1

Introduction to the Internet of Things

Detlef Schoder

Department of Information Systems and Information Management, University of Cologne, Köln, Germany

1.1 Introduction

Early in 1926, Nikola Tesla envisioned a "connected world." He told *Colliers Magazine* in an interview (Kennedy, 1926):

> "When wireless is perfectly applied, the whole Earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole [. . .] and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket."

Kevin Ashton was the first to use the term Internet of Things (IoT) in 1999 (Ashton, 2009) in the context of supply chain management with radio frequency identification (RFID)-tagged or barcoded items (things) offering greater efficiency and accountability to businesses. As Ashton wrote in the *RFID Journal* (June 22, 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, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best."

In the same year, Gershenfeld (1999) published his work "When Things Start to Think," in which he envisioned the evolution of the World Wide Web as being a state in which "things start to use the Net so that people don't need to." ATMs could be considered as one of the first smart objects, which went online as early

Internet of Things A to Z: Technologies and Applications, First Edition. Edited by Qusay F. Hassan.
© 2018 by The Institute of Electrical and Electronics Engineers, Inc. Published 2018 by John Wiley & Sons, Inc.

as 1974. In addition, early examples of various prototype devices include vending machines in the 1980s performed by the Computer Science Department of Carnegie Mellon University. Since then, understanding of the possible breadth of IoT has become much more inclusive, comprising a wide range of application domains, including health care, utilities, transportation, and so on, as well as personal, home, and mobile application scenarios (Gubbi et al., 2013; Sundmaeker et al., 2010). More recently, the "Industrial Internet of Things" (IIoT) has further expanded the scope of IoT (see Section 1.2.2 and Chapter 11). With IoT, a world of networked, "intelligent," or "smart" objects (Ashton, 2009; Weiser, 1991; Weiser and Brown, 1996; Lyytinen and Yoo, 2002; Aggarwal et al., 2013; Gubbi et al., 2013; Mattern and Flörkemeier, 2010; Atzori et al., 2014; Chui et al., 2010) is envisioned. Recently, novel extensions of IoT have emerged, which include not only physical objects but also virtual objects[1] (which may blur the core concept of IoT that predominately focuses on physical things and objects). The common denominator of these varied conceptions of IoT is that "things" are expected to become active elements in business, information, and social processes.

If one recognizes the broad spectrum of application scenarios, the more general term "Net" would be more adequate than "Internet," since not all communication occurs via the Internet. Communication also does not exclusively occur between things/devices, but also between things and people. So, it would be more appropriate to use the terms the "Internet of Everything"[2] or "Net of Everything" instead of "Internet of Things."

As the most well-known visionary of the computerized and interlinked physical world, Mark Weiser asserts that a connected world of things is designed to help people with their activities in an unobtrusive manner. Interaction occurs with everyday—but computationally augmented—artifacts through natural interactions, our senses, and the spoken word (Weiser, 1991). In the course of miniaturization, the increasingly smaller technical components will be embedded into physical components, with as little intrusiveness for users as possible or without attracting attention at all. For example, miniaturized computers (or components thereof) and wearables with sensors are directly

1 Increasing numbers of physical objects/things are beginning to be seen in digital format or even only in digital format. Examples of this include books, maps, e-tickets of any sort, business cards, electronic purses, and so on. Consequently, not all "virtual objects" that are currently used are digital models of physical objects (pendants), but rather these objects "stand on their own" with no physical counterpart. Virtual objects can be defined as a digital element with a specific purpose, comprised of data and capable of performing actions (Espada et al., 2011).

2 The term "Internet of Everything" was coined by Cisco Systems and basically refers to applying the IoT model to everything, thus creating new capacities and smart processes in virtually every field. Cisco calls it the connection of "people, process, data and things." The Internet of Everything may be perceived as a variation or extension of IoT, subtly distinguishing itself by emphasizing the connection of people to things.

incorporated into pieces of clothing. In his essay in 1991, "The Computer for the 21st Century," Mark Weiser first expressed this vision while he was a Chief Technologist at the Xerox Palo Alto Research Center in the late 1980s (Weiser, 1991, 1993; Weiser and Brown, 1996; Weiser et al., 1999). Since then, this work ranks among the most cited academic papers in related academic disciplines that envision a connected world of everyday things. This vision and the related developments are referred to by Weiser as "Ubiquitous Computing" (also known as "Ubicomp"). Since its conceptual inception more than 25 years ago, many more related and modified concepts have emerged, including pervasive, nomadic, calm, invisible, universal, and sentinel computing, as well as ambient intelligence.[3] The Cluster of European Research Projects on the Internet of Things (CERP-IoT) blend together building blocks that derive from the aforementioned concepts and emphasize the symbiotic interaction of the real and physical with the digital and virtual world. From their perspective, physical objects have virtual counterparts representing them, which translate them into computable parts of the physical world. The CERP-IoT vision has recently become even more comprehensive by incorporating issues of Social Media, anticipating massive user interaction with things and linking to additional information regarding identity, status, location, or any other business, social, or privately relevant information (Chapter 1 of Uckelmann et al., 2011). Essentially, ITU (2005) defines IoT as a concept that allows people and things to be connected anytime, anyplace, with anything and anyone (and adding—according to CERP-IoT, 2009—ideally using any path/network and any service). Another line popularized by CISCO asserts a simple concept: The IoT is born when more things are connected via the Internet as human beings. As such, the advent of IoT may be dated around 2008/2009 (Evans, 2011) or 2011 (Gubbi et al., 2013). According to the lnternational Data Corporation (IDC)'s Worldwide Internet of Things Forecast, 2015–2020, 30 billion connected (autonomous) things are predicted to be part of the IoT by 2020. Another estimate anticipates approximately 1000 devices per person by 2025 (Sangiovanni-Vincentelli, 2014).

IoT is at the center of overlapping Internet-oriented (middleware), things-oriented (sensors), and semantic-oriented (knowledge) visions (Atzori et al., 2010). Specifically, (i) Internet-oriented, which emphasizes the networking paradigm and exploiting the established IP-based networking infrastructure, in order to achieve an efficient connection between devices, and on developing lightweight protocols in order to meet IoT specifics (see Section 1.5.2); (ii) things-oriented, which focuses on physical objects and on finding means that are able to identify and integrate them with the virtual (cyber) world; and

3 For a discussion on similarities and differences, see, for example, Aarts et al. (2001); for a summary of more than 20 years of the "Ubicomp" vision, see, for example, Cáceres and Friday (2012).

(iii) semantic-oriented, which aims to utilize semantic technologies, making sense of objects and their data to represent, store, interconnect, and manage the enormous amount of information provided by the increasing number of IoT objects (Atzori et al., 2010; Borgia, 2014).

As IoT continues to evolve, its comprehensive definition is also likely to develop.[4] Accordingly, the IEEE IoT initiative gives its community members an opportunity to contribute to the definition of the IoT (IEEE, 2015, 2017). The document presents two definitions, one for 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 second definition is for large-scale scenarios: "Internet of Things envisions a self-configuring, adaptive, complex network that interconnects 'Things' to the Internet through the utilization 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."

Incorporating various perspectives while revealing its nucleus, we may consolidate and define:

> IoT is a world of interconnected things which are capable of sensing, actuating and communicating among themselves and with the environment (i.e., smart things or smart objects) while providing the ability to share information and act in parts autonomously to real/physical world events and by triggering processes and creating services with or without direct human intervention.

We intentionally leave out whether this "big plot" will necessarily be realized on standard communication protocols or a unified framework. Although a unified framework would certainly be optimal, it may not be necessary or even achievable given the dimensionalities and complexities of a likely very highly heterogeneous computerized world of interconnected things.

In order to better structure the scale and scope of IoT, this chapter provides an introductory overview and briefly outlines the conceptual core ideas as laid out

4 A broad range of IoT definitions can be found in Minoli (2013).

prior to IoT with "Ubiquitous Computing." The chapter covers not only technical but also nontechnical issues of IoT.

1.2 Internet of Things Concepts

With technical advancements, our interaction with information systems is changing, both at work and during leisure time. Information, sensor, and network technology are becoming increasingly small, more powerful, and more frequently used. People no longer only encounter information technology at common points in their lives, such as in offices or at desks, but as information and communication infrastructures, which are present in increasing areas of everyday life. These infrastructures are characterized by the fact that they not only include classic devices, for example, PCs and mobile phones, but that information and communication technology is also embedded in objects and environments.

The Ubiquitous Computing vision of Mark Weiser implies that computers, as we currently know them, "disappear," or, more precisely, move into the background. Everyday objects and our immediate environment then assume the tasks and abilities of computers (Weiser and Brown, 1996). In his seminal paper, Weiser describes this as follows: "The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it" (Weiser, 1991). Through the physical embedding of IT, everyday objects and our everyday environment become "smart," that is, capable of processing and providing information, but not necessarily intelligent in the sense of human cognitive intelligence. In another highly regarded article, Weiser together with Brown introduced the notion of "Calm Computing." They also refer to a connected world full of computers. However, only in cases of service provision or when a need exists for interaction do those computers or their respective services become "visible"; at other times, those capabilities are "calm" in the background, and not intrusive or even visible to the users (Weiser and Brown, 1996).

The core concepts comprising IoT, as well as related concepts and models, will be presented in the following sections.

1.2.1 Core Concepts: Smart Objects and Smart Environments

A smart object is a physical object in which a processor, data storage system, sensor system, and network technology are embedded (Poslad, 2009; Kortuem et al., 2010; Sánchez López et al., 2011). Some smart objects can also affect their environment by means of actuators. In principle, all physical objects can be turned into smart objects, for example, conventional everyday objects such as pens,[5] wristwatches (there are numerous wristwatch models with sensors and

5 A well-known example of a computerized version of a pen is the Anoto Pen, see www.anoto.com.

processors, for example, to measure the heart rate or to determine geographic position), or automobiles (more recently, autonomous automobiles). In an industrial context, it could be a machine or the product to be manipulated. Smart objects may also be anywhere. In fact, there are almost no restrictions regarding domains: consumer electronic devices, home appliances, medical devices, cameras, and all sorts of sensors and data-generating devices. Most smart objects have a user interface and interaction capabilities to communicate with the environment or other devices (e.g., displays). The capability of smart objects to communicate with other objects and with their environment is a core component of IoT. In line with this is the idea that specific information can be retrieved via any networked smart object, which is uniquely identified and localized, and may have its "own home page," that is, unique address. Today, one can take advantage of a broad range of fairly inexpensive, tiny, and relatively powerful components, including sensors, actuators, and single board computers (SBC), to enrich physical things and connect them to the Internet. SBCs, such as Raspberry Pi, BeagleBone Black, and Intel Edison Open, as well as open-source electronics, such as Arduino, which entered the market between 2005 and 2008, catalyzed millions of new ideas and projects. Creating and collecting data about the status of physical objects may establish the basis for interesting home and office automation projects, education, and leisure activities with real-time visualizations of information generated from data "on the go" (Baras and Brito, 2017). Moreover, one can utilize the remote networks of intelligent devices deployed somewhere else.

Tightly coupled to "smart objects" is the concept of "smart environments." One definition emphasizes the physical extent to which smart objects are deployed and interacting. A compilation of smart objects within a given space, such as a closed space (automobile, house, room) or an outside area, for example, a district or an entire city (i.e., a smart city; see Chapter 12), turns a common environment into a smart one. Another definition asserts that sensors are the key factor in a smart environment. Essential for a smart environment is the context information gathered by sensors in order to provide adapted applications and services. Weiser et al. (1999) defined a smart environment as "the physical world that is richly and invisibly interwoven with sensors, actuators, displays, and computational elements, embedded seamlessly in the everyday objects of our lives, and connected through a continuous network."

1.2.2 Related Concepts: Machine-to-Machine Communications, Industrial Internet of Things, and Industry 4.0

IoT is not a construct that has appeared suddenly or without precursors. Technological forerunners and various conceptualizations exist prior to the relatively new "IoT" label, for example, machine-to-machine (M2M) communications. In addition, recent derivatives exist, for example, the Industrial

Internet of Things and Industry 4.0. The subsequent sections attempt to discern their similarities and differences, and how these concepts relate to each other.

1.2.2.1 Machine-to-Machine Communications

M2M communications refers to direct wired or wireless communication between devices using any communications channel that does not necessarily require direct human intervention (ETSI, 2010). As such, M2M can be viewed as the forerunner of IoT. M2M communication can include industrial production facilities, enabling a sensor or meter to communicate the data that it records (e.g., temperature, throughput, and inventory level) to application software that can further process them (e.g., adjusting an industrial process based on technical parameters, such as temperature or triggering new processes, such as placing orders to replenish inventory). Such communication was aimed at monitoring remote machines from which data were received, processed at some central station, and eventually relayed back to those machines with adjusted parameters, if necessary. A core motivation for many organizations is to reduce service management costs through remote diagnostics, remote troubleshooting, remote updates, and other remote capabilities that reduce the need to deploy field service personnel (Polsonetti, 2014). IoT accommodates the same devices/assets/machines as M2M applications, but also very small (low-power), personal, and inexpensive devices with sometimes very limited functionality that might not be able to justify a dedicated M2M hardware module. Although IoT and M2M communications have remote access to machines, or in more general terms "devices," in common, there are no other major similarities. For example, traditional M2M solutions typically rely on point-to-point communications using embedded hardware modules and dedicated protocols. In contrast, IoT solutions depend predominantly on IP-based networks to interface device data to a cloud or middleware platform primarily using common/open protocols (in order to ensure maximum interoperability, in the sense of a remote device connected to some central hub, as well as particular interoperability among the devices themselves). Another difference is that M2M solutions offer remote access to machine data that are traditionally targeted at point solutions in service management applications. In the past, these data are rarely, if ever, integrated with enterprise applications to help improve overall business performance. Finally, IoT-based data delivery increasingly involves cloud services enabling access by any sanctioned enterprise application, whereas M2M typically employs direct point-to-point communication. The cloud-based architecture also makes IoT inherently more scalable, eliminating the need for incremental hard-wired connections or SIM card installations. M2M is often referred to as "plumbing," while IoT is viewed as a universal enabler (Polsonetti, 2014). It could be argued that the conceptual boundaries and visions of IoT and M2M have become increasingly overlapping. Indications of this include that more recent M2M communications have evolved into a system of networks that transmits

data to personal appliances. In this sense, M2M communication is taking increasingly advantage of the expansion of IP networks globally by switching from point-to-point proprietary style connections to IP-based multipoint communications. We may conclude that the focus of M2M issues tends to be more on the technical infrastructure layer. In contrast, the emerging IoT possesses much greater scope. IoT calls for the integration of device and sensor data with business intelligence, analytics, and other enterprise applications in order to achieve numerous benefits throughout manufacturing enterprises with a strong emphasis on improving products, processes, and business models.

