IoT: Science Fiction or Real Revolution?

Marco Furini[1], Federica Mandreoli[2], Riccardo Martoglia[2], and Manuela Montangero[2]

[1] Dipartimento di Comunicazione ed Economia
Universta di Modena and Reggio Emilia, Reggio Emilia, 42121, Italy,
marco.furini@unimore.it
[2] Dipartimento di Fisica, Informatica e Matematica
Universta di Modena and Reggio Emilia, Modena, 42121, Italy,
name.surname@unimore.it

Abstract. It's been many years since media began talking about the wonders of the IoT scenario, where a smart fridge checks the milk expiration date and automatically compiles the shopping list, but in the real life how many people have this smart fridge in the kitchen? Yet the interest around the IoT scenario is growing every day, so in this paper we try to figure out if IoT is science fiction or a real revolution. In particular, we describe in simple terms the IoT scenario, what can be done with current technologies, what are the main obstacles that limit the success and the wide use of IoT and we highlight directions that can make IoT a true reality.

Key words: Internet of Things, Smart Home, Smart City, Health-care, Retail Industry, Smart Factory

1 The IoT Scenario

In recent years, the term Internet of Things (IoT) is receiving considerable attention by governments, researchers, managers, media, etc. IoT refers to a scenario where people and physical objects (e.g., sensors, devices, etc.) are connected and able to communicate with each other with the result of transforming the physical world that surrounds us. Vehicles, home appliances, smartphones, home sensors, wearable sensors, environment devices are examples of objects that can be transformed into smart objects in order to be part of an IoT scenario. Indeed, by providing these objects with the ability to communicate, we allow them to capture and share data, we can control and analyze their actions to take decisions and to produce intelligent services able to transform our personal and professional life [1].

To clarify the idea, here is an example of how smart objects can change some everyday actions. In the morning, the alarm clock does not just wake us up, but it also turns on the coffee machine; the mattress turns on the room lights when we get up; the bathroom lights are switched on when we touch the door; television and lights are turned on when we go into the kitchen and the coffee machine begins pouring the coffee into the cup. Before going out,

the umbrella handle lights if rain is expected and when we close the door all the house lights go off and the blinds are lowered. In the evening, when we get home, the heating is turned on by our smartphone that uses the GPS to check whether we are close to home or not; the house lights are turned on when we open the door. This is just an example of how our private life will change thanks to IoT technologies, but the scenario is definitely wider: a city may become smart by using sensors and devices to monitor and manage traffic, to improve the efficiency of waste management, to plan urban and transportation changes; health-care may become smart by using sensors and devices to improve emergency services, to provide elderly assistance and medical aids; industries may use IoT to improve security in automotive transportation, to make logistics more efficient, to improve industrial automation; energy providers may use IoT to intelligently mange energy distribution [2, 3]. Needless to say, the IoT scenario is expected to transform every aspect of our life [3, 4, 5, 6, 7].

Millions of physical objects are being connected to the Internet [8] and several research reports agree that by 2020 the IoT scenario will include more than 20 billion of smart objects. These objects are enabled by several technological changes that caused, among others, a lowering of the production costs of sensors and devices, an increase of computational capacity and an ubiquitous networking coverage. In this scenario, objects are equipped with sensors and/or actuators and with suitable communication protocols that make them integral part of the Internet [4, 9]. To clarify, the IoT can be thought of as the interconnection of objects with the Internet, as shown in Figure 1. At objects level we have sensors that perform actions like "feel", "ear", "measure", "check" (i.e., sensors have different abilities like acoustic, liquid, temperature, pressure, force, etc.) and we have actuators that perform actions through electrical, hydraulic, pneumatic or mechanical movements. All these objects communicate with each other through sensor networks [8, 10, 11] that use data link protocols like NFC, RFID, LTE, Wi-Fi, Zigbee, etc., and communicate with the platform and with the application levels through Internet communication technologies.

