LAPPEENRANTA-LAHTI UNIVERSITY OF TECHNOLOGY LUT
School of Business and Management
Master's Programme in Supply Management

Rita Nakari

IOT SERVICE SUPPLY CHAIN AND RISK MANAGEMENT IN THE HEALTH CARE SECTOR

Master's Thesis, 2020

Examiners:

1st Supervisor: Professor Anni-Kaisa Kähkönen
2nd Supervisor: Post-Doctoral Researcher Mika Immonen

ABSTRACT

Lappeenranta-Lahti University of Technology LUT
School of Business and Management
Master's Programme in Supply Management

Rita Nakari

IoT service supply chain and risk management in the health care sector

Master's thesis
2020
90 pages, 9 figures, 8 tables and 2 appendices
Examiners: Professor Anni-Kaisa Kähkönen and Post-Doctoral Researcher Mika Immonen
Keywords: IoT, service supply chain management, supply chain risk management

Health care is going to face challenges in the future as the number of aging people grows faster than ever. The expectations towards IoT have grown because it can provide solutions to these challenges. The published literature about IoT is often focused on technology. A research gap concerning how IoT services function from a business point of view was identified. IoT solutions are complex and require a lot of know-how. Thus, it makes no sense for health care providers to produce the solutions alone and that is why they buy solutions as a service. Therefore, the objective of this thesis is to examine the IoT service supply chain and what to take into consideration when either buying or supplying IoT solutions. In addition, possible risks related to the supply chain were studied.

The thesis was made in cooperation with ELSA testbed project. The study was conducted as a qualitative case study. The primary data source was six case company interviews and other materials about the project was used as a secondary data source. Abductive research method was used to analyze the collected data. The main goal of IoT solutions is to find valuable knowledge from the data. The process begins with collecting the data and forwarding it a platform through networks. In the platform the data can be analyzed and based on the analyzed data services can be built. Trust, communication, cooperation, co-creation and commitment were identified to be factors that affect how successful the service supply chain becomes. Risk management approaches differ depending on whether the companies are providing the solution or buying it. However, data security was a risk that all of the companies encountered, especially in the health care sector where the collected data can be very sensitive.

TIIVISTELMÄ

Lappeenrannan-Lahden teknillinen yliopisto LUT
School of Business and Management
Master's Programme in Supply Management

Rita Nakari

IoT-palveluiden toimitusketjun johtaminen ja riskien hallinta terveydenhuoltoalalla

Pro gradu -tutkielma
2020
90 sivua, 9 kuvaa, 8 taulukkoa ja 2 liitettä
Tarkastajat: professori Anni-Kaisa Kähkönen ja tutkijaopettaja Mika Immonen
Hakusanat: IoT, palvelujen toimitusketjun johtaminen, toimitusketjun riskien hallinta

Terveydenhuoltoala tulee kohtaamaan tulevaisuudessa haasteita, kun ikääntyvien ihmisten määrä tulee kasvamaan nopeammin kuin koskaan. Odotukset IoT:ta kohtaan ovat kasvaneet, koska sen avulla voidaan ratkaista näitä ikääntymisen aiheuttamia resurssiongelmia. Aiheeseen liittyvä kirjallisuus keskittyy usein teknologiaan, mutta IoT-palveluiden toimitusketjuun liittyvää tutkimusta liiketoiminnan näkökulmasta ei ole aiemmin tehty. IoT-palvelut ovat monimutkaisia ratkaisuja, jotka vaativat paljon erilaista osaamista, minkä takia terveydenhuollon tarjoajien ei ole järkevää tuottaa IoT-ratkaisuja yksin. Siten, tämän pro gradu -tutkielman tavoitteena on tutkia IoT-palveluiden toimitusketjua ja mitä eri toimijoiden on otettava huomioon joko IoT-ratkaisuja ostettaessa tai tuottaessa. Lisäksi tavoitteena oli tunnistaa mahdollisia toimitusketjuun liittyviä riskejä.

