The Internet of Things: Opportunities, Challenges, and Social Implications of an Emerging Paradigm

Ulrika H. Westergren

The Internet of Things: Opportunities, Challenges, and Social Implications of an Emerging Paradigm

Ulrika H. Westergren [0000-0001-7349-6818]

Department of Informatics, Umeå University, Sweden
ulrika.westergren@umu.se

Abstract. The Internet of Things (IoT) is an ongoing technological revolution where ordinary objects are fitted with sensing capability and connected to the Internet. The number of smart and connected devices is increasing exponentially, creating an arena for both product and service innovation. Research on the IoT has to date focused mainly on the technology itself, with less attention being directed toward the potential for value creation and the social implications of this phenomenon. This essay examines that gap and takes a look at the emergence of IoT from a social perspective. Addressing both the private and public sectors, it takes a look at opportunities and challenges associated with IoT implementation and use and discusses implications for a number of different actors. In addition, it shows how IoT is connected to a strong discourse on security, privacy and ethical use of technology and offers suggestions for future research directions grounded in IoT as being a current example of the ongoing digital transformation of society.

Keywords: Internet of Things, Digital Transformation, Value Creation, Social Implications.

1 Introduction

Over the past 20 years we have witnessed the dawning of a new digital era, where information technology has become smarter, faster, smaller and cheaper and, as a result, an integral part of our daily lives. The exponential growth of the Internet of Things (IoT), where ordinary objects are embedded with sensors and Internet connectivity, has moved the frontlines for what ICT is, does, and facilitates, and serves as a key enabler of the digitalization of society (Krotov, 2017). Encompassing everything from smart homes with intelligent lighting, remote-controlled thermostats and advanced home security systems, to health care applications, personal monitoring devices and fitness trackers, as well as solutions for smart agriculture, connected vehicles, and industrial applications where product and process data are collected and analyzed for logistical, strategic, and product-development purposes, the IoT creates vast opportunities for both product and service innovation. These opportunities are based on the availability of real-time, context-aware data. For example, a smart object can transmit information about its exact location, usage, and condition, and programmed to send alerts if values deviate from a set norm. This means that maintenance needs and product failures can

be addressed as soon as they arise. However, the collected data can also be analyzed to find patterns and behaviors over time, and if combined with data from other connected products, IoT data can be used to make data-driven strategic decisions about whether a product should be updated, service performed, or a process optimized. In fact, this type of analysis makes it possible to make predictions about future behavior and foresee an incident before it actually occurs. In addition, real-time data can be collected and analyzed and used in the development of new products and services; during the procurement of services; or as input to ecosystems of IoT-suppliers that cooperate and jointly create value for their customers. The IoT thus enables situation-specific and efficient handling of both products and processes, based on data and actual needs instead of predefined variables, such as specified time intervals. It comes as no surprise then, that the public and private sectors alike are scrambling to take advantage of the opportunities enabled by this new technological paradigm.

In order to do that, one needs a clear understanding of what the IoT is, what types of value it is likely to produce in different contexts, as well as a thorough consideration of the opportunities and challenges associated with sensor-based systems. The previous forecasted growth figures of 20 billion connected objects by the year 2020 have already been surpassed and new measures mention numbers of up to 75 billion connected objects in 2025 (Statista.com, 2020). This chapter takes a deeper look at the implications of the IoT and its effects on public- and private sector value creation, privacy and security. It draws on current research on IoT and highlights the social aspects of the technology. As both people and devices continue to move online, markets are predicted to transform and grow, creating an increase in innovations, productivity gains and economic growth. In addition, public organizations may take advantage of IoT to create value for citizens and make efficient use of public funding. The combination of technological advancements and new business logic makes the IoT a powerful and transformational force to be reckoned with for the private and public sector alike.

2 IoT Architecture

A fundamental building block of IoT is of course the technological components. Smart technology in itself is no novelty, and for example RFID-tags have been used for decades to identify and track specific objects (Gubbi, Buyya, Marusic & Palaniswami, 2013). However, miniaturization has made it possible to embed technology within a diverse range of objects and with the cost of technology going down, and the capacity going up, the number of smart objects is increasing exponentially. A smart object is defined as "an autonomous, physical digital object augmented with sensing/actuating, processing, storing, and networking capabilities" (Fortino & Trunfio, 2014). These smart objects form the basis of the IoT.