1.2.2.2 Industrial Internet and Industry 4.0

A broad segmentation of IoT comprises (i) a consumer-oriented perspective, including smart phones, connected automobiles, smart TVs, and wearables, and (ii) an industrial perspective. The latter includes, for example, power grids and power plants, transportation, wind turbines, and industrial equipment (Jeschke et al., 2016). The straightforward analogy is to translate objects within an industrial (production) context into smart objects. Production facilities, such as tools, conveyors, and even the products to be manipulated or built will become smart objects as conceptually defined here. In line with this perception, a "common factory" turns into a smart factory. It could be asserted that this may constitute the foundation for a fundamental new way of coordinating and producing goods. These expectations coalesce in labeling the upcoming era the "Fourth Industrial Revolution." Accordingly, the term Industrial Internet of Things or just Industrial Internet[6] is typically used. Moreover, in the context of IIoT, the term is often employed synonymously with Industry 4.0 or the original German term "Industrie 4.0,"[7] which is a label for various government initiatives in Germany (World Economic Forum, 2015). The differences between the terms or initiatives mainly concern stakeholders, geographical focus, and representation (Bledowski, 2015). IIoT also semantically describes a technological movement, while Industry 4.0 is more associated with expected economic impacts. The Industry 4.0 vision is anticipated to be realized by IIoT (Jeschke et al., 2016).

The proclaimed implications and benefits of IIoT are manifold and are rooted—as outlined in Section 1.6—in "derived qualities" from modern ICT, in particular context sensitivity, adaptability, proactivity, and increased data quality. Eventually, these derived qualities may help to achieve greater resource efficiency, shorter time-to-market, higher value products, and new services (Jeschke et al., 2016).

---

6 General Electric, which coined the term "Industrial Internet" as a holistic new application, joined with AT&T, Cisco, Intel, and IBM in 2014 to set up the Industrial Internet Consortium http://www.iiconsortium.org/.

7 The term "Industrie 4.0" is considered to have first been used at the Hannover Messe, Germany, in 2011.

1.3 Who Works on the Internet of Things?

A truly connected world in terms of IoT has not yet been fully achieved. However, a large number of organizations and alliances across industry, academia, and various levels of government are working on IoT and closely related streams, often in parts under different labels. This section compiles prominent national and international representatives from governmental bodies, academia, and industry (Rose et al., 2015; Gubbi et al., 2013; for standardizing, see Chapter 7 of this book). Supported by the European Commission 7th Framework program, a significant number of initiatives and projects have been funded, such as the Internet of Things Architecture (IoT-A) project and the Internet of Things-Initiative (IoT-i). The Internet of Things European Research Cluster (IERC), which coordinates ongoing activities in the area of IoT across Europe,[8] is a major organization in this area. The online companion website of the special issue on interoperability of IoT lists, among other collections, EU-funded projects started from January 1, 2016 and international IoT-projects.[9] The Alliance for Internet of Things Innovation (AIOTI) was launched by the European Commission to support the development of a European IoT ecosystem, including standardization policies.[10] Their working groups correspond to application areas of IoT, including smart living environments for aging well, smart farming and food safety, wearables, smart cities, smart mobility, smart water management, smart energy, and smart buildings and architecture. ETSI with its Connecting Things program is developing standards for data security, data management, data transport, and data processing related to potentially connecting billions of smart objects into a single communications network.[11] IEEE has a dedicated IoT initiative and clearinghouse of information for the technical community involved in research, implementation, application, and usage of IoT technologies.[12] The Internet Engineering Task Force (IETF) is the Internet's premier standards-setting body, and has an IoT directorate that coordinates related efforts across its working groups, reviews specifications for consistency, and monitors IoT-related activities in other standards groups.[13] As a major need exists for consensus around IoT technical issues, the Internet Protocol for Smart Objects (IPSO) Alliance was created. It has more than 60 member companies from leading technology communications and energy companies working together with standards bodies, such as IETF, IEEE, and ITU. China has prominently set IoT on its strategic agenda, including

8 http://www.internet-of-things-research.eu/.
9 https://www.computer.org/web/ computingnow/archive/interoperability-in-the-internet-of-things-december-2016-introduction?lf1=8161623904b709516091377b61283885.
10 https://ec.europa.eu/digital-agenda/en/alliance-internet-thingsinnovation-aioti.
11 http://www.etsi.org/technologies-clusters/clusters/connectingthings.
12 http://iot.ieee.org/.
13 https://trac.tools.ietf.org/area/int/trac/wiki/.

state-based and industry-funded initiatives (e.g., "Internet of Things Union Sensing China" in Wuxi). In addition, the Industrial Internet Consortium (IIC) works on an industrial grade IoT architectural framework and released a reference architecture for IoT in 2015.[14] In addition, literally all major national and supranational standardization bodies work on IoT issues, including ISO/IECJTC-1.[15] For example, the ITU has set up a "Study Group 20."[16] The Manufacturers Alliance for Productivity and Innovation (MAPI) is developing Industry 4.0 for industrial applications of IoT.[17] OASIS is developing open protocols to ensure interoperability for IoT, especially based on Message Queuing Telemetry Transport (MQTT) as its messaging protocol of choice for IoT.[18] The Online Trust Alliance, a group of security vendors, has developed a draft trust framework for IoT applications, focused on security, privacy, and sustainability.[19] The Open Management Group is a technical standards consortium that is developing several IoT standards, including Data Distribution Service (DDS) and Interaction Flow Modeling Language (IFML) along with dependability frameworks, threat modeling, and a unified component model for real-time and embedded systems.[20] At the same time, large-scale initiatives are underway in Japan, Korea, the United States, and Australia where industry, associated organizations, and government agencies are collaborating on various programs, such as smart city initiatives, smart grid programs incorporating smart metering technologies (in some European countries, smart metering has become legally mandated for new buildings), and the implementation of high-speed broadband infrastructures (e.g., in Germany).

1.4 Internet of Things Framework

The brief discussion in the following paragraph of technical, economic, and social issues reveals that IoT encompasses a wide area of topics and disciplines. Aimed at structuring the field, we propose the following four-layer "Internet of Things Framework" (Figure 1.1).

At the core, modern information and communication technologies form the technical foundation of IoT (covered in layer 1). IoT generates a network of unambiguously identifiable physical objects (things). Networking, and thus also the ability to communicate, does not only refer to human participants but also to the objects (or things) involved. These things are equipped with miniaturized

14 http://www.industrialinternetconsortium.org/.
15 http://www.iso.org/iso/internet_of_things_report-jtc1.pdf.
16 http://www.itu.int/en/ITU-T/studygroups/2013-2016/20/Pages/default.aspx.
17 https://www.mapi.net/research/publications/industrie-4-0-vsindustrial-internet.
18 https://www.oasis-open.org/committees/tc_cat.php?cat=iot.
19 https://otalliance.org/initiatives/internet-things.
20 http://www.omg.org/hottopics/iot-standards.htm.

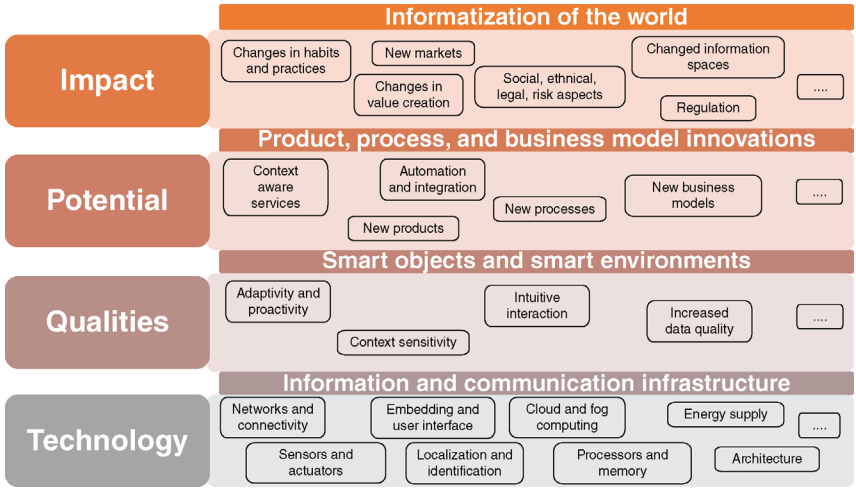

Figure 1.1 Internet of Things framework. (Adapted from Laudon et al., 2016.)

processors and actuators, for example, mechanical elements, temperature controllers, and audio or video output devices that can be utilized to control the objects and the environment. This allows for adapting objects and environments to our needs, interacting with the situation, and the provisioning of information and services according to specific situational requirements, that is, they become "smart objects" and "smart environments" (covered in layer 2). The automatic identification via RFID is often regarded as the basis for IoT. Sensors and actuators expand functionality by capturing states and the execution of actions or effects on reality.

This results in potential for new services, including consumer products as well as new business processes and business models (covered in layer 3). Products for consumers, for example, may hold and provide a large amount of information and can also offer customers with additional context-specific services during the post-sales phase. IoT also provides a higher level of data quality for business processes, enabling organizations to respond more rapidly and properly to events, and may contribute to improved efficiency, accuracy, and economic benefits (Sun et al., 2016). These potentials will lead to various product, process, and business model innovations. As these innovations affect our everyday lives, they have a wide impact on individuals, society, markets, and companies (covered in layer 4). On the one hand, companies are under pressure to adapt to changed value creation and market structures, as well as changing customer needs. On the other hand, innovative companies are given the opportunity to develop new products, processes, and business models that enable them to better meet the needs of their customers, and thus participate in the design of a computerized world. The effects are manifold and not always solely positive for everyone. Indeed, IoT poses severe challenges to companies, individuals, and

societies as a whole. Major challenges and issues include (i) security, privacy, interoperability, and standards (see Part 3); (ii) legal, regulatory, and rights; and (iii) emerging economies and social impacts, for example, some jobs will disappear, new jobs will emerge, more utilization of technology may lead to less human and manual interaction, different forms of social life may evolve, and so on (Sun et al., 2016; Rose et al., 2015; Vermesan et al., 2011; Miorandi et al., 2012; Conti et al., 2012).

1.5 Information and Communication Technology Infrastructure

The layer "Technology" describes the building blocks of an information and communication technology (ICT) infrastructure for the computerization of the (everyday) world. These building blocks include multiple software and hardware components, as well as highly developed and novel technologies. They are used to connect virtual information about or from things to the physical real world. These include technologies for computing, storage, embedding, and mobile and wireless networking, as well as sensors and actuators. Furthermore, improved methods for energy supply, identification, and localization constitute basic elements of IoT. Typically, in order to deal with the enormous resultant complexity, a layered approach is taken.

The next sections describe the building blocks of the technology layer, which are a foundational dimension of IoT.

1.5.1 Architecture and Reference Models

Especially for the technology layer, the extant literature covers a multitude of architectural proposals, reference models, and technical descriptions of the current or envisioned state of IoT.[21] Figure 1.2 presents a high-level view in terms of a three-layered stack of IoT-relevant technologies: (i) the thing or device layer, (ii) the connectivity layer, and (iii) the application layer. At the device layer, IoT-specific hardware such as sensors, actuators, memory, and processors are added to existing core hardware components, and embedded software is intended to manage and operate the functionality of the particular physical thing. At the connectivity layer, communication protocols enable communication between things and connected infrastructure, for example,

21 A vast literature exists on the architecture of IoT. Overviews (and alternative perceptions of such architectures) are provided, for example, Porter and Heppelmann (2015), Gubbi et al. (2013), Borgia (2014), Karzel et al. (2016), Wortmann and Flüchter (2015), and Weyrich and Ebert (2016). Edited multipaper volumes have several additional illustrations, for example, Vermesan and Friess (2016).