Tutkielma tehtiin yhteistyössä ELSA testbed-projektin kanssa. Tutkielmassa käytettiin laadullista tutkimusmenetelmää. Tämän tapaustutkimuksen ensisijaisena tietolähteenä olivat kuusi case-yrityksen haastattelua ja muita projektia koskevia materiaaleja käytettiin toissijaisena tietolähteenä. Kerätyn aineiston analysointiin käytettiin teoriaohjaavaa sisällönanalyysiä. IoT-ratkaisuiden tavoite on löytää arvokasta tietoa datasta. Prosessi alkaa datan keräämisellä ja sen siirtämiselle jollekin alustalle internet-yhteyden avulla. Alustoilla dataa voidaan analysoida ja analysoidun datan perusteella voidaan rakentaa palveluja. Luottamus, kommunikaatio, yhteistyö, yhteiskehittäminen ja sitoutuminen tunnistettiin tekijöiksi, jotka vaikuttavat siihen, kuinka hyvin palvelun toimitusketjusta toimii. Kohdatut riskit ja riskienhallinta vaihtelevat sen mukaan, onko yritys ratkaisun tarjoaja vai sen ostaja. Tietoturva oli kuitenkin riski, jonka kaikki yritykset joutuvat ottamaan huomioon. Erityisesti terveydenhuollonalalla tietoturvaan tulee kiinnittää huomiota, koska kerätyt tiedot voivat olla hyvin arkaluontoisia.

ACKNOWLEDGEMENTS

It is hard to believe that this moment has arrived, and I'm actually almost done with my studies. I can't imagine a better place to study than LUT and Lappeenranta. I'm going to miss both of them a lot. For the first time ever, I don't have clear plans for my future, but perhaps that is a good thing.

First of all, I would like to thank Mika Immonen for guiding me during the writing process. I would also like to thank him and the rest of the ELSA project team for giving me this opportunity to do this thesis in cooperation with you. In addition, huge thanks to the interviewees for sharing their valuable opinions.

Finally, I want to thank my family for the support I received during my studies and of course, during my whole life. Last but not least, I want to thank my friends, especially RKK, for sharing the best years of my life with me. Finding such a supportive, but let's face it, a crazy group of friends is something that I will forever be grateful for.

Special thanks to SaiPa, Coca-Cola and TikTok for bringing joy to my life during this long process.

In Lappeenranta, 14.12.2020

Rita Nakari

Table of Contents

APPENDICES

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

IoT is a fairly new concept and it has been able to change the world quite fast. Kevin Ashton used the term IoT for the first time in 1999 (van Kranenburg & Bassi 2012, 1; Wang, Chaudhry & Li 2016, 239). Digitization refers to digital technologies becoming bigger parts of our everyday life. These new technologies provide new possibilities for connecting services and automation of operations. Digitization has also created a new phenomenon that can be even more remarkable: datafication. For instance, mobile phones and applications on them produce digital data. Datafication especially has a focus on how collected data creates value. Together digitization and datafication enable capturing events and series of occasions in the form of data. (Ylijoki & Porras 2016, 69; Lycett 2013, 382) This is also the main goal of IoT.

Technologies have become more user-friendly and cloud services have become cheaper and easier to access (Legner, Eymann, Hess, Matt, Böhmann, Drews, Mädche, Urbach and Ahlemann 2017, 302). This has enabled the success of IoT. In just three years between 2019 and 2022 the market revenue of IoT in expected to grow from 171 billion dollars to 241 billion dollars (Statista 2020a). Especially Germany, Japan, Spain and Switzerland are leaders in IoT industry. All in all, Europe is the leading continent in IoT usage and development. (Dlodlo, Foko, Mvelase & Mathaba 2012, 254). IoT and the amount of data caused by it has also affected the big data landscape (Marjani, Nasaruddin, Gani, Karim, Hashem, Siddiqa & Yaqoob 2017, 5247) Particularly during the past few decades, the usage of big data has significantly increased the amount and variety of data that firms can collect and utilize in their daily operations. (Assunta Barchiesi & Fronzetti 2019, 1) As IoT has become more popular, there are also more IoT solutions available (Lee & Lee 2018, 6860). There are companies that offer IoT products, application and services (Ju, Kim & Ahn 2016, 883). Depending on the application area, the possible benefits that can be reached may vary. In general, IoT solutions can help companies to save time and money. (Whitmore, Agarwal & Xu 2015, 270)