A simple conceptualization of IoT architecture is the three-layer architecture described by Lin et al. (2017). At the bottom we find the perception layer with smart objects, where there are sensors and actuators that capture context-aware data from physical objects. This is followed by the network layer, which consists of both connec-

tivity devices, protocols, and communication- and network technologies. Wireless networks that are short-range (such as Bluetooth, RFID, and Zigbee), medium-range (such as Wi-Fi and zWave), and long-range (such as LPWAN and VSAT) are being actively developed for IoT connectivity. Low power wide area networks (LPWAN) provide low cost, low-rate, long-range radio communication and leading technologies are Sigfox, LoRa, and NB-IoT (Mekki, Bajic, Chaxel & Meyer, 2019). The network layer receives data from the perception layer and transmits it further to or from devices and IoT applications. At the top, we find the application layer, which receives data transmitted from the network layer and uses it to perform operations or services. This basic architecture contains complex operations and some researchers have therefore suggested adding additional layers, for example a service/middleware layer between the network and application layers (Jin et al. 2017), and a business layer on top of the application layer, responsible for the management of the overall IoT system (Khan, Khan, Zaheer & Khan, 2012), to the architecture to better capture its complexity.

Once up and running, IoT devices are dependent on efficient power consumption in the form of reliable, long lasting batteries. As organizations start to implement IoT strategies at the core of their processes, systems must be able to deliver a continuous stream of real-time data. Unreliable devices could be detrimental to business, and the cost of constantly changing batteries would deplete the potential savings made by using IoT. Many IoT devices have batteries that last between three and ten years, but battery life remains a crucial question and there is ongoing research, both on battery technology development, but also on alternatives such as energy harvesting technology and remotely charging batteries, through for example Wireless Power Transfer (Torun et al. 2018).

IoT technology must meet high performance needs and ensure scalability and flexibility. The rapid rate of innovation has led to a multitude of different IoT solutions being simultaneously developed by different providers. However, due to a lack of common standards, each solution being developed is connected to its own set of various choices made in regard to architecture, APIs, devices, data formats, etcetera, which in turn causes interoperability problems (Noura, Atiquzzaman & Gaedke, 2019). Such interoperability issues may push businesses into vendor lock-ins and make it difficult to develop cross-platform IoT or to connect different systems to each other. The lack of agreed upon industry standards creates an uncertainty regarding “making the correct choices” and creating sustainable and interoperable IoT systems that will be able to function with other IoT systems. This ultimately prevents large-scale IoT where all smart objects can potentially be connected to each other and is seen, together with efficient energy consumption, as one of the big questions that has to be resolved in order for IoT to continue to grow and create value.

3 Creating value with IoT

The digitization of the physical world holds much untapped business potential (Brynjolfsson & McAfee, 2014). Previous research has shown that as technology is coming to permeate almost every aspect of our lives, firms must form strategies that

make use of the ongoing technical developments and combine them with new business logic in order to stay relevant to their customers (Saarikko, Westergren & Blomquist, 2017). In light of the rapid technological development, it has been suggested that managers need to develop the capacity to *sense*, *assess*, and *respond to* change (Haeckel, 2010). Strategically working with IoT thus incorporates asking questions about 1) How to create knowledge about technological developments, the research frontier and value creation potential? (sensing), 2) How to identify and evaluate IoT-value? (assessing), and 3) How to use and incorporate this knowledge into business processes? (responding). In addition, the speed of technological progress not only drives change, but also increases complexity and places high demands on finding staff with appropriate skills (Bullen, Abraham & Galup, 2007). Many firms are not able to deliver all competence in-house and therefore find it beneficial to participate in networks, forming ecosystems of firms, where mutual efforts reduce complexity and increase benefits for all participating actors (Teece, 2010). When entering into such arrangements, firms must reflect upon their role in the ecosystem and how the firm's identity is related to that role. There will be firms who supply the technology needed to implement IoT solutions, those who embed IoT into their products and services and offer new forms of value creation, and those who create entirely new services based on what the technology affords (Burkitt 2014; Westergren, Saarikko & Blomquist, 2018).