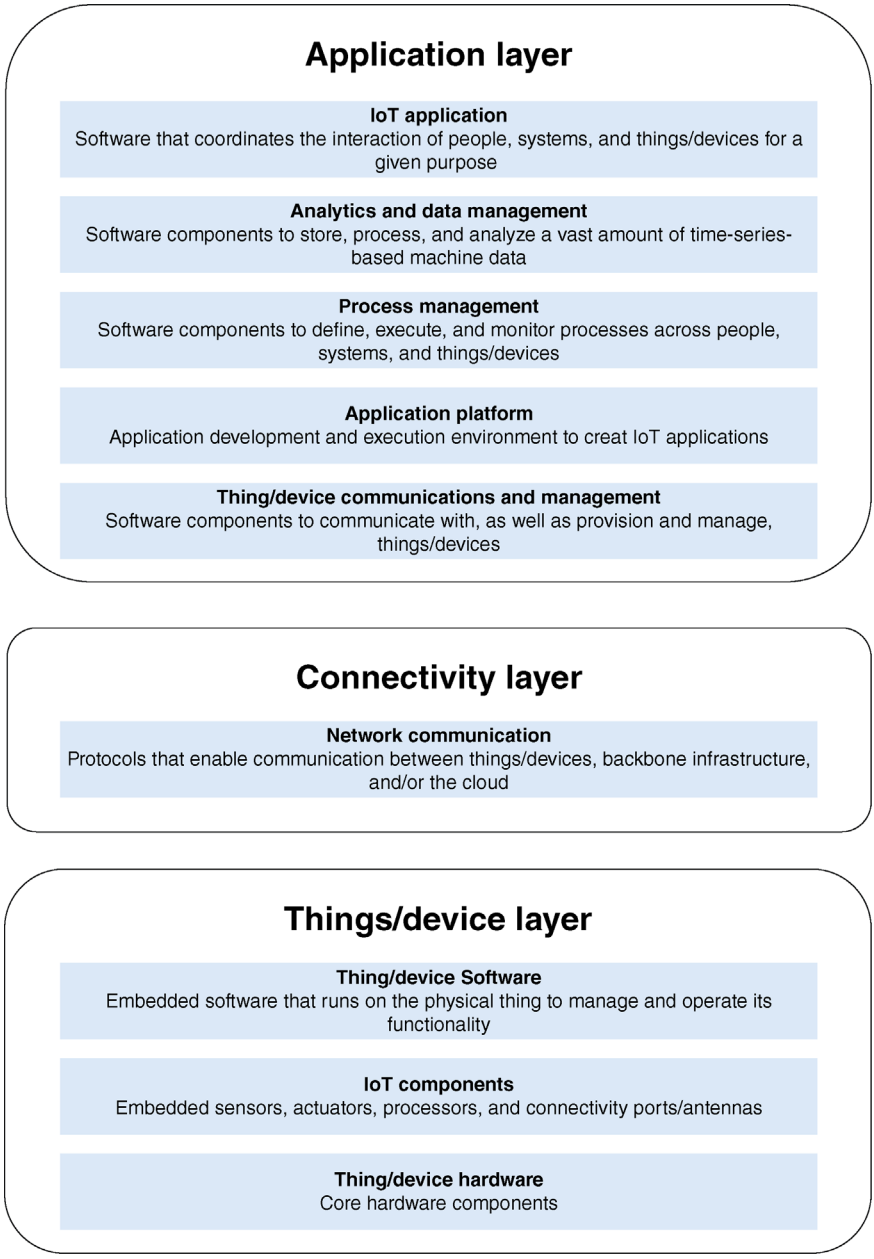

Figure 1.2 High-level view of an IoT architecture.

through cloud services. Accordingly, at the IoT application layer, device communication and related functionality is provided, while an application platform enables the development and execution of IoT applications. As more recent developments have proven, analytics and data management software are becoming increasingly critical to handle vast amounts of data, that is, store, process, and analyze the data generated by connected things. Moreover, process management software helps to define, execute, and monitor processes across people, systems, and things. Among the upper layers, IoT application software coordinates the interaction of people, systems, and things for a given purpose. Concerning all layers, software components manage identity and security aspects, as well as integration with business systems, for example, ERP or CRM, and with external information sources.

Table 1.1 lists prominent IoT reference architectures that are evolving in close collaboration between research and industry (see Part II). Recently, the IoT has received a boost from commercial engagement by large players throughout industries (Weyrich and Ebert, 2016): Google announced Brillo as an operating system for IoT devices in smart homes; more and more devices come equipped with M2M communications standards such as Bluetooth, ZigBee, and low-power Wi-FI; Microsoft has announced that Windows will support embedded systems and so on.

1.5.2 Networks and Connectivity

Network technologies connect objects that are equipped with information technology, and can be located in different locations. A large number of network technologies are available for this purpose, depending on the application. An application-related distinction feature is the scaling of the range. It ranges from global networks (satellites) over regional and local networks to so-called personal, body, and intrabody area networks. Personal area networks (PANs) can, for example, network via WLAN devices, typically in an area of up to 10 m^2 around one or two people.

In contrast to PCs, smartphones, and similar devices, loT devices are normally constrained regarding memory space, access to a continuous power supply, and processing capacity. Traditional protocols (in particular, the protocol stack TCP/IP) have not been designed with these requirements in mind. As a consequence, over the past years, many so-called lightweight communication protocols have been developed on virtually all layers of the protocol stack to create interoperability between IoT devices (Ahlgren et al., 2016). One approach to IoT interoperability is to consider the layered structure of the hardware/software stack (Fortino et al., 2016):

- The lower layers (according to the OSI model, the physical and data link layers; in the non-OSI context, sometimes labeled as the device layer) are aimed at seamlessly integrating new devices into the existing IoT ecosystem.

Table 1.1 Examples for IoT reference architectures.

Reference model	Founders	Latest release	IoT domain(s)	Viewpoints[a)]	Brief description
Internet of Things—Architecture (IoT-A)	NEC, CFR, ALBLF, SAP UniS, HEU, HSG, CEA, SIEMENS, ALUBE, FhG IML, and CATTID,	July 2012	Any	Functional and information	The "Internet of Things Architecture" (IoT-A) is an EU project. Based on a system requirement process, the outcomes cover a detailed architecture including the definition of a range of key components. It centers on a functional and an information perspective. http://www.meet-iot.eu/deliverables-IOTA/D1_3.pdf
Industrial Internet Reference Architecture (IIRA)	AT&T, Cisco, General Electric, IBM, and Intel	January 2017	Manufacturing	Business, usage, implementation, and functional	The IIRA is a standards-based architectural template and methodology. It is meant to enable Industrial Internet of Things system architects to design their own systems based on a common framework and concepts. http://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf
Reference Architecture Model Industrie 4.0 (RAMI 4.0)	The German Electrical and Electronic Manufacturers' Association, and its partners	July 2015	Manufacturing and Logistics	Business, functional, information, communication, integration, asset, lifecycle/value chain, and hierarchy	The RAMI 4.0 is a reference architecture taking into account particularities of Industrie 4.0/smart factories, which started in Germany and today is driven by all major companies and foundations in a large number of industry sectors. The RAMI 4.0 consists of a three-dimensional coordinate system that describes aspects of Industrie 4.0. www.zvei.org/en/association/specialist-divisions/automation/Pages/default.aspx
Cisco's Internet of Things Reference Model	Cisco	June 2014 (Draft)	Any	Any	The proposed IoT reference model is comprised of seven levels standardizing the concept and terminology surrounding IoT. From physical devices and controllers at level 1 to the collaboration and processes at level 7, the reference model sets out the functionalities required and concerns. http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf

a) A viewpoint is a set of conventions, templates, and patterns for creating a kind of view. It specifies the stakeholders whose interests are reflected in the viewpoint and the principles, guidelines, and template models to construct its views.

- The networking layer handles object mobility and information routing.
- The middleware layer facilitates seamless service discovery and management of smart objects.
- The application layer reuses heterogeneous application services from heterogeneous platforms.
- The data and semantics layer introduce common understandings of data and information.

The following are the prominent examples of standardized IP-based communication protocols for IoT devices: (i) on the application layer, IETF Constrained Application Protocol (CoAP)/REST engine and Message Queuing Telemetry Transport (MQTT); (ii) on the networking layer, IPv6 and RPL (and a derivative for low-power wireless personal area networks "6LoWPAN"); (iii) on the physical layer, IEEE 802.15.4 (Ahlgren et al., 2016). Examples for semantic oriented protocols include OPC UA (OPC Unified Architecture), UPnP (Universal Plug and Play), DPWS (Devices Profile for Web Services), CoAP (Constrained Application Protocol), and EXI (Efficient XML Interchange) (Weyrich and Ebert, 2016).

Interoperability has several dimensions. It is worth noting that even a high degree of standardization of protocols does not imply a high degree of standardization of data formats or device compatibility. In fact, interoperability is currently hampered by this condition. In an ideal situation, communication must be independent of the creator of a given fragment of the infrastructure. In reality, however, various players (including vendors) have their own IoT solutions that are more or less incompatible with other solutions, thus creating local "IoT silos" (Fortino et al., 2016). A large body of recent research into IoT is thus devoted to interoperability. The EU's Unify-IoT project may serve as an indication of this: They estimate more than 360 available IoT platform providers and determine that approximately 20 are somewhat popular. This indicates clearly that massive research efforts do not necessarily converge (Unify-IoT, 2016).[22]

For exchanging data between applications, devices, and objects, well-known communication standards exist, including Bluetooth, Wi-Fi,[23] and various mobile communication standards, such as GSM. Based on the use cases of

22 For various reports (deliverables) on IoT platform research of the EU-funded project Unify-IoT, refer to http://www.unify-iot.eu/.

23 Wi-Fi is a trademark of the Wi-Fi Alliance. It is a technology for wireless local area networking with devices based on the IEEE 802.11 standards. IEEE 802.11 is the radio frequency needed to transmit Wi-Fi. Devices that can use Wi-Fi technology include personal computers, video-game consoles, smartphones, digital cameras, tablet computers, digital audio players, and modern printers. Wi-Fi compatible devices can connect to the Internet via a WLAN network and a wireless access point, usually within a range of approximately 20 m indoors and a greater range outdoors.

mobile communications, major technological progress was achieved in terms of higher bandwidth (and accordingly, higher bit rates), multimedia streaming capabilities, and so on. However, as previously mentioned, most IoT use cases involve resource-constrained devices. Consequently, the goal of "Low Power, Wide Area Networks" (LPWAN) has become a core topic in IoT over the last few years. LPWAN is a broad term for a variety of technologies used to connect sensors and controllers to the Internet without the use of traditional Wi-Fi or cellular networks. At the same time, however, major players in cellular network industries are also further developing cellular-based networking standards, for example, LTE-M and NB-IoT. The latter is backed by leading manufacturers and by the world's 20 largest mobile operators. Further examples of activities forming new standards better suited for IoT use cases include LoRa and N-Wave, and Sigbox. The predominant design considerations are low energy consumption (up to more than 10 years of autonomy), strong penetration in indoor environments, and connecting a large number of sensors and devices with low bandwidth requirements. Table 1.2 summarizes selected communication protocols and standards currently under investigation or in use.[24]

1.5.3 Embedding

The anticipated omnipresence of a computerized world is, however, not to be implemented by setting up computers on the corners of every street. Instead, functionalities are embedded in objects and spaces. For example, conductive materials are woven into or printed on textiles. Objects are then computerized in this way, allowing us to immediately receive information about them and process them. The miniaturization of hardware is an essential prerequisite for the embedding of IT into objects. According to the still valid Moore's law,[25] miniaturization is accompanied by the improved performance of processors and increased storage capacities, with the cost of manufacturing the components remaining the same or even decreasing. These developments promote the general diffusion of information and communication technologies and allow them to be embedded in any, even small and short-lived, objects. This does not always concern increased performance, but can include other factors, for example, the energy efficiency of components. While embedding computers or components in physical things, novel challenges for the user interface often arise. For example, how does one communicate with "disappearing" computers? Displays, keyboards, and other commonly used input and output

24 Compilation taken from Baras and Brito (2017), with additions. Data sources are Postscapes (2017), Opensensors (2017), and ETSI (2016).

25 Whether and how long Moore's law may be still valid remains controversial (see several papers in *IEEE Spectrum*, 04/15).

Table 1.2 Overview of communication technologies and standards for IoT.

Name	Frequency	Range	Examples	Standards
Bluetooth BLE	2.4 GHz	1–100 m >100 m	Headsets, wearables, sports and fitness, health care, proximity, automotive	IEEE 802.15.1[a)] Bluetooth SIG [b)]
EnOcean	315 MHz, 868 MHz, 902 MHz	300 m outdoor, 30 m indoors	Monitoring and control systems, building automation, transportation, logistics	ISO/IEC 14543-3-10[c)]
GSM, LTE, LTE-M	Europe: 900 MHz and 1.8 GHz, USA: 1.9 GHz and 850 MHz		Mobile phones, asset tracking, smart meters, M2M	3GPP[d)]
6LoWPAN	2.4 GHz	10–30 m	Automation and entertainment applications in home, office, and factory environments	Adaption layer for Ipv6 over IEEE802.15.4[e)]
LoRa	Sub 1 GHz ISM band	2–5 km urban; 15 km suburban; 45 km rural	Smart city, long-range M2M	LoRaWAN[f)]
NB-IoT (narrow-band-IoT)	700–900 MHz	10–15 km rural deep indoor penetration	Smart meters, event detectors, smart cities, smart homes, industrial monitoring	3GPP LTE Release 13[g)]
NFC	13.56 MHz	Under 0.2 m	Smart wallets, smart cards, action tags, access control	ISO/IEC 18092[h)] ISO/IEC 14443-2,-3,-4[i)]
NWave	Sub 1 GHz ISM band	Up to 10 km	Agriculture, smart cities, smart meters, logistics, environmental	Weightless[j)]
RFID	120–150 kHz (LF), 13.56 MHz (HF), 2450–5800 MHz (microwave), 3.1–10 GHz (microwave)	10 cm to 200 m	Road tolls, building access, inventory, goods tracking	ISO 18000[k)]

DASH7	433 MHz (UHF), 865–868 MHz (Europe), 902–928 MHz (North America) UHF	0–5 km	Building automation, smart energy, smart city logistics	
SigFox[l)]	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[m)]
Wi-Fi	2.4 GHz, 3.6 GHz, 4.9–5 GHz	Up to 100 m	Routers, tablets, smartphones, laptops	IEEE 802.11[n)]
Z-Wave	ISM band 865–926 MHz	100 m	Monitoring and control for homes and light commercial environments	Z-Wave[o)]; recommendation ITU G.9959[p)]
ZigBee	2.4 GHz; 784 MHz in China, 868 MHz in Europe, and 915 MHz in USA and Australia	10–20 m	Home and building automation, WSN, industrial control	IEEE 802.15.4[q)]

a) http://www.ieee802.org/15/.
b) https://www.bluetooth.com/.
c) https://www.iso.org/standard/59865.html.
d) http://www.3gpp.org/.
e) https://standards.ieee.org/about/get/802/802.15.html.
f) https://www.lora-alliance.org/What-Is-LoRa/Technology.
g) http://www.3gpp.org/release-13.
h) https://www.iso.org/standard/56692.html.
i) https://www.iso.org/standard/50941.html; https://www.iso.org/standard/50942.html; https://www.iso.org/standard/50648.html; JIS X 6319-4 "FeliCa", http://nfc-forum.org/.
j) http://www.nwave.io/; http://www.weightless.org/.
k) https://www.iso.org/standard/46145.html.
l) https://www.sigfox.com/.
m) http://www.weightless.org/.
n) http://www.ieee802.org/11/.
o) http://www.zwave.de.
p) https://www.itu.int/rec/T-REC-G.9959.
q) http://standards.ieee.org/getieee802/download/802.15.4-2015.pdf.

devices may not always constitute the optimal solution. A need for new metaphors and user interfaces exists, in particular those suited for intuitive interaction (see Section 1.6.2.)