Since IoT is becoming more popular, also the number of researches about IoT and its applications has increased. Usually these researches are either business-related or technical-related. Particularly, the number of technical-related research grows all the time, and just between 2012 – 2017 over 100 000 publications were written. There has been a lot of focus specifically on IoT's cloud and middleware. (Chernyshev, Baig, Bello & Zeadally 2018, 1637-1638; Ambore & Suresh 2018, 177) Whitmore et al. (2015) have also noticed

the same thing in their literature analysis: research about IoT is mostly focused on technology. The reason behind it might be the fact that the IoT technology is still quite new and implementing it still is at an early stage. Many of the published papers are conference papers from technical and engineering conferences. The highest interest is towards IoT research has been mainly in Europe and Asia. (Whitmore et al. 2015. 269)

Producing services includes multiple parties: the service providers, the vendors of resources need to deliver these services and the clients. Also, the coordination and measuring the performance of the service supply chain may be more challenging. Therefore, information exchange between actors in service supply chain is enhanced. Collaboration is the key when producing services: many actors are involved in a complex chain in order to create value. (Giannakis 2011, 1810, 1817-1819) Earlier the service sector didn't gain much attention compared to, for example, manufacturing and agriculture industries as many economies were mainly built on them (Ellram, Tate & Billington 2007, 45). Nowadays many industries that earlier were just about manufacturing are becoming also services (Giannakis 2011, 1811). Traditionally the studies about services have concentrated on a specific process within a specific context instead of examining what kind of systems these processes and contexts form together. (Chandler & Lusch 2015, 7). Research about service supply chains is also still at an early stage but interest towards the subject is growing, even though in the past the focus has been more on traditional supply chain. Especially service supply chain logistics and productivity have been well discussed in the literature. (Choudhury, Paul, Rahman, Jia & Shukla 2020, 14)

All in all, the whole world of IoT and its applications is new which means that the literature available is quite limited. Existing researches and papers are usually written about specific field of business. The focus will be in the health care sector as there will be a lot of demand in the future due to growing number of aging people. Especially, studies about delivering and buying an IoT solution from a business point of view are quite rare as most of the studies are focused on the technical aspects of IoT. Therefore, this research's business aspect of IoT supply chain is an interesting as there is not much research about the subject. The study will be conducted as a case study and the primary data will be collected through theme interviews. The goal is to examine the service supply chain of an IoT solution in the health care sector.

1.1 Objectives and research questions

The IoT supply chain describes how data that is collected, for example, by IoT devices and sensors, become useful information for different parties. As the field of IoT supply chain is still quite new and there are not many researches done about the subject, the main objective of this study is to identify different steps in the IoT supply chain and how collected data transfers into valuable knowledge. In this thesis the focus was on parties that were involved in a testbed project in which companies were able to test their solutions with real patients. The project takes place between 2018 and 2020. Representatives from different case companies will be interviewed in order to get real-life examples from IoT supply chains and service supply chains around them. In addition, material about the project was also used as a secondary data source.

The main research question is:

How the IoT supply chain can be described from the perspective of customer needs?

In this case, customer is defined as the health care provider that buys IoT services from other companies. The customer perspective is chosen for this question because in supply chain management the focus has shifted from minimizing costs to customer experience. Traditionally the main goal has been to achieve the lowest possible prices. (Spekman, Kamauff & Myhr 1998, 631) Three sub-questions were developed in order to help answering the main research question and to get a thorough understanding of the studied subject. The first sub-question is about identifying different data sources from the end customers point of view in order to understand how they collect data. The second sub-question studies the actors and their participation in the IoT supply chain as producing an IoT solution may include many actors. Finally, the third sub-question is focused on risk management of the actors involved in the IoT supply chain. Therefore, these sub-questions are:

1. *How data sources are identified based on the needs of customers' intended applications?*

2. *How the roles of different actors can be defined in the IoT supply chain within intended applications?*

3. *How risk management approaches differ between actors which represent different parts of IoT supply chain or utilize varying data sources?*

1.2 Limitations

This thesis is based on B2B IoT solutions. All of the case companies are somehow involved in the service structure of a public actor. The case companies operate in the health care sector or have the technology that can be adapted in the health care sector. This should be taken into consideration when analyzing the results as the results could be different for companies that represent other business fields. More specifically, the focus is on solutions that assist elderly that are able to still live at home and on the companies that provide these services. Taking individual customers' experiences into consideration would be too broad for this thesis. This study is conducted as a qualitative research. The data will be collected through interviews from a case companies that either provide or buy IoT solutions as a service. Using qualitative research method enables getting a thorough understanding about the service supply chain of IoT and how companies feel about the new phenomena.