As these different types of firms come together, new and innovative IoT solutions and applications will be developed. Indeed, IoT solutions are used to enable the intelligent home, that is receptive to its residents' preferences and habits and offers a personalized smart living experience. IoT home automation solutions include controls for, lighting, entertainment, appliances and security. Furthermore, one sees the opportunity to use IoT to create data-driven insurance services for the safe home, where premiums and offers are linked to individuals' behavioral patterns and use nudging tactics to push for behaviors that are advantageous. Another area for IoT ecosystem innovation is the automotive industry, where IoT solutions may bring together such disparate actors as car manufacturers, insurance firms, and entertainment hubs. The possibility of incorporating IoT in cars and measuring a large amount of data points (Bian, Yang, Zhao & Liang, 2018; Husnjak, Peraković, Forenbacher & Mumdziev, 2015), makes it possible to relay vehicle data back to the manufacturer, download updates, and schedule repairs and maintenance as needed, as well as enables so-called usage-based insurance (UBI) where the insurance premium is based directly on the driver's behavior. The same data can also be fed back to the driver for the purpose of promoting eco-friendly and safe driving (Soleymanian, Weinberg & Zhu, 2019). In addition, IoT can be used to provide Wi-Fi onboard and entertainment services for passengers. A third example is the connected workplace where steady access to context-aware data can serve as the basis for climate control, efficient cleaning services, and intelligent lighting, providing the individual worker with a customized indoor climate and a more efficient workday (Mähler & Westergren, 2018). Being part of such an ecosystem comes with challenges of its own, as firms must collaborate with others in order to create business value and are thereby also subjected to others' time schedules, expectations and processes. A key to succeeding in ecosystems is thus creating organizational strategies that explicitly ac-

count for challenges associated with collaborative networks (Adner, 2006). This includes ideas on how to build trust among network partners and create a context that allows for both alignment of interests and adaptation to emerging conditions (Westergren, Holmström & Mathiassen, 2019).

The data that is captured, stored, and transmitted through IoT is at the heart of IoT value creation. In the private sector, service business firms mainly motivated by the possibility to increase process efficiency and to create efficient, customized services based on data analysis. They also see the potential in using accumulated data to better understand their customers and thus gain a competitive advantage when negotiating new contracts (Westergren et al., 2018). Manufacturing firms that incorporate IoT into their existing products see an opportunity to use data to reduce machine downtime, improve product quality and customer relations, as well as enhance supply chain efficiency (Dai et al., 2019). IoT provides a possibility to efficiently monitor products and offer context-based services after the point of sale (Baines and Lightfoot, 2014; Kortuem, Kawsar, Fitton & Sundramoorthy, 2010). A deeper understanding of a product in use can prevent costly unplanned stops and product failure and enable the service organization to adapt its business model to the benefit of both the supplier and customer (Brax & Jonsson, 2009). The move toward data-driven services, and the possibility to make informed decisions based on real-time contextual data, paves the way for proactive instead of reactive services and opens up for deeper levels of analyses (Tao, Qi, Liu & Kusiak, 2018). However, although access to data is seen as crucial, many firms lack the skills and analytical capabilities needed to use it for other purposes than quite basic anomaly detection and control. In order for firms to obtain greater value from IoT data and move toward prediction and optimization, they both need to develop analytical skills and resolve technical challenges regarding for example data acquisition, data preprocessing and storage, and data analytics, that need to be overcome (Dai et al., 2019).