Briefly speaking, the IoT architecture allows to extend today's Internet infrastructure with additional and innovative services. For this reason, different ICT consulting firms foresee an exponential growth of the IoT over the next few years. For instance, Gartner[1] forecasts that the IoT will generate revenue exceeding $300 billion in 2020, resulting in $1.9 trillion in global economic value-add through sales into diverse end markets; whereas [12] estimates that the whole annual economic impact caused by the IoT is in the range of $2.7 trillion to $6.2 trillion by 2025. The importance of this scenario is also highlighted by the amount of fundings that public governments are reserving to IoT research: the European Union is supporting different projects in the IoT area; the UK government, in March 2015, committed around €50 million to IoT research; Germany has earmarked up to €200 million to projects related to internet-based manufacturing; France reserves €50 million to digital development projects related to embedded software and connected objects [13].

[1] https://www.gartner.com/doc/2625419/forecast-internet-things-worldwide-

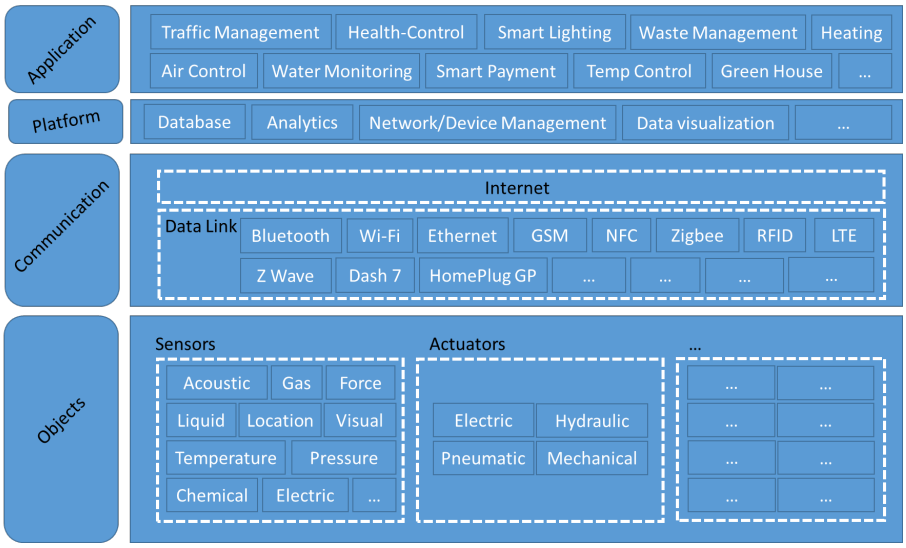

Fig. 1. The IoT archicture.

However, although many researches state that IoT technologies will affect several domains, there are some open issues like interoperability, security and privacy, that need to be addressed. In the following, after describing the most promising application domains for the IoT, we focus on these open issues and we provide some future directions that might help removing these burdens.

2 Fields of Applications

In recent years, academic and private researches proposed many different fields of applications for the IoT, from the well-know smart home to the less known smart agriculture. In all these fields of applications, the use of IoT aims to resolve in the rationalization of resources, and consequently monetary gain, while making the application field safer. Since it is useless to list all the IoT fields of application, in the following, we first describe two well-known IoT fields of applications and then we focus on three most promising ones.

Smart Home. Smart home is a firm and important field of application with a market expected to reach $121 billion by 2022 [14]. Comfort, security and energy efficiency are among the main benefits that a smart home can bring [15]. For instance, house owners might use their smartphone to control Wi-Fi enabled home electronics (e.g., appliances, heaters, hot water heaters, air conditioning, coffee machines, etc.) from anywhere, might increase home security (e.g., by using Wi-Fi connected cameras, sensors, and alarms) and might mange energy more efficiently (e.g., by using Wi-Fi outlets to turn off electronics when not in use). Gartner estimates that the number of devices and appliances currently

connected in our houses is about 600 million[2] including lighting, security and access control, heating and air conditioning managing, entertainment systems and smart kitchen.

Smart City. Smart cities market is estimated to grow from $52 billion in 2015 to $147 billion by 2020 [16]. Smarter utilization and deployment of public resources (e.g., lights, roads, parkings), better efficiency of services (e.g., garbage collection, public transport), better quality life (e.g., pollution and traffic control) and, in general, a reduction of wastes and costs for the public administration are among the main benefits that a smart city can bring [4]. For instance, simple objects equipped with LoRaWAN and Sigfox communication technologies can transform the act of parking, allowing citizens to detect available parking spots in an easy way. This would not only save citizens time, but it would also help to reduce pollution, thus improving the lives of citizens. Another example of how IoT can improve the lives of citizens is transforming the waste collection into smart collection: smart trashcans[3] monitor their content by means of GPS traceable wireless fill-level sensors and, when they need to be emptied, they send a real-time alert to the municipal services through LoRa, Sigfox and cellular networks. All reports are accessible by a Web secure platform that suggests the best (also from an economical point of view) collection route. Thus, waste collection can be rationalized avoiding too empty bins and preventing overflows in others.