1.3 Defining key concepts

IoT, also known as Internet of Things, Internet of Everything or the Industrial Internet is still relatively new phenomenon which is why there is no specific definition for it (Lee & Lee 2015, 431; Čolaković & Hadžialić 2018, 17). A few definitions of IoT are presented in the table 1 below. It is said that IoT is as remarkable as internet was a few decades ago. Some call it as the "next generation of internet". (Pang, Zheng, Tian, Kao-Walter, Dubrova & Chen 2015, 87) The main purpose of IoT is to collect information about the environment to understand it and act on it. It already has an impact on many fields of life, and it will continue to change our lives even more in the future. (Díaz, Martín & Rubio 2016, 100, 115)

Table 1. Definitions of IoT.

Definition	Author
“A new technology paradigm envisioned as a global network of machines and devices capable of interacting with each other.”	Lee & Lee (2015, 431)
“The inter-networking paradigm enabled by technology stack which provides a seamless connectivity between physical and virtual object to facilitate the development of intelligent services and applications with self-configuring capabilities.”	Čolaković & Hadžialić (2018, 19)
“Interconnection of sensing and actuating devices providing the ability to share information across platforms through a unified framework, developing a common operating picture for enabling innovative applications.”	Gubbi, Buyya, Marusic & Palaniswami (2013, 1647)
“The term Internet-of-Things is used as an umbrella keyword for covering various aspects related to the extension of the Internet and the Web into the physical realm, by means of the widespread deployment of spatially distributed devices with embedded identification, sensing and actuation capabilities.”	Miorandi, Sicari, De Pellegrini & Chlamtac (2012, 1497)

Service supply chain “is the network of suppliers, service providers, consumers and other supporting units that performs the function of transaction of resources required to produce services; transformation of these resources into supporting and core services; and the delivery of these services to customers” (Baltacioglu, Ada, Kaplan, Yurt & Cem Kaplan 2007, 112). Nowadays supply chains can be seen as collaborative customer-focused networks of companies whereas earlier they were only seen as linear chains of firms. (Kemppainen & Vepsäläinen 2003, 716)

IoT supply chain is described in this study as the process when data transfers in an IoT solution from the point it is collected till the point where the customer gets to utilize the data. The model is based on a service-oriented vision by Čolaković & Hadžialić (2018, 19) where physical and virtual are connected to ease the development of smart services and applications. It consists of several layers and the structure of IoT supply chain is presented in the following chapter 1.4.

Risk management means the processes that can be used to tackle different kinds of risks and to minimize the losses caused by them The term “risk” refers to uncertainty in the environment that may decrease the predictability of the performance and the company outcomes. Modern risk management focuses on proactive operations that aim at preventing the risks, whereas more traditional risk management concentrates on reacting to risks after they have occurred. (Suominen 2003, 27, 29; Miller 1992, 312)

Testbed means the development and testing of new products and services in real environment. Testbeds are utilized in product development in many different fields of business, especially when developing new technologies. These projects are important for new innovations. More testbed researches are done now than ever before (Chernyshev et al. 2018, 1643).

Big data is a term that is used to describe huge data sets that require, because of their size and complexity, advanced data storage, analysis and visualization technologies. (Chen, Chiang & Storey 2012, 1166) Big data is often described with 3 V’s which means that big data is high in volume, variety and velocity. Volume refers to the increasing amount of data. Variety is about the different sources and types of big data. Velocity refers to fast speed of data creation. (Ghasemaghaei, Ebrahimi & Hassanein 2018, 103) Some researches have also added 4 V’s to the description: variability, veracity, visualization and value. Variability means that there can be data which meaning changes constantly. Veracity ensures that the collected data is trusted, statistically reliable and that unauthorized people do not have access to it. Visualization means providing the data in way that it is readable. Lastly, value means that at best the collected and analyzed data can provide added value for different processes and overall companies’ daily operations. (Sivarajah, Kamal, Irani & Weerakkody 2017, 273; Demchenko, Grosso, de Laat & Membrey 2013, 50)