The majority of IoT initiatives have thus far been implemented in the private sector, but studies show that IoT adoption is increasing within the public sector as well (Borgia 2014; Neirotti et al. 2014; Saarikko et al. 2020). Under constant pressure to simultaneously lower costs and increase citizen value, the application of IoT in the public sector is mainly motivated by the possibility to improve efficiency, increase transparency and enhance public services (Saarikko et al. 2020). It is therefore not surprising to see that implemented solutions often focus on areas that are connected with high maintenance costs, such as infrastructure, utilities, transportation, and facility management and on services that are directly addressing citizen needs, such as various applications for health- and self-care. IoT enables in-home health care, where outpatients can continuously monitor their own condition, while staying connected to their health care provider (Delmastro, 2010; Pang et al., 2015) In addition, IoT may also support elderly or disabled citizens with assisted living solutions, where connected pressure pads can detect falls, and smart pill boxes can assist with medication adherence (Abbey et al., 2012). Public sector use of IoT also entails many smart city solutions, such as smart buildings with sensor-controlled ventilation and efficient power consumption, smart waste management, intelligent street lighting, smart parking solutions and more. Furthermore, there are IoT solutions that focus on citizen safety and continuously monitor urban environments as an aid to police in their work. Indeed, the incorporation of IoT into the

public sphere can provide more efficient and effective public services as well as encourage citizen participation. A challenge for this sector, however, is to find the economic space for innovation in a context often characterized by cost savings, which shows the importance of building a solid business case.

4 IoT challenges

We have seen how IoT enables innovation in both the private and the public sector and that there are many different ways in which IoT can create value. However, there are also a number of challenges that must be overcome in order for IoT to deliver on its promises. Some have already been mentioned, like the lack of common standards, battery life, problems of interoperability, scalability issues and other technological considerations. IoT data is often messy and comes from a range of heterogeneous sources which brings forth questions of data integration, reducing data redundancy and cleaning data, as well as data transmission and analysis (Dai et al., 2019). This creates a complex landscape for organizations looking to incorporate IoT into their processes and sets expectations concerning technical know-how. However, decisions about IoT investments are often made by managers who, while extensively trained to make business assessments, are not usually equipped to make decisions that require extensive and deep knowledge of emerging technologies. Poor understanding of the technological dimension may lead to investment in narrow, proprietary solutions and enhance the interoperability problem, as isolated solutions create challenges in accessing, sharing, and reusing data in different services and contexts. In order to avoid vendor lock-ins or being stuck with ill-fitting solutions, many therefore choose to partner with firms that can provide both private and public sector organizations with the technological expertise needed to make choices about sensors, connectivity, application- and IoT platforms, and IoT standards (Saarikko et al., 2017). By teaming up with trusted partners in IoT ecosystems, organizations can thus make use of network competence and overcome challenges related to a lack of technological competence.

The decision to invest in IoT is not only about making technology choices, it is about building a proper business case, that clearly states *what* problems IoT is expected to solve, *how* the application of IoT will provide value, and *for whom*. By identifying IoT application areas, it is also easier to map out what potential value might be created and where the pitfalls are. The implementation of IoT within the public sector differs from IoT usage within the private sector in a number of ways. A challenge for any public organization is to create economic spaces for innovation when daily activities most often are characterized by cost savings. Public sector IoT value creation thus often focuses on improving efficiency, increasing transparency, developing public services, and enhancing the quality of life for citizens- actions that directly or indirectly cater to citizens' needs. Private sector use of IoT, on the other hand, is about increasing profit, capturing market shares, and creating value for customers. Furthermore, firms in the private sector normally have a well-defined customer base as opposed to the public sector where needs of citizens of all ages, capabilities and interests must be included and addressed. This creates a complex and dynamic innovation landscape, which

should be acknowledged and accounted for in each new IoT project. Despite the growing number of IoT ecosystems and partnerships, many IoT solutions are being developed in-house, and in the public organizations, often in projects financed by external funds. A challenge for project based IoT innovation is to move from short term project activities to long term sustainable solutions that become an integrated part in daily operations.