Health-care. Medical and health-care are a very attractive application area for IoT [3] and the market is expected to create about $1.1 - $2.5 trillion in value by 2025 [12]. Cost efficiency, reliability and safety are among the main benefits that smart health-care can bring: patients monitoring might be done in remote and in real-time through the use of smart objects and sensors, smart objects might be used to replace human regular checks of patients vital signs, home health might be improved by issuing alerts if some irregularity is detected. For example, smart prescription bottles[4] have sensors that register actions on bottles (as opening, or reducing their content) and are rechargeable using a standard micro-USB port. Bottles use the cellular technology to (world wide) communicate with the servers of the service provider that check on the patient activity in real time. If the patient does not stick to his/her medical prescription and forgets to take his/her medications or takes an overdose, the patient is immediately alerted with land-line or cell phone calls, text messages, or caregivers. There also exist smart pills[5] that contain specifically designed ingestible sensors (approved by both the U.S. Food and Drug Administration and CE marked in the E.U.) that activate by contact with people stomaches at the time of ingestion and communicate with a matching sensor placed in a patch worn by the patient. The patch automatically logs the number, type and time when medications are taken, together with body vital signs (e.g. heart rate, body position, etc.). All these data are then shared,

[2] http://www.gartner.com/newsroom/id/3008917
[3] https://www.smartbin.com/
[4] https://adheretech.com/
[5] http://www.proteus.com/

via Bluetooth, with the patient mobile device through a specific app that stores the data on a cloud service accessible to the patient and his physician. It is thus possible to reduce costs and save time by letting smart objects do tasks that can be easily accomplished by machines, not to mention that the large set of collected data might be analyzed to gather new insights on patient health-care.

Retail Industry. The IoT retail market size is expected to reach $54 billion by 2022 according to a report by Grand View Research, Inc. Better customer experience, more efficient and secure supply chain and the development of new channels and revenue streams are among the main benefits that smart retail industry can bring. For instance, sensors can be used to track customers behaviors in order to better organize products placements; RFID can be used to track products in the supply chain [17] and to update in real time inventories information from off-the-shelves products; smart price tags can be used to change, in real-time, the product price based on demands, sales, etc.; smart codes can give customers more information about products, and sensors can be used to automate many functions that are manually performed [18].

Smart Factory. The smart factory market size is expected to reach $75 billion by 2020. In a Smart Factory [19], the manufacturing solutions exploit flexible and adaptive production processes, where the actors are equipped with enough computing and communication capabilities to give them an ability to act independently, without direct human intervention. For example, BMW has developed a tracking system based on RFIDs to enhance motor production and client customization. An RFID tag is attached to each engine as an unique identifier at the beginning of the assembly line and read at turn-points in the line to decide which way the engine should go (*e.g.*, lift or work station). Moreover, the tag brings along information about the customization of that specific car body, so that it is fast to recover and check information such as car color, internal details and door number. This brings to higher levels of automation, but also to optimizations in reducing unnecessary labor and waste of resources. The benefits could also go beyond the actual production of the goods. For instance, in a food supply chain scenario, IoT can enhance the whole process, from farms to processing plants, from processing plants to stores and from stores to consumers [17].

Although at first sight the above examples may look like a successful realization of IoT technologies, to a closer look they are just single IoT applications and do not represent a complete IoT scenario. Indeed, examples also showed one of the main problems that limits a successful employment of IoT technologies: the lack of interoperability between objects of the same scenario. For instance, a smart city is likely to have several different sub-networks (e.g., one for the sensors of the waste management system, one for the parking facilities, one for pollution measurement, etc.), each one working independently very well and suitable to provide an IoT service, but unable to interact with each other. Therefore, it is difficult to create a smart city. Indeed, there might be cities using many IoT applications, but these can not be labeled as complete smart cities. The

current IoT scenario reminds the networking scenario of the 70s, composed of many networks (e.g., milnet, nsf-net, cs-net, etc.) unable to communicate within each other. Another example is what is happening in the health-care scenario: we have many companies each building their successful IoT ecosystem, but these systems only communicate within themselves and do not interact among each other. Once again, this reminds the scenario of the 70s, when each computer company developed its own operating system that was unfortunately unable to interact with the others. The fragmented scenario of the 70s was virtually unified by the standardization of protocols and services provided by the Internet and the Web. As discussed in the following section, likely, it is necessary to follow a similar path to make the IoT a successful scenario.