1.4 Theoretical framework of the research

Theoretical framework combines the theoretical and empirical parts together. It helps to solve the research questions and it is the basis of this research. Supply chain is defined in this thesis as “a set of primarily collaborative activities and relationships that link companies in the value-creation process, in order to provide the final customer with appropriate value mix of products and/or services”. These collaborative activities can be anything from designing to delivering the product or service. (Braziotis, Bourlakis, Rogers & Tannok 2013, 648). IoT supply chain can be considered as a service supply chain because companies

usually do not produce the whole process themselves. It is more cost-efficient to outsource other than company's key activities (Baltacioglu et al. 2007, 107). The service supply chain is a network of parties that aims to create value for the customer (Normann & Ramírez 1993, 66) which consists of the product, service and information (Sintonen & Immonen 2013, 1308). In this thesis a five-layer structure of IoT solution is used. There are other possible structures as well used in some researches. Often a four-layer structure is used, and it is seen as the classification standard that offers consistency for IoT development. (Lee, Bae & Kim 2017, 2) This is usually used in studies that are written about a technological perspective of IoT. As the customer is emphasized in this research, it was added to the framework. The whole process starts with collecting data and then transforming it into a format that can be utilized by, for example, companies. Theoretical framework is presented in the figure 1.

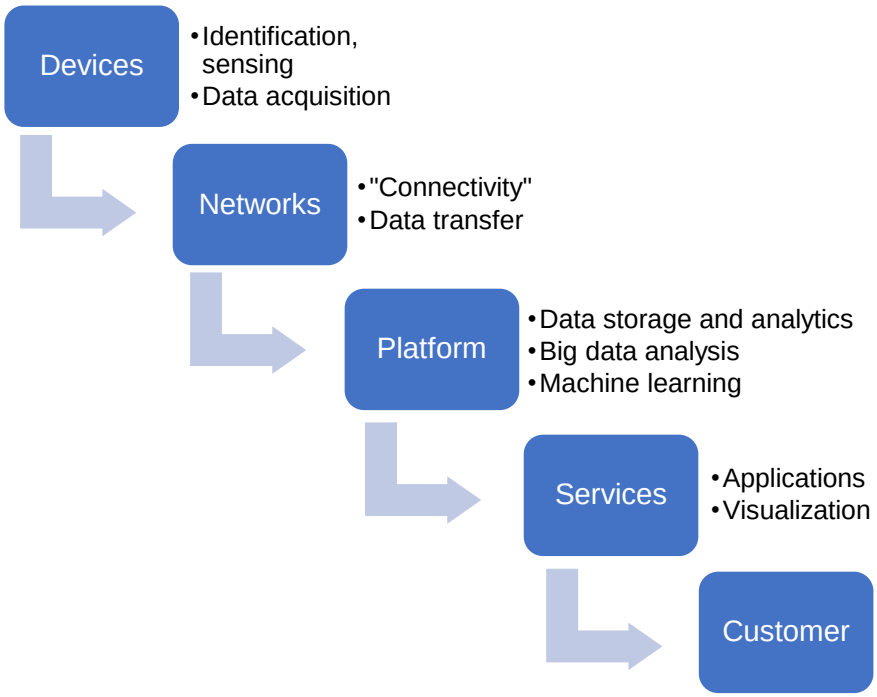

Figure 1. IoT supply chain (adopted from Čolaković & Hadžialić 2018, 19; Lee et al. 2017, 3)

The first step in IoT supply chain is collecting data by IoT constrained devices. Often these devices have sensors that can be embedded to almost any device, like mobile phones. Sensors observe and evaluate changes in its environment, for example, changes in the temperature, light or movement. Data can also be collected from smart objects, social media

and the web. Data is not analyzed in this layer; thus, the collected data is forwarded to a data storage through the network. (Čolaković & Hadžialić 2018, 21, 24)

The next step in the supply chain is network layer. Network is a crucial part of the IoT supply chain as it allows the communication between objects and between objects and internet. Network layer consists of hardware, software, technologies and protocols. Depending on the devices, network connections can be either wireless or wired connections. However, most of them have wireless connections because it has better availability and mobility. There are dozens of different kinds of network solutions that can be used in the IoT supply chain, and new technologies emerge all the time. Connectivity of the network layer refers to the fact that IoT devices are connected to other devices or applications anytime and anywhere which enables efficient and real-time transferring of data. (Čolaković & Hadžialić 2018, 19-22)