1.5.4 Sensors

Sensors are technical components for the qualitative or quantitative measurement of certain chemical or physical variables and properties, for example, temperature, light (intensity and color), acceleration, electricity, and so on. The recorded measured values are usually converted into electronic signals. Currently, we are already surrounded by sensors in many places. For example, modern automobiles contain hundreds of sensors, for example, rain sensors for windshield wiper systems, crash sensors for air bag release systems, and lane and parking-assist sensors. Indeed, modern automobiles, some with far more than 200 sensors and a few dozen microprocessors (Economist, 2009), constitute a good example of this. In fact, the ordinary automobile is increasingly becoming one unified computerized object. In addition, when a sensor is employed together with a processor (controller), a power supply, and a unit for data transmission, this is referred to as a *sensor node*.

A sensor node's primary function is to collect, preprocess, and transmit sensor data from its environment to other sensor nodes or a base station. Examples of sensor categories include (Baras and Brito, 2017) the following:

- *Location:* GPS, GLONASS, Galileo
- *Biometric:* fingerprint, iris, face
- *Acoustic:* microphone
- *Environmental:* temperature, humidity, pressure
- *Motion:* accelerometer, gyroscope

Sensor nodes can form Wireless Sensor Networks (WSN) by means of their transmission unit. For example, these are utilized to (i) detect earthquakes, forest fires, avalanches, as well as terrorist attacks; (ii) monitor vehicle traffic, particularly in tunnels; (iii) track the movements of wild animals; (iv) protect property; (v) operate and manage machines and vehicles efficiently; (vi) establish security areas; (vii) monitor supply chain management; and (viii) discover chemical, biological, and radiological material. For the operation of sensor networks, special software is required, which ensures a dynamic and robust self-organization of the sensor network that functions in a safe and scalable manner. This is because sensor nodes can fail, change their position, or be only online intermittently. WSN can consist of several hundred or hundreds of thousands of sensor nodes, which are deployed either inside of the phenomenon or very close to it.[26] Sensor nodes are connected to an intermediary network that forward the data

26 For an excellent overview on sensor networks, see Akyildiz et al. (2002).

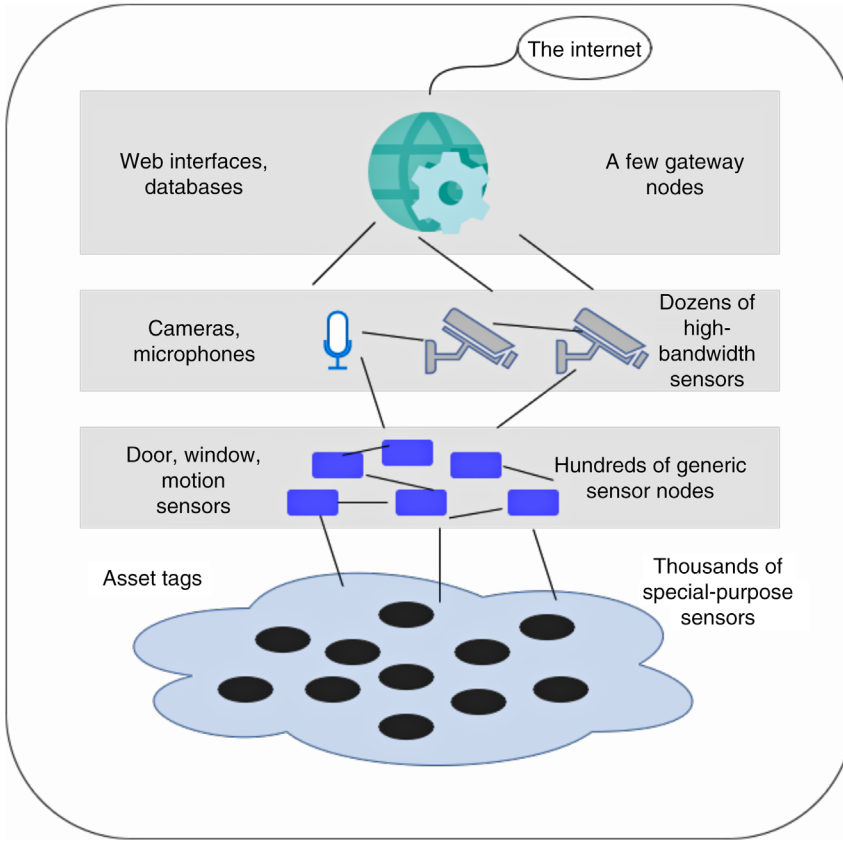

Figure 1.3 Hierarchical deployment of a wireless sensor network.

that they collect to a computer for analysis. Sensor nodes are installed in their workspace to function for years, preferably without requiring any maintenance or human intervention. They must therefore have a low energy requirement and have batteries that are functional over several years. The construction of a typical WSN is layered (see Figure 1.3) (Hill et al., 2004). Specifically, it begins with sensors on the lower level and continues up to the top-level nodes for data collection, analysis, and storage. Simple and complex data are routed through a network to an automated facility that provides continuous monitoring and control of the dedicated environment. WSNs do not necessarily operate on all layers with the common TCP/IP stack and may use dedicated lightweight protocols instead.

Each platform class handles different types of sensing (according to Hill et al., 2004, p. 42). As sensors are foundational to both smart objects and sensor nodes, they are a crucial component of an IoT world. In fact, WSNs will facilitate the

proliferation of many applications. The small, robust, inexpensive, and low-powered WSN sensors will bring the IoT to even the smallest objects installed in any kind of environment, at reasonable costs (IEC, 2014).

1.5.5 Actuators

Actuators convert electrical signals (e.g., commands emanating from the control computer) into mechanical motion or other physical variables (e.g., pressure or temperature), and thus actively intervene with the control system and/or set variables. In the field of measurement and control engineering, actuators are the signal-related counterparts to sensors. Types of actuators include hydraulic, pneumatic, electric, mechanical, and piezoelectric. They convert signals or setting and regulation specifications of a control into (mostly) mechanical work. A simple example of this is the opening and closing of a valve, for example, in a heating system or in the case of engine controls. The output of optical (via displays) or acoustic signals can also be subsumed under actuators, since they can trigger an effect in the real environment. In robotics, the term *effector* is often used as an equivalent for actuators. Effectors allow a robot to grasp and manipulate objects, and thus produce an effect. In a computerized world of things, actuators play an increasingly important role in the realization of actions and effects as a counterpart to the (previously) sensory-detected corresponding contexts. Actuators are a key building block in more recent perceptions of the "Fourth Industrial Revolution" in manufacturing as an Industry 4.0 conceptualization postulate.

1.5.6 Power Supply

While many technologies are already available on the market or at least have been tested in research contexts, unsolved technical problems remain. A very limiting factor of the mobility of smart objects is their energy supply. Although batteries are becoming smaller and more powerful, today's mobile devices still have very limited battery capacities. The heavy research on improved battery technologies has only produced relatively mild progress in battery performance. In fact, it is continually falling behind other relevant technological developments. Some argue that there will soon be (or even exist today, as initial reports on burning smartphone devices may prove) a limit reached in which energy density becomes so high that the respective devices become a serious threat to safety. To counteract these challenges, several avenues of research are being pursued, including intelligent designs that require less battery power. This can be achieved by departing from the idea that everything has to be online all of the time. Sometimes, it is sufficient to only occasionally know about a status shift of an object. This can be communicated with much less relative effort and demand on bandwidth and energy. Another strategy is to

harvest energy "on the fly." The development of technologies for the utilization of alternative sources of energy, such as the sun, wind, and water is progressing rapidly, partly due to political pressure. We have already witnessed this type of integration into portable devices, for example, smartphones with solar cells. Moreover, approaches to extracting energy from the external sources of solar, thermal, piezoelectric, mechanical, and kinetic energy are already established, referred to as *energy harvesting* (Anton and Sodano, 2007; Sudevalayam and Kulkarni, 2011). These approaches are particularly suitable (because of their independence of fixed infrastructures) for the power supply of mobile and autonomous devices, such as sensor nodes. A promising idea for personally used mobile devices is the tapping of the energy that a person naturally produces and emits. Through movement and metabolism (warmth), a person expends several kilowatt hours (heat and movement power). At the same time, several hundreds and up to 1000 W can be generated and stored, which could theoretically generate sufficient power for the operation of a notebook computer. Energy generation from blood glucose or other energy potentials, such as the pH level of body fluids, is also conceivable. Effectively, however, only a fraction of this can currently be accessed, if at all, and the impairment imposed by the required devices on the user may, in some instances, still be too great. Other innovative approaches are biofuel cells that work with bacteria. Through the decomposition products of bacteria, energy can be generated from organic substances. An application of this is to install biofuel cells in wastewater treatment plants and sewage treatment plants, where large quantities of energy-rich organic substances are present.

1.5.7 Identification

An important prerequisite for the linking of information with real entities in our environment is an unambiguous identification of things and people. The umbrella term "Automatic Identification (Auto-ID) and Mobility (AIM) technologies" describes a diverse family of technologies that share the common purpose of identifying, tracking, recording, storing, and communicating essential business, personal, and product data. Several identification technologies exist, for example, biometric, barcodes, and RFID. Applications of RFID, which have been known since the 1960s, have especially become a catalyzer for IoT scenarios.

1.5.7.1 Radio Frequency Identification

Radio frequency identification systems use tiny, so-called *tags* with embedded microchips that typically contain a small amount of computer memory and transmit their content via radio signals over a short distance to specific RFID readers (see Chapter 5). The reader captures these data, decodes them, and sends them to a host computer for further processing via a wired or wireless

network. In fact, RFID tags can be considered as electronic barcodes (Welbourne et al., 2009). However, in contrast to barcodes, RFID tags do not require visual contact in order to be read. The RFID reader consists of an antenna and a radio transmitter with a decoding function, and is attached to a stationary or handheld device. Depending on output power, radio frequency, and ambient conditions, the reader emits radio waves in ranges between 2.5 cm and 30 m. If a passive RFID tag reaches the range of the reader, the tag is activated and begins sending data, that is, the prerecorded number(s) in the tag. In the case of active tags, which are battery powered, the tag itself is capable of sending data. As RFID tags can store a (unique) number and can be physically attached to an object, the object becomes automatically and contactless identified. Due to these major functionalities, RFID is considered to constitute a key technology as it bridges the physical world and virtual world, that is, physical objects become uniquely identifiable. In materials management and supply chain management, RFID systems can record and manage more detailed information about specific items in warehouses or in production much better than do barcode systems. When a large number of items are shipped together, RFID systems track each pallet, batch, or individual item in the delivery. Moreover, the number of reading points is technically unlimited. When there are more reading points in place, manufacturers can better follow the life cycle of each product, aimed at understanding product deficiencies and successes. Another example is books in libraries that use an RFID chip to allow users, by means of RFID reading systems, to borrow and return books without other assistance. In this way, hours of operation restrictions and waiting in lines are avoided. RFID has been available for decades, but the widespread use of tags was delayed as long as the cost of each tag ranged between €1 and 20. Currently, the simplest tags—purchased in large quantities—cost less than €0.10, and probably in only few years will cost less than €0.01. With this dramatic reduction in the cost of tags, RFID has become profitable for many more applications. In particular, the deployment of a large number of tags has become economically feasible, even for low-value items. Cost drivers for an RFID system, however, also include the installation of RFID readers and tagging systems. In addition, companies are likely to have to upgrade their hardware and software systems to process the enormous amounts of data produced by RFID systems. In fact, the monitored transactions could easily add up to hundreds of terabytes. In order to filter, collect, and prevent RFID data from overloading corporate networks and system applications, special middleware is required. The applications need to be redesigned to accommodate the massive volumes of RFID-generated data, as well as to share data with other applications. Large enterprise software vendors, including SAP and Oracle, offer RFID-enabled versions of their supply chain management applications. The power of RFID for IoT is amplified when used together with addressing schemes, in particular the Electronic Product Code (see the next section).

1.5.7.2 Addressing Schemes Based on IPv6 and Electronic Product Code

Addressing schemes has become a crucial task in identifying things. The challenge in an IoT scenario is to uniquely identify billions of devices and, for many application scenarios, to also control them. The top technical challenges are uniqueness, reliability, persistence, and scalability. Internet Protocol version 6 (IPv6) and the Electronic Product Code are important building blocks for IoT.[27]

IPv6 is the most recent version of the Internet Protocol (IP), which is the communications protocol that provides an identification and location system for computers on networks and helps to route traffic across the Internet. The idea of IP is to connect every device to a network while assigning a unique IP address for identification and location definition. With the rapid growth of the Internet after commercialization in the 1990s, it became evident that far more addresses would be needed to connect all devices than its predecessor—the IPv4—had available. By the late 1990s, the Internet Engineering Task Force (IETF) formalized the successor protocol, that is, IPv6. IPv6 uses a 128-bit address, theoretically allowing 2^{128}, or approximately 3.4×10^{38} addresses. In other words, the total number of possible IPv6 addresses is more than 7.9×10^{28} times as many as IPv4, which uses 32-bit addresses and provides approximately 4.3 billion addresses. This seemed to be more than sufficient to assign a unique address to any number of man-made objects present or to be built. IPv6 has incorporated both a rich address scheme and a great deal of sophisticated functionality (for dynamic address management, intelligent routing, etc.), which adds to the so-called protocol overhead and renders IPv6 a relatively heavy protocol. In addition, IPv6 does not fit well, especially regarding the application scenarios of WSNs, which may coordinate extreme large numbers of networked sensors and would not need all of the networking functionalities that come with IP. However, not all layers of a typical WSN usually operate within the established IP stack and can therefore not take advantage of the address scheme provided by IPv6. This calls for an additional subnet layer or for the development of a lightweight form of IPv6 (e.g., 6LoWPAN) that are better suited for IoT scenarios.