3 Open Issues and Future Directions

The IoT might open a wide new world of opportunities to offer new services to users, in many different forms, but for an actual large-scale employment it is still necessary to address some important open issues, including the ones related to interoperability, security and privacy, and devising new business models.

3.1 Interoperability

IoT objects and devices are produced by different vendors, have different technical characteristics and specifications (*e.g.*, smartphones are very different from simple RFID tags), use different communication protocols (Zigbee, Bluetooth, Bluetooth Low Energy, Wi-Fi, GSM, 3G and LTE, just to name few), and are often integrated with other heterogeneous sources of information. This heterogeneity is a big issue: on the one side, producers that want to invest do not have clear indications on standards to adopt when developing IoT products and do not know for how long their products will last on the IoT market; on the other side, users who want to buy IoT products do not know for how long these will be compatible with the upcoming IoT scenario.

Open standards seem to be the right answer to these problems, as they can give clear guidelines to create a competitive environment for companies to deliver quality products. The IEEE Standards Association (IEEE-SA) already started a process to develop open standards for the IoT[6] and even some private companies (*e.g.*, AllSeen Alliance) are contributing (and asking for contribution) to create open source frameworks to design common standards so that different devices might communicate between themselves, regardless of their brand, category and technical equipment. Needless to say, once open standards are defined, producers should be enforced to apply these standards (*e.g.*, identifying appropriate SLA, Service Level Agreements, for each service) in order to make human users trust new services offered through the IoT.

[6] http://standards.ieee.org/innovate/iot/projects.html

In addition, the traditional Internet architecture needs to be revised to match the IoT challenges, both at low and high level. One main reason is the tremendous number of objects willing to connect to the Internet: 2010 has seen the surpass of the number of objects connected to the Internet over the earth's human population [8] and we have to expect that the former number is going to increase terrifically in the near future. Thus, we also have to expect a great increase of the traffic on the Internet, incurring into possible delays and in an increase of bandwidth request. Therefore, to allow IoT scalability, IPv6 and new generation of communication protocols (*e.g.*, 5G is to provide speed between 10-800Gbps, compared to the current technology 4G with speed of 2-1000 Mbps) seem to be mandatory.

There are also issues of interoperability at the platform level, concerning the need of integrating raw data coming from IoT objects with static and historical data stored in databases or accessible through Web services. For instance, let us consider a smart city control center that offers various cutting-edge services such as smart parking and dashboard view [20]. To this end, it is necessary to integrate heterogeneous information coming, for instance, from On Board Units and/or smartphones and multi-sensor weather stations together with official data available on Web sites, predictions on weather and traffic, tube schedules, etc. Indeed, information integration has been recognized as a key (and costly) challenge faced by large organizations today [21]. It is also well understood that information integration is not a single problem but, rather, a collection of interrelated problems that are addressed under the umbrella of architectures and unified data models. These problems include extracting and cleaning data from the sources, transforming data from the sources into data conforming with the unified format, and answering queries over the unified format. A possible answer to these problems is the dataspace paradigm [22], an emerging approach in the information integration agenda. In a dataspace, data coexist while the actual integration efforts are faced when needed. This paradigm might represent a good answer to the problem of interoperability for IoT because of the high level of heterogeneity of the involved information sources and the need of a large scale deployment. To this end, open source platforms might be used to facilitate the development of IoT applications through plug-in services for push/pull data connection and integrated view creation and maintenance.

3.2 Security and privacy

One of the main advantages of IoT is the possibility to gather large sets of data that, properly analyzed, give information that can be used to provide better services. However (and again), issues arise: being connected to the Internet (and often unattended), objects are possible target to a wide range of security attacks that can lead to data leakage and/or data manipulation. Some recent examples of security issues include: a smart doorbell receiving the video feed from someone else house, people taking unauthorized control of the security system of specific buildings (e.g., houses, banks, factories, etc.), attackers compromising on-line car systems and stopping/speeding up cars with malicious intent. If customer

are expected to use IoT technology and products, they must be assured that no accidental and/or malicious behavior might loose, steal or manipulate their data.