Another major challenge is ensuring IoT security. IoT devices are easily accessible and often have limited built-in security features. The possibility of data leakage and node compromising is high (Jing et al., 2014) and the more IoT is incorporated into products, services and processes, the more one opens up for the possibility of malicious attacks and malware. Distributed denial-of-service attacks may use botnets to infiltrate ordinary smart home objects, causing networks to overflow and services to crash (Bertino & Islam, 2017). Hackers may take control over self-driving cars or disrupt critical IoT healthcare solutions (Yang et al., 2017), and ransomware attacks can be used to interrupt industrial IoT applications causing standstills or production failure. Ultimately human safety could be at risk. Making security a priority should thus be essential for any IoT project. Due to the heterogeneous nature of IoT systems and their inherent design that encourages flexibility and scalability, traditional security measures are often insufficient. Since IoT systems are too dynamic and too complex to benefit from a "one solution fits all"-package (Sicari, Rizzardi, Grieco & Coen-Porisini, 2015), there is a call for customizable IoT security architectures, that are carefully tailored to meet specific application needs, while at the same time ensuring a systematic and grounded approach to IoT security (Jing et al., 2014). Previous research shows how issues such as authentication and authorization, privacy and confidentiality, and secure communication and computation must be addressed before, during and after IoT implementation (Alaba, Othman, Hashem & Alotaibi, 2017; Li, Yan & Chang, 2018). By defining needs and balancing the potential for value creation with the prospect of putting themselves and their customers at risk, organizations can prepare to use IoT in a safe and secure way. This includes asking questions regarding what needs to be protected and for how long, who has access to data, how will data be communicated, what standards will be used, and how accessible and simple to use should the IoT system be? In order to make sure all parts of the system are protected secure solutions must then be implemented at all layers of the IoT architecture (Sicari et al., 2015). IoT system failure can be detrimental to business and poorly developed IoT security can deplete not only company assets but also customer trust. Finding ways to ensure IoT security thus remains one of the major challenges with IoT

Smart solutions affect their surroundings. By constantly capturing, collecting and communicating data, IoT can be used to customize environments and offer services based on individual preferences. However, as more and more objects become connected to each other and to the Internet, there is also a potent risk of privacy infringements for example through identification, localization, tracking, and profiling (Ziegeldorf, Morchon & Wehrle, 2014). Ensuring privacy and an ethical use of data is thus a central concern for IoT adopters, making sure personal and potentially sensitive data do not end up in the wrong hands (Perera et al., 2020), or are wrongly interpreted and misused. Context-aware data can be used to track, monitor, and map out individual behaviors

and patterns not only of objects, but of humans in proximity to smart objects, without them even being aware of this happening. For example, the use of room occupancy sensors to control indoor climate can be an efficient solution that saves energy and provides individuals with optimized working conditions. However, the same sensors could be used to discern who stays in their office at their desk, and who spends a lot of time by the coffee machine, effectively transforming climate control into a surveillance tool. In such a scenario, it is of the utmost importance to reflect not only on what IoT can do and what patterns can become visible through the analysis of real-time contextual data, but also on what is desirable, necessary, and ethically justifiable. This requires being able to balance the perceived benefits of transparency (from the perspective of the observer) with the risks of privacy infringements (from the perspective of the observed) enabled by smart technology (Bernstein, 2017). As IoT continues to grow in scope and pervade all aspects of human life, new privacy threats such as privacy-violating interactions and presentations, lifecycle transitions, inventory attacks, and information linkages will surface, and the need for privacy-aware IoT applications will increase (Ziegeldorf et al., 2014; Perera et al., 2020). A successful implementation of IoT technology whether it be in the private or public domain, must therefore consider the privacy implications and possible ethical consequences of IoT use.

5 Summary and conclusions

The IoT is only in its infancy. The growth thus far has been exponential and shows no signs of waning. As our world gets connected the potential for innovation is immense, and future IoT developments are projected to have an even more transformational impact on society. The research community has largely focused on the technological implications of IoT. This essay positions IoT as a socio-technical phenomenon and presents a number of opportunities and challenges that both private and public organizations face when engaging with IoT. By tracing the progress trajectory of IoT we can see certain patterns that emerge. First, **technological knowledge** is becoming a central concern for all types of organizations. In order to keep up with the rapid rate of digital innovation, organizations must develop an ability to sense, assess, and respond to technological change, either by developing skills in-house or by teaming with partners that can provide them with new competence. Second, a clear idea of **value creation** should be at the heart of all IoT investments. By building a business case and considering not only what IoT can do, but what value it will create and for whom, IoT moves from being just another technological phenomenon to a transformational power with the potential to cause long lasting change. Third, **security issues** threaten to hamper IoT development. Due to the complex and dynamic nature of IoT, security solutions need to be customized to the specific context, and many organizations find it hard to gain an overview of all potential risks and threats. Ranging from annoying (as in someone remotely turning lights on and off) to potentially life threatening (if said lights are traffic lights and unauthorized remote access may cause lethal accidents), IoT security issues must be swiftly identified and dealt with, to ensure safety and to build trust. Fourth, IoT enables unprecedented amounts of data to be generated, collected and analysed. While