The Auto-ID Center at MIT (now Auto-ID Labs, an international research network)[28] and the development community around RFID played a crucial role

27 Many more addressing schemes exist. An early concept that may gain more interest again in terms of IoT is the so-called MAC address. "MAC" reads media access control. It is a unique identifier assigned to network interfaces for communications at the data link layer of a network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet and Wi-Fi. MAC addresses are most often assigned by the manufacturer to devices that will be connected to a network. Usually the unique number is stored in the device, such as the card's read-only memory or some other firmware mechanism. This unique number could also be defined as an Ethernet hardware address, hardware address, or physical address. Accordingly, things that have a MAC address become uniquely addressable.

28 http://autoidlabs.org/wordpress_website/.

in the conceptualization and identification of the standardization efforts needed. The core idea is to discover information about a (RFID-) tagged object by browsing an Internet address or a database entry corresponding to a particular code stored within an RFID tag. They worked on the development of the Electronic Product Code (EPC) (EPCglobal Inc., 2014), that is, a universal identifier that provides a unique identity for every physical object, for all time.[29] Today, the concepts are more general and are not limited to RFID only. A thing can be any real/physical object, but also a virtual/digital entity, which moves in time and space and can be uniquely identified by assigned identification numbers, names, and/or location addresses. For virtual objects, corresponding concepts are Uniform Resource Identifiers (URI) and IP addresses, which allow identifying and discovering an object's presence on the Web.[30] Based on the well-established Domain Name System (DNS),[31] in an IoT context, IP addresses can also be utilized as identifiers for networked objects together with name labels. The core idea is to extend the already existing DNS programming interfaces and formats to small networks where there are no name servers available. One key concept is the multicast Domain Name System (mDNS), which resolves host names to IP addresses within small networks that do not include a local name server (Cheshire, 2017).

1.5.8 Localization

In addition to identification, the position of an object or a human being is essential contextual information. Localization techniques can be employed for determining position, which either localize an object externally or with which an object determines its position itself. Examples of "global" positioning systems are the Global Positioning System (GPS) of the Unites States, GLONASS (Russia), Galileo (European Union), and BeiDou (China). A distinction is made between four types. In trilateration, distances are measured to at least three points, the position of which is known, and the geometrical intersection is used to determine the position. This can be carried out in networks simply by means of propagation times of transmitted signals. Similarly, triangulation, in which angles or directional dimensions are used for the calculation of distance and

29 Its structure is defined in the EPCglobal Tag Data Standard, which is an open standard freely available for download from the website of EPCglobal, Inc.; http://www.gs1.org/epcglobal.

30 A corresponding standardization initiative is organized by the Hypercat Alliance, http://www.hypercat.io/.

31 The Domain Name System (DNS) is a hierarchical decentralized naming system for resources connected to the Internet or a private network. Most prominently, it translates domain names (which are more suited for human readability) to the numerical IP addresses needed for locating and identifying computer services and devices with the underlying network protocols. Since its inception in the 1980s, it has become a worldwide, distributed directory service and an essential component of the functionality of the Internet.

position, also exists. On the other hand, position is measured with the ambient determination by means of the next known point. This method is already utilized today in mobile radio localization in GSM networks by assignment to a mobile radio cell. Another technique, scene analysis, determines position based on specific features of the point of view (called a "footprint"). These features can be actual images of the landscape from the corresponding viewing angle or can be stored beforehand in a table with specific measured values of a point of view, for example, electromagnetic values or radiation specifications in one or several present WLANs. Challenges in localization procedures are the tracking of moving objects and the handling of covered or indoor objects (problematic with GPS positioning) or radiation and falsification of radio waves. However, in recent years, much effort has been invested in indoor localization technologies (Koyuncu and Yang, 2010).

1.5.9 Cloud Computing and Fog Computing

The large and increasing numbers of IoT devices will lead to rapid growth of collected data. Often, such data will have a device–time–space relationship (i.e., time and position data that tightly relate to a specific device). In IoT scenarios, it is likely that such data are shared among several applications, necessitating greater interoperability. Moreover, additional dimensions of objects might be of interest, including different types of sensor data or meta-data, about the object. This creates new data management issues and may change the predominant way of processing. Specifically, processing may move away from a formerly "offline" or batch mode, in which storage and query as well as processing and transactions might have occurred with some delay without negatively affecting applications or services toward a more "online" or real-time world, where collecting, processing, and acting upon data may not allow major delays (Borgia, 2014). Apart from "real-time processing" needs, data archiving with intelligent policies to distill, index, and intentionally delete data in efficient ways is still a major challenge. Several alternative solutions exist, including central approaches, decentralized or data-centric storages that are as near as possible to its production points or – as a kind of mixture – dynamically adjust the data storage position according to specific conditions (see Borgia, 2014, "Data management" for a set of references and Chapter 4 of this book). In order to meet data management challenges,[32] cloud and fog computing are among the most important approaches to cope with IoT data management issues.

Cloud computing is a concept in which computing performance, storage, software, and other services are provided as a group of virtualized resources over

32 Borgia (2014) lists IoT general requirements, such as heterogeneity, scalability, cost minimization, self-service, flexibility, quality of service, and secure environment for which cloud computing and fog computing may contribute answers.

a network, primarily the Internet. In addition to this, the "Cloud" of resources can be accessed at any time from any connected device and site (Zhang et al., 2010; Weinhardt et al., 2009; Armbrust et al., 2010). Typically, users automatically receive cloud resources, such as server time or network storage, without a need for further negotiation with the service provider in an "on-demand self-service" and in an "elastic" manner. This is of tremendous value to the user, as he or she need not to hold available such resources even in the case of large demand. Those resources, and in particular the management of up- and down-scaling, are delegated to the cloud service provider. Most often, cloud services come as a measured service: Cloud resource charges are based on the resources actually used (Mell and Grance, 2011). Cloud computing is seen as a major building block of Ubicomp scenarios (Gubbi et al., 2013; Cáceres and Friday, 2012) in order to cope with the challenges of efficient, secure, scalable, and market-oriented computing and storage. In principle, Cloud computing achieves excellent results in terms of networking resources and storing and accessing data related to or derived from connected things. However, regarding latency-sensitive applications, which require nodes in the vicinity to meet their delay requirements, cloud computing may possess some limitations—especially when millions of devices are to be handled in a time-critical manner. New use cases may arise that call for tight control of physically dispersed, yet specifically located, sensors or actuators (e.g., a plant with machines that have to react to sudden changes in the environment or production process). In response to these challenges, the fog computing paradigm (also referred to as "edge computing") is proposed (Bonomi, 2011; Bonomi et al., 2012), which should not replace the cloud computing paradigm, but extend it.[33] Fog computing, as a highly virtualized platform, provides computing, storage, and networking services between end devices and traditional cloud computing data centers that are typically, but not exclusively, located at the edge of a network. Focusing more on the "edge of the network," however, implies a number of characteristics that make fog computing a nontrivial extension of cloud computing. Fog computing is expected, for example, to deal with widely distributed and mobile deployments in which very large numbers of nodes are involved, for example, fast-moving and large groups of vehicles along highways or large-scale sensor networks to monitor the environment). Since its conceptual inception just some years ago, fog computing has achieved remarkable interest in academia (Dastjerdi and Buyya, 2016) and industrial research (see, for example, the Open Fog Consortium, founded in 2015).[34]

33 There is a significant increase in extant literature on fog computing. *IEEE Internet Computing* devotes a special issue to fog computing in its March 2017 issue.

34 https://www.openfogconsortium.org/.

1.6 Derived Qualities of Modern ICT

Modern information and communication technology infrastructures enable the following qualities: context awareness, adaptability, proactivity, high data quality, and intuitive interaction.

1.6.1 Context Awareness, Adaptability, and Proactivity

Context awareness (also context dependency) is a behavior that depends on information about the context of any entity (programs, people, objects). Information about contexts can be obtained from a wide variety of sources, in particular, via sensors. This information is used to draw conclusions about the context and to adapt the behavior adequately. The utilization of contextual information is most frequently associated with time and location aspects, in the latter case referenced as location-based services. However, any further aspects can be included in a context model if corresponding information sources or sensors exist (Perera et al., 2015). This can be, for example, archive data or biometric data, the temperature in an environment, or relationships between people (Dey, 2001; Dourish, 2004; Coutaz et al., 2005).[35]

Context sensitivity allows for adaptability and proactivity. It is even less intrusive and disruptive when services and functionalities provided by smart environments adapt to the context and are proactively offered outside of a smart environment. Currently, the degree of customization of conventional computers and mobile phones is very low. Adaptations to regional conditions, such as language and time settings, are customary. It is expected that more contextual information will be utilized in the future, and device settings and services will automatically adapt accordingly, such as the position of the user, his or her health or emotional state, his or her plans, tasks to be done, and other factors in the environment that affect the user. Proactivity unites the adaptability of applications in the background and an anticipated interaction of a designated user with the offered service. Services are automatically offered to a user in the ideal case wherever and whenever they are needed. The initiator is the smart environment itself, and not the potential user. This quality entails a major requirement: The smart environment must be able to correctly recognize the context and the intentions of the user. It is questionable whether this can also be achieved reliably in complex situations. A simple example shows only one of the difficulties for a reliable implementation: If a person falls unconsciously to the ground, the automated sending of an emergency call is useful, but this case is different from "similar" occurrences, for example, if the person drops suddenly and deliberately on the sofa to rest. The recognition of the situation and the

35 For an in-depth recapitulation of what context is and whether context can be computerized, consult Dourish (2004).

"right" context (context awareness) is one of the core challenges of the realization of a computerized world.

1.6.2 Increased Data Quality

The improved availability of data in terms of quantity ("we know more about the status of a thing or related process") and quality ("we know more details about it") may constitute the most obvious change resulting from omnipresent information-gathering mainly through sensors. Obtaining better data about things in general is fundamental for any improvement related to products, processes, and business models. The subsequent sections will differentiate four dimensions of (improved) data quality and its effects, that is, the substitution and elasticity effect.

1.6.2.1 Dimensions of Data Quality

IoT platforms allow for an increase of data quality at approximately the same cost and in a simpler way than previously. These improvements can be described by four dimensions of data quality.

1) *Object Granularity and Type.* Falling hardware costs and miniaturization simplify the use of technical components on individual objects at lower costs. Granularity refers to the number of objects of a group or class, through which the information is aggregated. Due to certain concepts, such as ubiquitous computing, fine-grained data can be acquired for individuals, and even very small objects. Today, containers and pallets are tracked on their delivery routes using RFID and GPS. Soon, the data acquisition for each of the products on the pallets, including a small item, such as a yogurt cup, becomes affordable. This means that all object types, including products of low value and with a short lifetime, are also recorded within economic boundaries.
2) *Time Granularity.* Efficient data transmission and wireless networks in smart environments enable simple, continuous data collection in real time. Although inventory is still carried out periodically and manually in many companies, it can run continuously and automatically with an RFID system. This means that current inventory data can be called up at any time, and changes can be viewed in real time or very promptly. However, real-time data collection is problematic, for example, on flights in which data transmissions can interfere with air traffic, and when objects move very quickly or relevant features of the environment change very rapidly.
3) *Data Content.* RFID is a cost-effective, highly tested technology for contactless individual object identification. It offers several advantages over the conventional barcode and serial IDs, which can only be read by visual contact. Through RFID, an individual ID can be linked to the object both physically and digitally simultaneously. The EPC is such a unique ID. Depending on the tag type, additional data, such as the date of manufacture and the production location, can be stored on an RFID tag. However, the

storage space is typically limited to a few kilobytes. Only the utilization of additional data stores and sensors at the object and in the environment allows for more comprehensive object or context data.

4) *Reach.* The dimension reach is less dependent on technologies than on application concepts. Through networking, the integration of applications and information systems is generally possible throughout a company or in an interorganizational manner. However, cooperative agreements and agreements on standards are crucial for the success of implementations. In supply chain management, data standards, such as EAN and EPC from GS1, are particularly widespread. Other standards, such as XML, Semantic Web standards, and Web Services, make it easier to implement these applications.

1.6.2.2 Effects of Increased Data Quality

Equipping the infrastructure with sensors and actuators has two effects. First, there is a substitution effect. Conventional data collection and retrieval (e.g., manual or barcode) are automated, and media discontinuities are avoided. Second, an elasticity effect exists (Fleisch and Tellkamp, 2006). In addition, new data can now be collected and utilized. As a result, companies can map real-world information in real time, and thus use it to directly control processes and activities. This allows digitization of management regimes and leads to better decision-making. Business can easily collect more data and enrich existing collections with new data quality. The data may also be employed for triggers and alarm functions for certain events, for example, if a delivery transport is stuck in heavy traffic. If this concept is implemented together with business partners and transferred into an integrated information system, the so-called event-driven supply chain management can be implemented. Furthermore, automated processes lead to independent monitoring and control, for example, in production processes. With very high data quality, in particular with high time granularity, a real-time process control of the company can be implemented on the basis of the automatically recorded data, which are directly available for management via fast network connections, regardless of where the decision-makers would like to retrieve them. It is critical to consider whether real-time data are actually required for all processes and tasks, or whether summarizing the data in larger reporting cycles is already sufficiently appropriate.