The third step in the IoT supply chain is platform layer which is located between IoT objects and application layer. It is a cornerstone of the IoT solutions. The platform layer is for storing data and processing it. Analyses can be made with the help of, for instance, big data and machine learning. It also enables managing and monitoring the whole system from sensors to applications. (Rayes & Salam 2019, 206) Usually there are many different IoT devices for different purposes which makes the collected data quite versatile. This layer is necessary as it extracts heterogeneity of the collected data so that there can be seamless integration with anything. (Díaz et al. 2016, 107) Users and applications can access collected data through this layer (Calbimonte, Sarni, Eberle & Aberer 2014, 51). The increased amount of data has led to a need to develop new platforms that can provide better scalability, storage and processing. These platforms are important parts of IoT systems as they make it possible to integrate IoT objects with different network technologies. (Čolaković & Hadžialić 2018, 20)

The fourth step in the IoT supply chain is the service layer which refers to the point where companies are utilizing the collected data in different ways. Application services are produced through the IoT platforms. Some platform providers can offer, for example, analytics tools as well. They provide accessible user applications that ease the processing, understanding and utilizing the collected data. IoT has already provided a lot of smart applications to many industries and it has potential to offer them to almost every market. (Čolaković & Hadžialić 2018, 20; Díaz 2016, 100)

The final step in this framework is delivering the service to the customer. As this thesis is based on B2B solutions, the end-user is not emphasized here. The customer aspect was added to this framework as it is interesting to study this phenomenon also from their point of view. Examining the customer's experiences adds more depth to the studying process of a service supply chain. In addition, IoT affects significantly the health care sector and therefore, getting their opinions is valuable.

1.5 Structure of thesis

This thesis is structured as follows. There are six main chapters that include several subchapters. The first main chapter is an introduction to the subject and to the objectives this study. Also, the background of it and the research questions of this thesis are presented. The second chapter concentrates on IoT markets and the IoT trends. Also, a short introduction to IoT solutions for health care is made. The next chapter is focused on the theory this research is based on. The main focus is on service supply chain, IoT and its supply chain. The fourth chapter is about the research methodology used in this thesis. In addition, the case companies and data collection and analysis processes are shortly presented.

The following main chapter is the empirical part that seeks to answer to the research questions through interviews and examining the other materials that are related to this testbed project. In the sixth and final chapter conclusions are made, answers to the research questions are given and empirical findings are reflected to the theory presented earlier. The quality of the research will be evaluated. Finally, possible implications are suggested, and future research suggestions are made.

2 TRENDS IN IOT SECTOR

This second chapter presents the situation and trends in the IoT market. In addition, using IoT solutions in health care will be examined. Mega trends shape the lives of billions of people around the world. Among climate change, drastically growing amount of people and urbanization, connectivity is one of the biggest mega trends right now and in the near future. (European Strategy and Policy Analysis System 2020). Nowadays people do not only connect with each other, but they connect with devices, and on top of that devices can connect with other devices without humans.

2.1 IoT market

According to predictions the number of IoT connected devices worldwide will grow from 22 billion devices to 50 billion between 2018 and 2030 (Statista 2020b). The IoT devices are estimated to generate nearly 80 zettabytes of data in 2025 (International Data Corporation 2019). These devices can be basically anything from, for example, health care applications to agriculture applications and the number of fields of applications grows continuously. Particularly, smart homes, smart industry and smart traffics are areas that are significantly growing. IoT enables connections and data transfer at all times anywhere by anyone or anything. (Čolaković & Hadžialić 2018, 17-18; Wortmann & Flüchter 2015, 221). The market share of IoT in the Nordic and Baltic countries and a forecast presented is in the figure 2. The figure is based on data by Statista.

