT systems also give rise to concerns about "data tsunamis" (Breur, 2015) and information overload, although ongoing research and improvement in data management practices and middleware systems has seen these concerns diminish (McKnight, 2007; Sarma, 2004). However, despite the huge quantities of data generated, or perhaps because of them, many organizations are not making optimum use of their data (Vos, 2014). Organizations have been found to struggle with using data generated by IoT-type systems to inform business decisions (Alvarez, 2004), as well as having problems negotiating ownership of data assets shared between organizations (Smith, 2006).

The massive databases derived from IoT systems have led to concerns for possible privacy or confidentiality infringements. Data collected from location-aware devices, such as RFID tags, or Bluetooth-enabled smart devices carried by individuals could theoretically be used to track the device's owner. Further, data collected by IoT systems could be aggregated and used to identify individuals, while health-related data could be compromised, leading to concerns that individual privacy rights could be violated. Solutions to these problems rely on either forming trusted relationships, allowing individuals to control their own interactions with the IoT, or regulation of IoT interactions, ensuring that organizations act in an appropriate way.

2.3.7 Legislation and Governance

The interaction between technology and regulation, or government, has always been a difficult one. Most governments are reluctant to legislate on technology matters, arguing that legislation constrains innovation (European Commission, 2013), and preferring technology-agnostic regulation that does not require changes with every new advance (Santucci, 2010). Further, the pace and scale of technology change make passing legislation difficult, with most jurisdictions focusing on technology-neutral regulations.

The scale of the IoT, and the potentially sensitive nature of the data collected by IoT systems, has attracted attention from various regulating bodies. The EU in particular has implemented a variety of regulations, and issued guidance for organizations and member states with respect to the use and implementation of IoT systems, especially in cross-border systems (European Commission, 2013). Standards bodies such as the IEEE, International Organization for Standardization (ISO), and GS1 are also heavily involved in promoting the standardization of infrastructure and other IoT components.

The need for the standardization of infrastructure and communications protocols, the traffic of data across national boundaries, and the associated cloud-based databases will require some form of governance, even if it is just to make sure the entire IoT infrastructure can function. Further, the need to ensure individual privacy often is poorly balanced with the need of organizations to use data collected from IoT systems (Friedewald and Raabe, 2011). It is likely that the DDoS attacks of recent times will spur regulators to action, if the industry does not move toward self-regulation (Wong, 2016). Governance of IoT systems is seldom discussed in literature, but the necessity to address problems integrating disparate IoT systems owned by competing organizations, adhere to national regulation, ensure the privacy of individuals and confidentiality of business data, and secure IoT infrastructure against attack is likely to require a great deal of research and organizational resources. No one can predict the unintended benefits or consequences of the IoT, and responsibility for managing the system is unclear. A multistakeholder governance model is the most likely given the large number of interested parties. It is very unlikely that a single organization or governmental group will succeed in controlling the IoT.

2.4 BUILDING THE BLOCKS INTO THE IoT

As the use of RFID and WSN technologies has become more common, the emergence of a true IoT has become a possibility, with predictions of billions of devices connected to the Internet by 2020 (Nordrum, 2016). However, challenges still remain with the implementation, connectivity, and use of IoT technology. The majority of IoT systems sit within a closed ecosystem containing the organization, its application partners, and its users. Tags and sensors from other IoT systems can be detected and read by the organizations readers, but they cannot be identified. So, while it might be possible to network these systems together into one continuous IoT, this cannot be done yet. These are the siloed "intranets of things" discussed earlier (Zorzi et al., 2010). In order to implement an effective IoT, it is essential that the various IoT components can be identified and communicate with the network or each other, be they RFID, WSN, Bluetooth devices, or something else. As new devices and protocols attempt to join the IoT, each must also be integrated and secured in some way. In order to seamlessly interact, an integrated communications protocol or a method of ensuring interoperability is required (Yoo, 2010). Connecting these IoT systems or "intranets" together presents many challenges apart from interoperability, including standards, data processing and management, privacy, security, trust, and governance, which have already been discussed.

Smart cities provide a test bed for IoT systems implementation on a larger scale. Cities such as New Songdo in Korea or the SmartSantander EU project allow for IoT systems to be explored and refined in real-world environments (Hernández-Muñoz et al., 2011). Smart city initiatives highlight the ways that daily life can be made easier through, for example, smart motorways and better use of public resources, as well as the issues and challenges facing smart environments (European Commission, 2015). Although smart city implementations offer many advantages, including more efficient management, better availability of information, improved transportation services, and opportunities to peruse creative ideas (Boulos and Al-Shorbaji, 2014), there are also challenges. Some of these might be expected in an IoT context, including heterogeneity, scalability, and integration (Hernández-Muñoz et al., 2011). Some solutions have been offered with respect to technical challenges, including the use of cognitive management frameworks based on virtual objects, which considers the value of IoT devices within the smart city, as well as how, why, and when to connect devices (Vlacheas et al., 2013). Other challenges focus more on the governance of the cities themselves, with questions being raised about the nature of agreements with technology providers, and whether those providers have too great a role in shaping the nature of the technology deployments, potentially causing technology lock-in (Greenfield, 2013). There is no doubt that FIoT research will focus on the issues presented by the smart city environments as researchers and technicians continue to address the problems of integrating siloed intranets of things into one cohesive IoT.

2.5 CONCLUSION

The heterogeneous nature of the IoT, as well as the enormous scale of IoT systems, means that grasping the full range of technologies and issues presented by the concept is challenging. This chapter has presented a high-level introduction to the issues faced in integrating today's organizational IoT systems into the wider IoT environment, from the more technical need to ensure the use of appropriate standards to streamline integration, through to privacy, security, trust, and legislative considerations. Despite the work presented here, there is still an ongoing need to consider how the increasing numbers of IoT-capable devices can be integrated into the IoT, and to find ways to unpick the complex social, organizational, and technical arrangements they bring.

In terms of the technology forming the basis of the IoT, which is not much discussed in this chapter, miniaturization (Vermesan et al., 2011), power supply (Atzori et al., 2010), the use of fog and cloud storage (Bonomi et al., 2012), and device self-management (Theodoridis et al., 2013) will continue to present research challenges. The role of the IoT in sustainability, recycling, and green