1.6.3 Intuitive Interaction

Technology disappears by embedding it in the physical environment so that it is no longer perceptible. This makes it even more necessary that functionality and operability remain recognizable to the user. This can be termed the "invisibility dilemma." The solution to this dilemma constitutes the design of an intuitive human–computer interaction. A key concept is the implicit use of information systems (Kranz et al., 2010). It works like automatic sliding doors, which open as soon as a person approaches, without an explicit command. For example, the

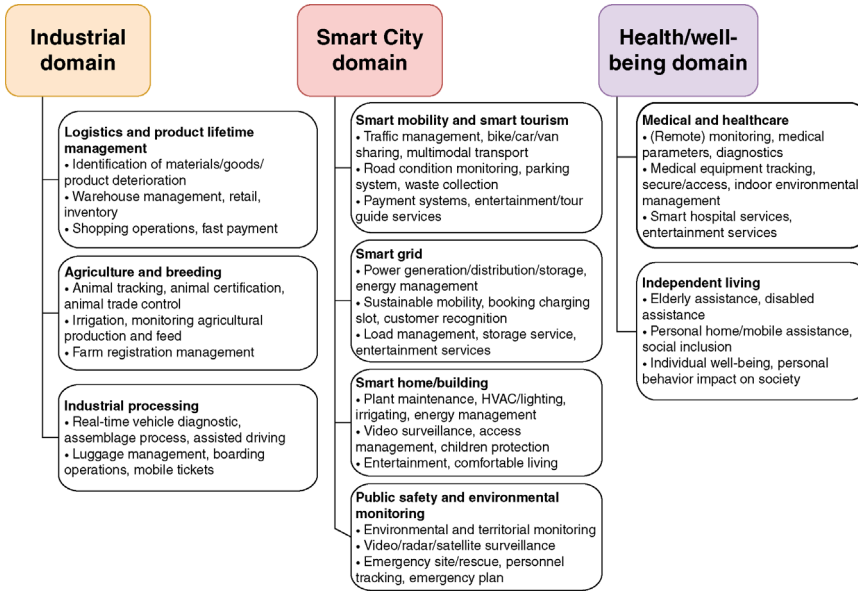

Figure 1.4 IoT application domains and related applications. (Adapted from Borgia, 2014, p. 9.)

natural behaviors of people are used, which are recognized, for example, by language, glances, facial expressions, and movements.

1.7 Potential for Product, Process, and Business Model Innovations

Opportunities for product, process, and business model innovations reside in two fields: (i) innovating within the IoT ecosystem; and (ii) innovating based on the IoT ecosystem. The focus here will be on the latter.[36] The presented qualities of modern information and communication infrastructures, as well as the congruency of smart objects and smart environments, offer great potential for innovation in nearly every field (see Figure 1.4). This is mainly due to the new or enriched "qualities" that an informatized infrastructure provides (see Section 1.6).[37]

36 A good overview of aspects of innovating within the IoT ecosystem is provided by the EU-funded H2020 UNIFY-IoT project: Supporting Internet of Things Activities on Innovation Ecosystems, Deliverable 02.01, IoT Business Models Framework, http://www.unify-iot.eu/wp-content/uploads/2016/10/D02_01_WP02_H2020_UNIFY-IoT_Final.pdf (retrieved January 29, 2017).

37 Borgia (2014) attempts to enumerate the domains and perceivable applications; see Parts IV and V for detailed examples.

Companies can develop new or improved processes or products (which include services here) in order to gain an advantage against their competitors. Existing business models may also be changed (Iansiti and Lakhani, 2014). However, how can companies create such innovations? For the development of applications, two approaches can be determined: problem-initiated innovation and the technology-driven innovation.

In the case of problem-initiated innovation, new technologies are developed or utilized in a targeted manner to solve a specific problem. This often leads to incremental innovations that initially increase the efficiency of existing business processes or products or services. In his seminal article, March (1991) speaks of "exploitation." These innovations are usually triggered by the user, who expresses a desire for improvement. Through IoT, control and information-intensive processes can be improved. By using RFID, sensors, and localization procedures, supply chains can be automated and controlled in real time. This avoids or reduces costs due to unexpected disturbances. In addition, antitheft protection can be improved and anticounterfeiting measures can be increased.

Technology-driven innovations sometimes exhibit a radical character since they help solve existing problems in a completely new way. In terms of March (1991), a highly cited technology management researcher, this is labeled "Exploration." In a typical case, the developer (inventor) or an expert in the corresponding technology has an idea of how to use it in a valuable way. He or she focuses on the special features of the technology. The features of smart environments have already been presented. As a result, new services and products can be developed that offer customers added value over old and comparable products. With IoT, computerized products and context-based services can be offered. As the technology-driven innovation does not originate from the user, a danger exists that it will not fulfill user needs. Therefore, users should be integrated into the innovation process as early as possible. If innovations are aligned with the actual needs of their users, business processes and products can not only be improved but also be fundamentally innovated.

The power for innovation may be illustrated by three categories: (i) new products; (ii) new processes; and (iii) new business models.

1.7.1 Product Innovation

Most traditional products can become smart objects by enriching them with information technology. Then, the products can store information about their entire product life cycle from manufacture to disposal, and possibly exchange it with other products, smart environments, or users. Equipped with appropriate processors and a control program, they can even adapt their behavior to specific contexts or trigger autonomous actions. A real example is pans, which read in recipes via RFID and prepare the food with the stated temperature and cooking time. For this purpose, they can communicate with the stove (which must have

appropriate, coordinated communication standards) and regulate the degree of heat. New products and related value-added services benefit from data present in higher granularity (Fano and Gershman, 2002; Ferguson, 2002; Allmendinger and Lombreglia, 2005; Iansiti and Lakhani, 2014).

1.7.2 Process Innovation

In combination with novel information and communication technology infrastructures that achieve a previously unprecedented level of data quality, processes can be more precisely captured and assessed, as well as processed faster, and in a more integrated and automated manner. In addition, these achievements can be obtained in extreme cases in near-real time or in real time. Many processes benefit from context-based information.

The core factor for improved processes is improved data, or data that have been distilled to more meaningful information. The ubiquity of information gathering and presentation is accompanied by the fact that the number and size of media discontinuities between the virtual and the real world are reduced. This closes the gap between the real and the virtual world. This also opens the path to better automation and integration (Chui et al., 2010). When data are entered manually into the system via the keyboard, errors can occur at every media discontinuity; apart from another problem, that time will elapse before data are recorded and ready for further processing. A technical approach is the encoding of data using barcodes. This idea first appeared in the 1930s. Successors of the first, one-dimensional barcodes are two-dimensional codes, also called *2D codes*. The information is stored not only on one axis, but vertically and horizontally. There are many coding schemes, of which one of the best known is the "QR code"—quick response code. The acceptance of further dimensions (color, time) results in 3D or 4D code, which can also store more information in a compact manner. With RFID (see Section 1.5.7.1), media discontinuities are greatly reduced, and the data are immediately transferred to a connected back end system after contactless detection. The same applies to data from wireless sensor nodes. Data acquisition, processing, and distribution are automated in the computerized world, that is, human intervention is no longer required. However, intervention points, for example, for configuration, subsequent control, or in the event of a malfunction, should still be available. Through automatic data transmission between networked objects and environments, a media-free integration of applications and enterprise systems can be implemented. This means that data are forwarded to authorized systems according to defined rules, and processed there according to the application. The prerequisites for this are uniform data formats and communication rules (protocols). In other words, the systems must be capable of mutual understanding. For example, which context data belong to which object and how to interpret special sensor measurement values must be known. If smart objects are equipped with artificial intelligence,

self-controlling processes can be realized. In this context, for example, delivery packages or products "take their own way to the destination" and pass on production information to machinery or transport vehicles. These intelligent objects make autonomous decisions and organize themselves in a decentralized manner. One way of embedding these skills into objects is software agents, that is, a self-executing software program that makes decisions based on rules and learned knowledge, which, in some way, control or influence their environment through actuators, adapt to changes, and react to expected and unexpected events.

1.7.3 Business Model Innovation

Business models are also affected or altered by computerized worlds or can only be realized through them (Chan, 2015). For example: (i) Companies have the opportunity to redesign their pricing through the improved information base. In this way, customers' different payment options could be better recognized by means of price discrimination. For example, in the course of exploiting individual contexts, corresponding pricing can be made. An actual implementation of such price models is the "pay as you drive" tariffs for automobile insurance. (ii) Enterprises can redefine existing value chains. One example of this is the Zipcar, one of the world's largest car-sharing companies. The available automobiles or their positional data are automatically transmitted to the control center so that car-sharing members can quickly identify driving opportunities via a web interface. The company views itself less as a car rental company than as a flexible mobility service provider. (iii) The computerization of the everyday world could lead to new care services, for example, in the health sector. Together with the presented "smart home," people that require intensive care could live better and longer in an environment that is familiar to them.

Particularly in the field of mobile communications, location-based services are already being used, which consider the position of the user and, for example, display restaurants in the current environment of the user. Context-based services include not only location information but also other relevant information about the environment and the user. In smart environments, context data can be utilized to provide services that are adapted to the situation, the user, his or her tasks, wishes, plans, and other factors, or react to a specific context with meaningful actions or suggestions. Navigation systems that receive information about road conditions and traffic on the target route in real time are able to reconcile this context information with the user's target data and then make flexible route adjustments. This could also warn the driver of any short-term accidents coming up or imminent tire damage (if sensors are installed on the tire/wheel system of the automobile). In addition, context-based marketing is tuned to customers, their whereabouts, and other context factors, so that as little randomness as possible is caused by unsuitable advertising campaigns, for

example, offers of umbrellas, which can be bought in the surrounding area during rainy weather. Personal customer data can also be used to differentiate customer groups. In the case of scarce resources, service differentiation can be carried out. Important customers are treated preferentially. Product and information individualization also create added value. Information is individually tailored and adjusted, and product properties adapted to individual preferences, so that the customer can achieve a higher level of satisfaction.

The mentioned examples and the major trend that increasing numbers of things are creating more data have produced conceptualizations, including "data centricity," "competing on analytics," "Big Data-based business models," and so on. IoT and its implications for sensors and creating ever-increasing amounts of data constitute a new opportunity for creativity aimed at transforming data into value-creation activities.

1.8 Implications and Challenges

The computerization of the (everyday) world is accompanied by major implications and challenges, which can be characterized as (i) new markets; (ii) changed value creation; (iii) increased awareness of information spaces; and (iv) and social, ethical, legal, and risk aspects.

1.8.1 New Markets

A computerized world of connected things opens the door to innovations that facilitate new interactions among things and humans, and allows the realization of smart cities, infrastructures, and services that promise an enhancement of quality of life. By 2025, IoT could have an economic impact of US$11 trillion per year, which would represent approximately 11% of the world economy; and that users will deploy 1 trillion IoT devices (Manyika et al., 2015; Buyya and Dastjerdi, 2016).

Many reports and white papers (Ducatel et al., 2001) provide scenarios for impacts on hospitals, transportation systems, parcel services, supermarkets, offices, and other areas of everyday life. An illustrative example of the impact of computerized worlds on our everyday lives is the "smart home." In the smart home, devices, objects, and rooms are computerized and networked. The inhabitants can control furnishings, such as lights, doors, refrigerators, curtains, and so on, via remote control, voice control, or hand movements. They are also able to use the Internet to check whether everything is working well and acceptable in the house. The smart home also recognizes sensors that indicate when someone is in the house, and can turn on the lights automatically when an occupant enters a dark room. It can also recognize and store the preferences of residents. For example, in the case of a resident who watches his or her favorite television series every Saturday afternoon, the television is turned on with a

corresponding transmitter or, if the resident is not at home, the sequence is automatically recorded. In addition, when food and related supplies are used daily, a sensor, after checking the contents of the refrigerator, sends a message to the digital notepad in the kitchen and places the products on a shopping list, which each of the residents can access by smartphone, for example, while they are at the supermarket. More integrated scenarios might trigger autonomous replenishment systems consisting of third-party-provided robots physically refilling, for example, a refrigerator. This and other scenarios can be developed much further. The essential point, however, is that the actors in a computerized world are aware of the potential impact on value-added features and markets. These are particularly the result of the fact that, as the example scenario shows, many more actors are involved in value creation for a customer.

1.8.2 Changed Value Creation

Together with higher data quality (as shown above), the importance of data and information as a resource for value creation is clear. This can be seen simply by observing the effects of a computerized world on value creation at different levels. On the individual level, consumers and producers are living in a computerized world. On the one hand, consumers are provided with information as consumer goods (either in the form of information services or in combination with computerized products) and, on the other hand, as input for decisions. Information can reduce search costs and facilitate rational action, as decisions can be weighed more accurately with more relevant information. On the other hand, for the convenience of context-based offers, the disclosure of personal preferences, personal data, and payment needs is required. In addition to efficiency improvements and cost advantages, producers can also benefit from differentiation, price discrimination, and bundling strategies by improving the information base. This creates great potential for the optimized elimination of the consumer's willingness-to-pay. For groups of individuals and organizations, the coordination and control of certain processes is facilitated. This makes it easier to ascertain the location and activities of the employees. Members of organizations can be brought to the same level of information due to better networking. This creates starting points for the analysis and improvement of group coordination. Contracts in the field of risk distribution and incentives can be made more equitable by capturing behavior that has not yet been observable at low cost. This allows a more equitable distribution of risk. Examples of this are working and insurance contracts, product guarantees (e.g., "Has a customer carefully maintained his or her automobile?"), and emissions monitoring for harmful exhaust fumes. Based on economic analyses, an increase in the efficiency of economic trade can be foreseen. One of the main effects of computerized worlds in the context of value creation is the reduction of information asymmetries. In real markets, based on the asymmetric distribution of information, two effects may arise: adverse selection and moral hazard.