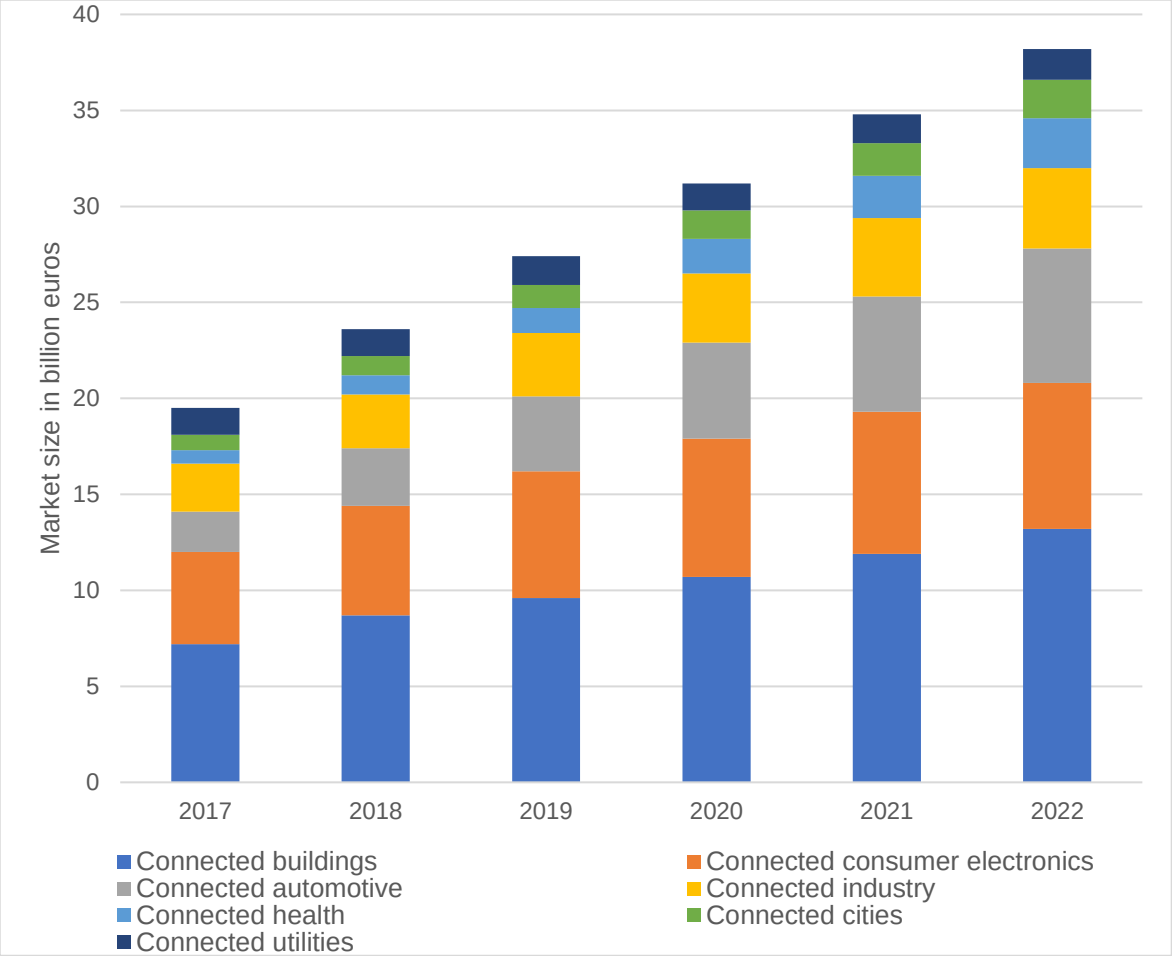

Figure 2. Internet of things (IoT) market size in the Nordic and Baltic countries forecast by category (based on data by Statista 2020c)

Based on the figure 2, the market size of all these sectors is estimated to nearly double in just five years, between 2017-2022. Connected buildings clearly has the largest market size. However, the share of connected health is also expected to grow in the near future. The value of the market size is expected to increase from 0,8 billion euros to 2 billion euros by 2022. The market share of connected consumer electronics is expected to grow. This can also be beneficial for health care, in case using the data collected by consumer devices could be used in health care someday. All in all, this study supports the estimations about the rapidly increasing amount of data and number of IoT devices.

2.2 IoT trends

In the future, things that are connected to the internet will be the main consumer of data traffic instead of human beings (Aloi, Caliciuri, Fortino, Gravina, Pace, Russo & Savaglio

2017, 74). Below in the figure 3, there is a hype cycle that presents the maturity and adaptation of different IoT solutions. (Gartner 2020)