In the IoT scenario, security solutions cannot be limited to the single object or device, but they must be end-to-end solutions, going from the application level to the object level and vice-versa. Again, the heterogeneity of IoT interacting objects further complicates matters as different objects require different security levels (*e.g.*, fitness wearables vs. health care applications). Given such an extremely heterogeneous and vulnerable scenario, it is fundamental to provide security solutions at least for the following problems: *authentication* (any object involved in a communication must be clearly and uniquely identified); *confidentiality* (data must be secure and available only to authorized entities); *integrity* (data must not be altered by anyone when traveling from one point to another, or while stored in some database); *fault-tolerance* (even in the presence of a fault, security services must be continuously provided).

In addition to security, privacy plays an important role. Consider for instance the case of a person wearing a smart wrist collecting data such as heart rate, blood pressure, etc. One can imagine that the customer expects these data to be used to improve his/her personal performances or for self-usage check ups, but surely not that these data might become available (without his/her allowance) to his/her health insurance and used to tune the insurance policy cost or even to deny the policy. In the Internet scenario, consumers are becoming more and more aware that data are now trading currencies for services (let's just think at Gmail or Facebook), and, since most of the collected data are personal and sensitive, users are increasingly interested in their privacy [23, 24]; the lack of clarity about who has access to data may limit the growth of the IoT scenario. Possible solutions to these privacy issues are new policies reassuring customers that data do not concern individuals but aggregates, clarifying the use of data, for how long these data are stored, and who has access to them.

3.3 Business

The lack of clear, widely accepted and successful business models, of use cases and of return of investment examples are slowing down the adoption of the IoT [25].

Although there are some early players that successfully invested in IoT (e.g., companies in the fitness and/or smart home scenarios), most of the companies are still thinking whether to enter or not in the IoT, because the scenario has characteristics that limit the development of a solid business model. According to [26], there are three main reasons that limit the design of a generic and successful IoT business model: i) diversity of objects, ii) immaturity of innovation, and iii) unstructured ecosystem. The diversity of objects and the immaturity of innovation cause the employment of several different proprietary platforms and end-to-end IoT solutions, whereas the unstructured ecosystem causes doubts to investors because the scenario is too chaotic, just like the Internet was in the mid-90s.

The solution to these problems is closely dependent on the solution of the problems highlighted above. In particular, it is fundamental to first address the problems related to interoperability and security, as this would make available IoT communication standards and IoT end-to-end security solutions. These solutions could be the building blocks on which to build solid business models for the IoT scenario.

4 Conclusions

The interest around the IoT scenario is enormous, billions of objects/devices are being connected to the Internet to create the biggest network we have never seen, opening the possibility to create a new world of services in extremely different fields of application that can be offered to users by using the information that these devices can gather. Examples of how these smart objects can change the way we live and/or we work are written everywhere, from technological blogs to mass-media newspapers. Since it's been many years since media began talking about the wonders of IoT technologies, in this paper we tried to figure out if the IoT scenario is science fiction or a real revolution. We observed a very fragmented scenario that might compromise the successful employment of IoT: proliferation of communication technologies, absence of end-to-end security solutions and of solid business models that are able to guarantee a profitable return of investments. We also observed, by looking at some IoT examples, the benefits of IoT technologies, and we are positive about the fact that IoT may improve citizens life quality. Finally, since we are deeply convinced that a real employment of IoT passes through the unification (either virtual or not) of the fragmented scenario, we proposed some guidelines that move the IoT towards this direction.