Adverse selection occurs because certain information is not observable by providers. For automobile insurance, this is information about whether a new policyholder is a good or a poor driver. The downside for good drivers that emerges from adverse selection is that they pay, in principle, just as high of an insurance premiums as poor ones (as long as the automobile insurance provider cannot distinguish a good driver from a poor one). Moral hazard causes a change in behavior, as the risk of discovery of especially bad behavior decreases. Thus, a driver can intentionally reduce the risk of accidents by driving at a reasonable speed, abstaining from alcohol, observing distances, and so on. As a result of the conclusion of an insurance policy, the incentive to avoid accidents is, at least theoretically, reduced. A stereotyped form of moral hazard is that drivers become even more risk-averse, as they feel that they are already well covered for financial risks of careless or risk-taking driving. Sensors are also able to observe behavior in an objective manner. Speed, travel times and distances, braking behavior, as well as attention and alcohol levels can be measured, in principle. An automobile insurance company can now introduce price differentiation according to the real behavior and abilities of the drivers. This has already occurred in 2004 in Great Britain in the insurance company Norwich Union, which offered the tariff "pay as you drive" to automobile drivers. As a part of the program, they installed a black box in the automobile, which collected the relevant data about the driving behavior and sent them to Norwich Union.

Not only technical but also socioeconomic networks will be much more abundant between companies, users, consumers, and even objects. From an economic perspective, this creates network effects on consumption and production. This means that the benefit of a technology will increase with increasing numbers of users in the market. In order to obtain market share for products or standards associated with network effects, low prices are to be expected at the very beginning in order to build up critical mass.

1.8.3 Increased Awareness for Information Spaces

For context-based services, information is often required, which is owned by different actors. Thus, such services may be based on information from the user, for example, his or her name and allergies, to information from the owner of an environment, for example, the position of a user in a supermarket, as well as products in his or her environment, and information from the service provider, for example, information on allergenic substances in a specific product. Therefore, context-based services cannot be offered if each actor would protect his or her information from external access. Rather, information spaces must be created in which different information systems are brought together by different actors. An information space thus includes all of the data and relevant information obtained in a smart environment to provide users with context-based services and applications. Access to an information space can be restricted to certain actors, but it can also be publicly accessible, so that third parties can utilize the information for innovative

services. The main challenge is that third parties comprehend the information available in the information spaces. For this purpose, semantic technologies may constitute a useful approach. The management of information spaces can be viewed as a task of information management (Schoder, 2011). As indicated, the provision of smart, context-based services requires information spaces that encompass the information systems of different actors. This presents companies with the challenge of managing these information spaces to provide shared value with partners and for their own benefit. This management takes place in a relationship of tension between the potential for innovation induced by the opening up of information spaces and the desire to profit exclusively from closed information spaces with the presumed retention of full control and data integrity. On the one hand, opening up information spaces means that third parties can access the information and integrate it into new, innovative services. This is already currently apparent as an opening of information systems, such as Google Maps and Facebook, which has led to a huge number of mashups and externally developed, innovative applications. In a computerized world in which data about reality are available at a much higher level of quality, a dramatically greater potential for innovation is to be expected if the data are freely accessible. On the other hand, the question arises of how a company can benefit from the fact that third parties use their information to create innovations. Companies could therefore rely on keeping their information spaces closed in order to exclude competitors and to utilize access to the information space as a source of revenue. Such information spaces, however, would run counter the realization of a computerized world. For information space management, the question arises as to how far information spaces should be opened in order to increase the potential for innovation and, on the other hand, to profit as much as possible. In addition, this raises the question of who should own and control devices and their data? A simple use case illustrates the conflict (Cáceres and Friday, 2012), that is, augmented home thermostats (rendering them as smart objects) connected to a smart power grid. Who should own the data that are generated through the home thermostat at the user's home: the end user or the service provider? What happens when the user's (local) desires to be comfortable conflict with the provider's (global) goals to save energy?

1.8.4 Social, Ethical, Legal, and Risk Aspects

Informatized worlds exist in a constant tension between innovation (the technically feasible) and individual and social acceptance (the socially desirable). The difficulties with the above-mentioned pricing strategies are, above all, customer acceptance and related concerns regarding the violation of privacy (Shin, 2010). Obtaining fine-grained data on entities, and especially individuals, expose the core dilemma in a modern IoT. Specifically, any person-related information may do both: enrich context- and person-related, individual services, and constitute potential intrusion into privacy, leading to resistance (Garfield, 2005). Besides privacy, many other fundamental challenges exist with

regard to (IT) security, trust, and so on. The lack of security across IoT in general and the Industrial Internet of Things in particular has come to light largely due to an experimental search engine called Shodan (Wright, 2017). Launched in 2009, the service crawls nearly four billion devices from which, at any given time, several hundred million devices are turned on (depending on network connectivity). As a threat analysis based on Shodan showed, more than 100,000 IoT devices can be easily attacked, among them being special-purpose industrial computers for regulating the flow of water, transportation systems, and even entire power grids (Leverett, 2011). Many of these systems were designed before the advent of IoT, and thus did not consider these types of security threats. IoT certainly is confronted with literally all security problems already known from other IT-based concepts and artifacts—and may add some more aspects if not just by the severity and importance.

Some examples of pressing research questions include the following[38]:

- How should we cope with privacy issues in Ubicomp scenarios focusing on system design considerations? (Langheinrich, 2001)
- Who is accountable for decisions made by autonomous systems? (Berman and Cerf, 2017)
- How do we promote the ethical use of IoT technologies? (Berman and Cerf, 2017)
- What role does trust management play in IoT scenarios? (Sicari et al., 2014; Yan et al., 2014)
- What can middleware do for security and privacy issues? (Atzori et al., 2010)
- What are the security requirements to deal with data confidentiality? (Miorandi et al., 2012)
- What are the relevant legislative challenges? (Weber, 2010)
- What are appropriate architectural options for security and privacy, in particular the advantages and disadvantages of centralized and distributed architectures? (Roman et al., 2013)
- What are the principal attack models and threats? (Hu, 2016)

In order to include some sensitivity in the scale and scope of social, ethical, legal, and risk aspects of IoT, there is a focus on "data" and related data privacy issues (Cáceres and Friday, 2012).[39] It is worth noting that this list of questions is not exhaustive.

---

38 An overview by Rose et al. (2015), published by the Internet Society, provides a broad spectrum of issues raised by IoT, including security, privacy, interoperability/standards, regulatory, legal, as well as emerging economy and development issues.

39 Cáceres and Friday (2012) created a list of relevant questions in the context of Ubicomp scenarios, which, by definition, have the "user" as a focal element and amplify privacy issues. On the other hand, IoT may encompass more generic scenarios, in which the user is not always the immediate focal element.

- When can we infer with certainty? We need to take into account that sensed data or interactions are imprecise observations of the world, often taken from multiple sensors and at varying points in time. IoT environments must consider this evidence and make a judgment of when and how to react. Full appreciation of the value and meaning of data is certainly application and context dependent. Do we have machines (or more precisely software) that are advanced enough to "understand" such context and data properly?
- Where are data located? It is easier to answer this question in the context of technical aspects of cloud and fog computing architectures. However, regarding ownership, control of data, and access to data, obtaining the answer is substantially more challenging. For many environments, such as rooms, homes, companies, and hospitals, the demand for security and privacy requires enforcing conventional, legal, and physical boundaries.
- How long should data persist? What does the environment know about us? What should it know and with what should we trust it? How long should data be retained? What is transient and what should persist? Can we delete data, and can they be forgotten? Who has (the right) to access data? Who is the owner of sensed data? Is it the sensor's owner, the owner of the environment where the sensor is working, or the collector of data (Foster, 2017)?

Most, if not all, of these questions have gained prominence recently with the advent of "Big Data" and its unprecedented scale of storing, computing, and executing data and gaining insight from them. In addition, questions exist that are related to who will pay for IoT infrastructures (less obviously, but eventually, the common citizen with his or her tax dollars). Regulations concerning who is responsible for managing and maintaining local, regional, national, and supernational infrastructures are needed, and to a large extent not yet defined. Due to technical issues and a general reluctance, it will not be the common user who will be manager of his or her own data, that is, it will be service providers. Managed services would certainly reduce complexity for the end user, and obscure complicated technological interfaces. However, managed services also introduce their own tension between manageability and cost for the provider versus flexibility and control for the end user (Cáceres and Friday, 2012). One example of an initiative that addresses policy and regulation issues is the Mauritius Declaration on the Internet of Things. Excerpted example statements include the following[40]:

- IoT sensor data are high in quantity, quality, and sensitivity, and as such should be regarded and treated as personal data.

40 Mauritius Declaration on the Internet of Things, Balaclava, https://icdppc.org/wp-content/uploads/2015/02/Mauritius-Declaration.pdf (October 14, 2014).

- Transparency for all stakeholders is key. Those who offer IoT devices should inform the user so that he/she becomes clear about what data are collected, for what purposes, and how long these data are retained.
- Privacy by design should be the default design principle.
- In order to cope with security challenges, one way to minimize the risk to individuals is to ensure that data can be processed on the device itself (local processing). Where this is not an option, companies should ensure end-to-end encryption to protect the data from unwarranted interference and/or tampering.
- The data protection and privacy authorities should ensure compliance with the data protection and privacy laws in their respective countries, as well as with internationally agreed privacy principles, including appropriate enforcement action, either unilaterally or through means of international cooperation.

Taking into account the enormous challenges faced by IoT developers, data protection authorities and individuals should engage in a strong, active, and constructive debate on the social, ethical, legal, and risk aspects of IoT.

1.9 Conclusion

While the concept of combining computers, sensors, and networks to monitor and control devices has existed for decades, the recent confluence of key technologies and market trends is catalyzing the idea of IoT.

In order to better structure the scale and scope of IoT, this chapter provided an introductory overview, and briefly sketched the conceptual core ideas as laid out prior to IoT with "ubiquitous computing." The chapter presented a four-layer "Internet of Things" framework that covers not only technical but also non-technical issues of IoT.

IoT promises to form the foundation of new products, processes, and business models, and may fundamentally affect both B2C and B2B markets, as well as the way that we produce goods as envisioned with derivatives, including the Industrial Internet of Things and Industry 4.0. While the ramifications are very likely significant, a number of potential challenges may obstruct this vision, particularly in the areas of security, privacy, interoperability, standards, as well as legal, regulatory, and rights issues, and the inclusion of emerging economies. IoT encompasses not only technological but also social and policy considerations. IoT is already rapidly becoming more and more of a reality, and a vast space currently exists for new designs and realizations of creators and developers.

References

Aarts, E., Harwig, R., and Schuurmans, M. (2001) Ambient intelligence, in Denning, P. (ed.), *The Invisible Future: The Seamless Integration of Technology in Everyday Life*, McGraw-Hill, New York, pp. 235–250.

Aggarwal, C.C., Ashish, N., and Sheth, A. (2013) The Internet of Things: a survey from the data-centric perspective, in Aggarwal, C.C. (ed.), *Managing and Mining Sensor Data*, Springer.

Ahlgren, B., Hidell, M., and Hgai, E. (2016) Internet of Things for Smart Cities: interoperability and open data. *IEEE Internet Computing*, 52–56.

Akyildiz, I.F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. (2002) Wireless sensor networks: a survey. *Computer Networks*, **38**(2002), 393–422.

Allmendinger, G. and Lombreglia, R. (2005) Four strategies for the age of smart services. *Harvard Business Review*, **83**(10), S.131–S.145.

Anton, S. and Sodano, H. (2007) A review of power harvesting using piezoelectric materials (2003–2006). *Smart Materials and Structures*, **16**(3), R1–R21.

Armbrust, M., Fox, A., Griffith, R., Joseph A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., and Stoica, I. (2010) A view of cloud computing. *Communications of the ACM*, **53**, 50–58. doi: 10.1145/1721654.1721672

Ashton, K. (2009) That 'Internet of Things' thing: in the real world, things matter more than ideas. RFID Journal. C Available at http://www.rfidjournal.com/articles/view?4986 (retrieved December 2, 2016).

Atzori, L., Lera A., and Morabito, G. (2010) The Internet of Things: A Survey. *Computer Networks*, **54**(15), 2787–2805.

Atzori, L., Lera, A., and Morabito, G. (2014) From "smart objects" to "social objects": the next evolutionary step of the Internet of Things. *IEEE Communications Magazine*, **52**(1), 97–105.

Baras, K. and Brito, L. (2017) Introduction to the Internet of Things, in Hassan, Q.F. (ed.), *Internet of Things: Challenges, Advances, and Applications*, CRC Press.

Berman, F. and Cerf, V.G. (2017) Social and ethical behavior in the Internet of Things. *Communications of the ACM*, **60**(2), 6–7.

Bledowski, K. (2015) The Internet of Things: Industrie 4.0 vs. the Industrial Internet. Available at https://www.mapi.net/forecasts-data/internet-things-industrie-40-vs-industrial-internet.

Bonomi, F. (2011) Connected vehicles, the Internet of Things, and fog computing. The Eighth ACM International Workshop on VehiculAr Inter-NETworking (VANET 2011).

Bonomi, F., Milito, R., Zhu, J., and Addepalli, S. (2012) Fog computing and its role in the Internet of Things. Proceedings of MCC'12, August 17, 2012, Helsinki, Finland.

Borgia, E. (2014) The Internet of Things vision: key features, applications and open issues. *Computer Communications*, **54**, 1–31.

Buyya, R. and Dastjerdi, A. (2016) *Internet of Things: Principles and Paradigms*, Morgan Kaufmann.

Cáceres, R. and Friday, A. (2012) Ubicomp Systems at 20: progress, opportunities, and challenges. *IEEE Pervasive Computing*, **11**, 14–21.

Jain, F A.K., Hong, F L., Pankanti, S.. and CERP-IoT (2009) Internet of Things: Strategic Research Roadmap. Technical Report, Cluster of European Research Projects on the Internet of Things, September 2009. Available at http://www.internet-of-things-research.eu/pdf/IoT_Cluster_Strategic_Research_Agenda_2009.pdf.