data can be used to increase transparency, improve efficiency, and enhance efficacy, the apparent risk of misuse, for example, unwarranted tracking and profiling means **privacy and ethics** must be on the agenda. A secure, responsible, and ethical use of IoT has the potential to transform society and provide value far beyond that found in ordinary technological innovation. Further research should therefore address IoT as an integral part of the ongoing digital transformation of society and take a deeper look at implications for both individuals and organizations. By conceiving of IoT as a technological, social, and cultural phenomenon, we can begin to understand its full potential and create strategies to account for both opportunities and challenges, as well as social implications, of this emerging paradigm.

References

1. Abbey, B., Alipour, A., Gilmour, L., Camp, C., Hofer, C., Lederer, R., & Sadowski, C. (2012, June). A remotely programmable smart pillbox for enhancing medication adherence. In *2012 25th IEEE International Symposium on Computer-Based Medical Systems (CBMS)* (pp. 1-4). IEEE.
2. Adner, R. (2006). "Match your innovation strategy to your innovation ecosystem." *Harvard business review* 84 (4), 98–107.
3. Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*, 88, 10-28.
4. Baines, T. and Lightfoot, H.W. (2014), "Servitization of the manufacturing firm: Exploring the operations practices and technologies that deliver advanced services", *International Journal of Operations and Production Management*, Vol. 34, No. 1, pp. 2-35.
5. Bernstein, E. S. (2017). Making transparency transparent: The evolution of observation in management theory. *Academy of Management Annals*, *11*(1), 217-266.
6. Bertino, E., & Islam, N. (2017). Botnets and internet of things security. *Computer*, *50*(2), 76-79.
7. Bian, Y., Yang, C., Zhao, J. L., & Liang, L. (2018). Good drivers pay less: A study of usage-based vehicle insurance models. Transportation research part A: policy and practice, 107, 20-34.
8. Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, *54*, 1-31.
9. Brax, S. A. and Jonsson, K. (2009), "Developing integrated solution offerings for remote diagnostics: a comparative case study of two manufacturers", *International Journal of Operations and Production Management*, Vol. 29, No. 5, pp. 539-560.
10. Brynjolfsson, E., & McAfee, A. (2014). The second machine age: Work, progress, and prosperity in a time of brilliant technologies. WW Norton & Company.
11. Bullen, C., Abraham, T., & Galup, S. D. (2007). IT workforce trends: implications for curriculum and hiring. *Communications of the Association for Information Systems*, *20*(1), 34.
12. Burkitt, F. 2014."A strategist's guide to the Internet of Things", *Strategy+Business*, (4:77), pp. 2-12.
13. Dai, H. N., Wang, H., Xu, G., Wan, J., & Imran, M. (2019). Big data analytics for manufacturing internet of things: opportunities, challenges and enabling technologies. *Enterprise Information Systems*, 1-25.
14. Delmastro, F. (2012). Pervasive communications in healthcare. *Computer Communications*, *35*(11), 1284-1295.