References

1. R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan. Internet of things (iot) security: Current status, challenges and prospective measures. In *2015 10th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 336–341, Dec 2015.
2. P. Bellavista, G. Cardone, A. Corradi, and L. Foschini. Convergence of manet and wsn in iot urban scenarios. *IEEE Sensors Journal*, 13(10):3558–3567, Oct 2013.
3. S. M. R. Islam, D. Kwak, M. H. Kabir, M. Hossain, and K. S. Kwak. The internet of things for health care: A comprehensive survey. *IEEE Access*, 3:678–708, 2015.
4. A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi. Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1):22–32, Feb 2014.
5. Marco Roccetti, Stefano Ferretti, Claudio Palazzi, Paola Salomoni, and Marco Furini. Riding the web evolution: From egoism to altruism. In *2008 5th IEEE Consumer Communications and Networking Conference*, pages 1123–1127, Jan 2008.
6. Stefano Ferretti, Marco Furini, Claudio E. Palazzi, Marco Roccetti, and Paola Salomoni. Www recycling for a better world. *Commun. ACM*, 53(4):139–143, 2010.

7. Manuela Montangero and Marco Furini. Trank: Ranking twitter users according to specific topics. In *Consumer Communications and Networking Conference (CCNC), 2015 12th Annual IEEE*, pages 767–772, Jan 2015.
8. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash. Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys Tutorials*, 17(4):2347–2376, Fourthquarter 2015.
9. Luigi Atzori, Antonio Iera, and Giacomo Morabito. The internet of things: A survey. *Comput. Netw.*, 54(15):2787–2805, October 2010.
10. Luciano Bononi, Lorenzo Donatiello, and Marco Furini. Real-time traffic in ad-hoc sensor networks. In *Proceedings of IEEE International Conference on Communications (ICC))*, pages 1–5, 2009.
11. Lorenzo Donatiello and Marco Furini. Ad hoc networks: A protocol for supporting qos applications. In *Proceedings of the 17th International Parallel and Distributed Processing Symposium (IPDPS 2003)*, April 2003.
12. James Manyika, Michael Chui, Jacques Bughin, Richard Dobbs, Peter Bisson, and Alex Marrs. Disruptive technologies: Advances that will transform life, business, and the global economy. Technical report, 2013.
13. Ron Davis. The internet of things. *European Parliamentary Research*, May 2015.
14. marketsandmarkets.com. Smart home market by product, security & access control, hvac, entertainment, home healthcare and smart kitchen, software & service and geography - global forecast to 2022. Technical report, 2016.
15. Muhammad Alam, Bin Reaz, and Mohd Ali. A review of smart homes - past, present, and future. *IEEE Transactions on Systems, Man, and Cybernetics*, 2012.
16. marketsandmarkets.com. Internet of things (iot) in smart cities market by solutions platform application - global forecast to 2020. Technical report, 2016.
17. Xiaorong Zhao, Honghui Fan, Hongjin Zhu, Zhongjun Fu, and Hanyu Fu. The design of the internet of things solution for food supply chain. In *International Conference on Education, Management, Information and Medicine*, 2015.
18. Marco Furini and Claudia Pitzalis. Smart cart: when food enters the IoT scenario. In *Internet of Things*, volume 169. Springer International Publishing, 2016.
19. Branko Katalinic, Agnieszka Radziwon, Arne Bilberg, Marcel Bogers, and Erik Skov Madsen. International symposium on intelligent manufacturing and automation, 2013 the smart factory: Exploring adaptive and flexible manufacturing solutions. *Procedia Engineering*, 69:1184 – 1190, 2014.
20. Luca Carafoli, Federica Mandreoli, Riccardo Martoglia, and Wilma Penzo. A data management middleware for ITS services in smart cities. *J. UCS*, 22(2):228–246, 2016.
21. Philip A. Bernstein and Laura M. Haas. Information integration in the enterprise. *Commun. ACM*, 51(9):72–79, 2008.
22. Michael J. Franklin, Alon Y. Halevy, and David Maier. A first tutorial on dataspaces. *PVLDB*, 1(2):1516–1517, 2008.
23. Marco Furini and Valentina Tamanini. Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. *Multimedia Tools and Applications*, 74(21):9795–9825, 2015.
24. Marco Furini. Users behavior in location-aware services: Digital natives vs digital immigrants. *Advances in Human-Computer Interaction*, 2014, 2014.
25. Andres Laya, Vlad-loan Bratu, and Jan Markendahl. Who is investing in machine-to-machine communications? In *Proc. of the ITS Conference*, 2013.
26. Mika Westerlund, Seppo Leminen, and Mervi Rajahonka. Designing business models for the internet of things. *Technology Innovation Management Review*, 4:5–14, 07/2014 2014.