Chan, H.C.Y. (2015) Internet of Things business models. *Journal of Service Science and Management*, **8**, 552–568. http://dx.doi.org/10.4236/jssm.2015.84056.

Cheshire, S. (2017) Multicast DNS. Available at http://www.multicastdns.org/ (accessed February 27, 2017).

Chui, M., Löffler, M., and Roberts, R. (2010) The Internet of Things. *McKinsey Quarterly*, **2**, 2010.

Conti, M., Das, S. K., Bisdikian, C., Kumar, M., Ni, L.M., Passarella, A., Roussos, G., Tröster, G., Tsudik, G., and Zambonelli, F. (2012) Looking ahead in pervasive computing: challenges and opportunities in the era of cyber–physical convergence. *Pervasive and Mobile Computing*, **8**(1), 2–21.

Coutaz, J., Crowley, J.L., and Dobson, S. (2005) Context is key. *Communications of the ACM*, **48**(3), S.49–S.53.

Dastjerdi, A.V. and Buyya, R. (2016) Fog computing: helping the Internet of Things realize its potential. *Computer*, **49**(8), 112–116.

Dey A.K. (2001) Understanding and using context. *Personal and Ubiquitous Computing*, **5**(1), S.4–S.7.

Dourish, P. (2004) What we talk about when we talk about context. *Personal and Ubiquitous Computing*, **8**(1), S.19–S.30.

Ducatel, K., Bogdanowicz, M., Scapolo, F., Leijten, J., and Burgelman, J. (2001) Scenarios for ambient intelligence in 2010. IST Advisory Group, Office for Official Publications of the European Communities.

Economist (2009) The connected car. The Economist Technology Quarterly, pp. 14–15 (June 6).

EPCglobal Inc. (2014) GS1 EPC Tag Data Standard 1.9, 2014. Available at http://www.gs1.org/epc/tag-data-standard.

Espada, J.P., Martínez, O.S., García-Bustelo, B.C., and Lovelle, J.M. (2011) Virtual objects on the Internet of Things. *International Journal of Interactive Multimedia and Artificial Intelligence*, **1**(4), 23–29.

ETSI (2010) TC M2M, ETSI TS 102 689 v1.1.1 (2010-08): Machine-to-Machine Communications (M2M); M2M Service Requirements. Available at http://www.etsi.org/deliver/etsi_ts/102600_102699/102689/01.01.01_60/ts_102689v010101p.pdf.

ETSI (2016) SmartM2M; IoT Standards Landscape and Future Evolutions, ETSI TR 103 375 V1.1.1 (2016-10); Available at http://www.aioti.org/wp-content/uploads/2016/05/tr_103375v010101p.pdf (assessed February 27, 2017).

Evans, D. (2011) The Internet of Things. How the Next Evolution of the Internet Is Changing Everything [White Paper], Cisco Internet Business Solutions Group (IBSG).

Fano, A. and Gershman, A. (2002) The future of business services in the age of ubiquitous computing. *Communications of the ACM*, **45**(12), S.83–S.87.

Ferguson, G.T. (2002) Have your objects call my objects. *Harvard Business Review*, **80**(6), S.138–S.144.

Fleisch, E. and Tellkamp, C. (2006) The business value of ubiquitous computing technologies, in Roussos, G. (ed.), *Ubiquitous and Pervasive Commerce*, Springer, pp. S.93–S.113.

Fortino, G. Ganzha, M., Palau, C., and Paprzycki, M. (2016) Interoperability in the Internet of Things. Guest Editors' Introduction, Computing now [IEEE]. Available at https://www.computer.org/web/computingnow/archive/interoperability-in-the-internet-of-things-december-2016-introduction.

Foster, T. (2017) Regulation of the Internet of Things. Available at http://www.scl.org/site.aspx?i=ed47967 (accessed February 27, 2017).

Garfield, M.J. (2005) Acceptance of ubiquitous computing. *Information Systems Management*, **22**(4), 24–31.

Gershenfeld, N. (1999) *When Things Start to Think*, Holt, New York.

Gubbi, J., Buyya, R., Marusic, S., and Marimuthu, P. (2013) Internet of Things (IoT): a vision, architectural elements, and future directions. *Future Generation Computer Systems*, **29**(7), S.1645–S.1660.

Hill, J., Horton, M., Kling, R., and Krishnamurty, L. (2004) The platforms enabling wireless sensor networks. *Communications of the ACM*, **47**(6), 41–46.

Hu, F. (2016) *Security and Privacy in Internet of Things (IoTs): Models, Algorithms, and Implementations*, CRC Press. ISBN 9781498723183.

Iansiti, M. and Lakhani, R. (2014) Digital ubiquity: how connections, sensors, and data are revolutionizing business. *Harvard Business Review*, November, 90–99.

IEC (2014) Internet of Things – Wireless Sensor Networks [White paper].

IEEE (2015) Towards a definition of the Internet of Things (IoT). Available at http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

IEEE (2017) Define IoT – IEEE Internet of Things. Available at http://iot.ieee.org/definition.html (accessed February 27, 2017).

ITU Internet Reports (2005) The Internet of Things.

Jeschke, S., Brecher, C., Song, H., and Rawat, D.B. (eds.) (2016) *Industrial Internet of Things*, Springer Series in Wireless Technology, Springer International Publishing, Cham.

Karzel, D., Marginean, H., and Tran, T. (2016) A Reference Architecture for the Internet of Things https://www.infoq.com/articles/internet-of-things-reference-architecture (Accessed March 14, 2017).

Kennedy, J.B. (1926) Woman is boss: an interview with Nikola Tesla by John B. Kennedy. Colliers Magazine. Available athttp://www.tfcbooks.com/tesla/1926-01-30.htm (accessed January 30, 1926; retrieved on January 29, 2017).

Kortuem, G., Kawsar, F., Sundramoorthy, V., and Fitton, D. (2010) Smart objects as building blocks for the Internet of Things. *IEEE Internet Computing*, **14**(1), 44–51.

Koyuncu, H. and Yang, S. H. (2010) A Survey of indoor positioning and object locating systems. *International Journal of Computer Science and Network Security*, **10**(5), 121–128.

Kranz, M., Holleis, P., and Schmidt, A. (2010) Embedded interaction: interacting with the Internet of Things. *IEEE Internet Computing*, **14**(2), 46–53.

Langheinrich, M. (2001) Privacy by design: principles of privacy-aware ubiquitous systems, in Abowd, G.D., Brumitt, B., and Shafer, S.A. (eds.), *Ubicomp*, LNCS 2201, Springer, pp. 273–291.

Laudon, K.C., Laudon, J.P., and Schoder, D. (2016) *Wirtschaftsinformatik: Eine Einführung*, 3rd completely revised edition (in German), Pearson, ISBN: 97838689-4269-9.

Leverett, E.P. (2011) Quantitatively assessing and visualizing industrial system attack surfaces. Ph.D. thesis, Computer Laboratory, Darwin College, University of Cambridge. Available at https://www.cl.cam.ac.uk/~fms27/papers/2011-Leverett-industrial.pdf.

Lyytinen, K. and Yoo, Y. (2002) Ubiquitous computing. *Communications of the ACM*, 45(12), S.62–S.65.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J., and Aharon, D. (2015) *Unlocking the Potential of the Internet of Things*, McKinsey & Company.

March, J.G. (1991) Exploration and exploitation in organizational learning. *Organization Science*, **2**, 71–87.

Mattern, F. and Flörkemeier, C. (2010) Vom Internet der Computer zum Internet der Dinge. *Informatik-Spektrum*, **33**(2), S. 107–121.

Mell, D. and Grance, T. (2011) The NIST Definition of Cloud Computing. Special Publication (NIST SP) – 800-145.

Minoli, D. (2013) *Building the Internet of Things with IPv6 and MIPv6: the evolving world of M2M communications*, John Wiley & Sons, Inc., New York.

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

Opensensors (2017) How to choose the best connectivity network for your project. Available at https://publisher.opensensors.io/connectivity (accessed February 15, 2017).

Perera, C., Zaslavsky, A., Christen, P., and Georgakopoulos, D. (2015) Context aware computing for the Internet of Things: a survey. *IEEE Communications Surveys and Tutorials*, **16**(1), 414–454.

Polsonetti, C. (2014) Know the difference between IoT and M2M. Available at http://www.automationworld.com/cloud-computing/know-difference-between-iot-and-m2m (retrieved December 4, 2016).

Porter, M.E. and Heppelmann, J.E. (2015) How smart, connected products are transforming companies. *Harvard Business Review*, **October**, 96–112, 114.

Poslad, S. (2009) *Ubiquitous Computing: Smart Devices, Environments, and Interactions*, John Wiley & Sons, Inc. Chichester, UK.

Postscapes (2017) IoT standards and protocols. Available at http://www.postscapes.com/internet-of-things-protocols/ (accessed February 27, 2017).

Roman, R., Zhou, J., and Lopez, J. (2013) On the features and challenges of security and privacy in distributed Internet of Things. *Computer Networks*, **57**(10), 2266–2279.

Rose, K., Scott, E., and Lyman, C. (2015) *The Internet of Things: An Overview—Understanding the Issues and Challenges of a More Connected World*, The Internet Society.

Sánchez López, T., Ranasinghe, D. C., Patkai, B., and McFarlane, D. (2011) Taxonomy, technology and applications of smart objects. *Information Systems Frontiers*, **13**(2), 281–300.

Sangiovanni-Vincentelli, A. (2014) Let's get physical: adding physical dimensions to cyber systems. Internet of Everything Summit, Rome, July 2014.

Schoder, D. Informationsmanagement 2.0 – Nur der Wandel ist stetig. *Wirtschaftsinformatik & Management*, Ausgabe Nr. **2011-02**. S.54–S.59.

Shin, D.-H. (2010) Ubiquitous computing acceptance model: end user concern about security, privacy and risk. *International Journal of Mobile Communications*, **8**(2), 169–186.

Sicari, S., Rizzardi, A., Grieco, L., and Coen-Porisini, A. (2014) Security, privacy and trust in Internet of Things: the road ahead. *Computer Networks*, **76**, 146–164. doi: 10.1016/j.comnet.2014.11.008.

Sudevalayam, S. and Kulkarni, P. (2011) Energy harvesting sensor nodes: survey and implications. *IEEE Communications Surveys & Tutorials*, **13**(3), 443–461.

Sun, Y., Ringfang, B., Peter, T., and Xiuthen, C. (2016) [Editorial] New advances in data, information, and knowledge in the Internet of Things. *Personal and Ubiquitous Computing*, **20**, 653–655.

Sundmaeker, H., Guillemin, P., Friess, P., and Woelffle, S. (2010) Vision and Challenges for Realising the Internet of Things. Cluster of European Research Projects on the Internet of Things, European Commision.

Uckelmann, D., Harrison, M., and Michahelles, F. (eds.), (2011) *Architecting the Internet of Things*, 1st edn, Springer.

Unify-IoT (2016) Supporting Internet of Things Activities on Innovation Ecosystems [H2020 – UNIFY-IoT Project; Deliverable D03.01]. Report on IoT platform activities. Available at http://www.unify-iot.eu/wp-content/uploads/2016/10/D03_01_WP02_H2020_UNIFY-IoT_Final.pdf (retrieved January 29, 2017).

Vermesan, O. and Friess, P. (2016) *Digitizing the Industry: Internet of Things Connecting the Physical, Digital and Virtual Worlds*, River Publishers Series in Communications, River Publishers.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I.S., Mazura, M., Harrison, M., Eisenhauer, M., and Doody, P. (2011) Internet of Things strategic research roadmap. *Internet of Things: Global Technological and Societal Trends*, River Publishers, pp. 9–52.

Weber, R.H. (2010) Internet of Things: new security and privacy challenges. *Computer Law & Security Review*, **26**(1), 23–30. doi: 10.1016/j.clsr.20 09.11.0 08.

Weinhardt, C., Anandasivam, C., Blau, B., Borissov, N., Meinl, T., Michalk, W. and Stoesser, J. (2009) Cloud computing: a classification, business models and research directions. *Business & Information Systems Engineering*, **1**(5), 391–399.

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

Weiser, M. (1993) Some computer science issues in ubiquitous computing. *Communications of the ACM*, **36**(7), 75–84.

Weiser, M. and Brown, J.S. (1996) Designing calm technology. PowerGrid Journal, v 1.01.

Weiser, M., Gold, R., and Brown, J.S. (1999) The origins of ubiquitous computing research at PARC in the late 1980s. *IBM Systems Journal*, **38**(4), S.693–S.696.

Welbourne, E., Battle, L., Cole, G., Gould, K., Rector, K., Raymer, S., Balazinska, M., and Borriello, G. (2009) Building the Internet of Things using RFID: the RFID ecosystem experience. *IEEE Internet Computing*, **13**(3), 48–55.

Weyrich, M. and Ebert, C. (2016) Reference architectures for the Internet of Things. *IEEE Software*, **33**(1), 112–116.

World Economic Forum (2015) Industrial Internet of Things: unleashing the potential of connected products and services.

Wortmann, F. and Flüchter, K. (2015) Internet of Things: technology and value added. *Business & Information Systems Engineering*, **57**, 221. doi: 10.1007/s12599-015-0383-3.

Wright, A. (2017) Mapping the Internet of Things: researchers are discovering surprising new risks across the fast growing IoT. *Communications of the ACM*, **60**(1), 16–18.

Yan, Z., Zhang, P., and Vasilakos, A.V. (2014) A survey on trust management for Internet of Things. *Journal of Network and Computer Applications*, **42**, 120–134. doi: 10.1016/j.jnca.2014.01. 014. http://dx.doi.org/10.1016/j.jnca.2014.01.014.

Zhang, Q., Cheng, L., and Boutaba, R. (2010) Cloud computing: state-of-the-art and research challenges. *Journal of Internet Services and Applications*, **1**, 7–18. doi: 10.1007/s13174-010-0007-6.