15. Fortino, G., & Trunfio, P. (Eds.). (2014). Internet of things based on smart objects: Technology, middleware and applications. Springer Science & Business Media.
16. Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.
17. Haeckel, S. (2010). The post-industrial manager. *Marketing Management Magazine*, 24-32.
18. Husnjak, S., Peraković, D., Forenbacher, I., & Mumdziev, M. (2015). Telematics system in usage based motor insurance. Procedia Engineering, 100, 816-825.
19. Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014). Security of the Internet of Things: perspectives and challenges. *Wireless Networks*, *20*(8), 2481-2501.
20. Khan, R., Khan, S. U., Zaheer, R., & Khan, S. (2012, December). Future internet: the internet of things architecture, possible applications and key challenges. In *2012 10th international conference on frontiers of information technology*(pp. 257-260). IEEE
21. Kortuem, G., Kawsar, F., Fitton, D., & Sundramoorthy, V. (2010). Smart objects as building blocks for the internet of things. *Internet Computing, IEEE*, *14*(1), 44-51.
22. Krotov, V. (2017). The Internet of Things and new business opportunities. *Business Horizons, 60*(6), 831-841.
23. Li, J., Yan, Q., & Chang, V. (2018). Internet of Things: Security and privacy in a connected world. *Future Generation Computer Systems*, 78(3), 931-932
24. Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal*, *4*(5), 1125-1142.
25. Mähler, V., & Westergren, U. H. (2018). Working with IoT: A Case Study Detailing Workplace Digitalization Through IoT System Adoption. In *IFIP Internet of Things, 24th IFIP World Computer Congress, WCC 2018 Poznan, Poland, September 19–21, 2018*. Springer.
26. Mekki, K., Bajic, E., Chaxel, F., & Meyer, F. (2019). A comparative study of LPWAN technologies for large-scale IoT deployment. *ICT express*, *5*(1), 1-7.
27. Neirotti, P., De Marco, A., Cagliano, A. C., Mangano, G., & Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities*, *38*, 25-36.
28. Noura, M., Atiquzzaman, M., & Gaedke, M. (2019). Interoperability in internet of things: Taxonomies and open challenges. *Mobile Networks and Applications*, *24*(3), 796-809.
29. Pang, Z., Zheng, L., Tian, J., Kao-Walter, S., Dubrova, E., & Chen, Q. (2015). Design of a terminal solution for integration of in-home health care devices and services towards the Internet-of-Things. *Enterprise Information Systems*, *9*(1), 86-116.
30. Perera, C., Barhamgi, M., Bandara, A. K., Ajmal, M., Price, B., & Nuseibeh, B. (2020). Designing privacy-aware internet of things applications. *Information Sciences*, *512*, 238-257.
31. Saarikko, T., Westergren, U. H., & Blomquist, T. (2017). The Internet of Things: Are you ready for what's coming? *Business Horizons*, *60*(5), 667-676.
32. Saarikko, T., Westergren, U., & Jonsson, K. (2020, January). Here, there, but not everywhere: Adoption and diffusion of IoT in Swedish municipalities. In *Proceedings of the 53rd Hawaii International Conference on System Sciences*.
33. Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer networks*, *76*, 146-164.
34. Soleymanian, M., Weinberg, C. B., & Zhu, T. (2019). Sensor Data and Behavioral Tracking: Does Usage-Based Auto Insurance Benefit Drivers?. Marketing Science, 38(1), 21-43.
35. Tao, F., Qi, Q., Liu, A., & Kusiak, A. (2018). Data-driven smart manufacturing. *Journal of Manufacturing Systems*, *48*, 157-169.

36. Statista.com (2020) Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ Retrieved on March 20, 2020.
37. Teece, D. J. 2010. "Business models, business strategy and innovation," *Long range planning*, (43:2), pp. 172-194.
38. Torun, H. M., Pardue, C., Belleradj, M. L., Davis, A. K., & Swaminathan, M. (2018, May). Machine learning driven advanced packaging and miniaturization of IoT for wireless power transfer solutions. In *2018 IEEE 68th Electronic Components and Technology Conference (ECTC)* (pp. 2374-2381). IEEE.
39. Westergren, U. H., Saarikko, T., & Blomquist, T. (2018). Initiating the Internet of Things: Early Adopters' Expectations for Changing Business Practices and Implications for Working Life. In *The Internet of People, Things and Services* (pp. 111-131). Routledge.
40. Westergren, U.H., Holmström, J., & Mathiassen, L. (2019) Developing Inter-firm Collaboration to Create IT-based Value: A Contextual Ambidexterity Approach, *Information and Organization*, 29(4)
41. Yang, Y., Wu, L., Yin, G., Li, L., & Zhao, H. (2017). A survey on security and privacy issues in Internet-of-Things. *IEEE Internet of Things Journal*, *4*(5), 1250-1258.
42. Ziegeldorf, J. H., Morchon, O. G., & Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728-2742.