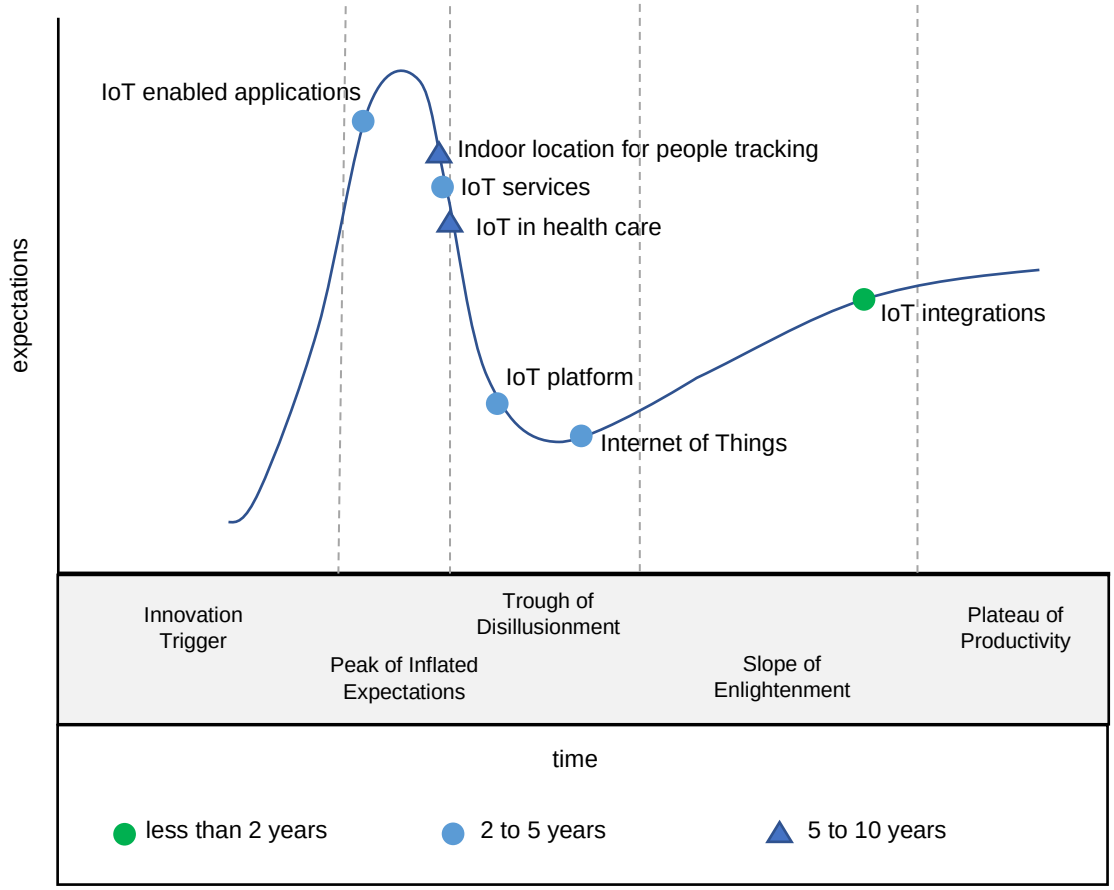

Figure 3. Hype cycle for the Internet of Things (adapted from Gartner 2020)

There are five stages that represent the technology life cycle. The first stage is called “Innovation Trigger” which means that a potential technology is about to gain more attention and the media interest may lead to even more publicity. Usually at this point there are no usable solutions avalaible. The following stage is “Peak of Inflated Expectations” where the publicity has led to success stories. However, many companies are still not ready to take action. “Trough of Disillusionment” is the third stage in this cycle. The interest towards a new technology decreases due to failed experiments. If the surviving providers are able to develop their products and the customers are satisfied, investments may continue. The fourth stage is the “Slope of Enlightenment” which means there is a better understanding about the technology and second- and third-generation products become available. More companies are involved in pilots. The final step in this hype cycle is the “Plateau of Productivity”. At this point mainstream adoption begins. Different shapes and colors of them represent the time until the plateau will be reached. (Gartner 2020)

IoT is already in the stage of Trough of Disillusionment and it is expected to reach the plateau within the next two to five years. The biggest hype around it has already decreased. From the figure it can also be seen that the expectations towards IoT in health care are very high but it will take five to ten years to reach to plateau. Also, other IoT services and IoT-enabled applications are right now facing a lot of expectations but as they quite new things, it will probably take a few years before they have breakthroughs in the market and the investments in them become successful. Based on the figure, it is quite clear that there are a lot of different IoT applications coming in the upcoming years. (Gartner 2020)

2.3 IoT in health care

At the moment people are aging faster than ever. Between the years 2015 and 2050 the amount of people who are over 60 years old will increase from 12 % to 22%. Countries need to make sure that their health systems are able to cope with the challenges that are caused by this demographic shift. (WHO 2018) In Finland, the goal is to offer elderly a possibility to live at home for as long as possible. In 2018 93 % of people who were 75 years or older still lived at home. (Finnish institute for health and welfare 2019) New smart technology can offer opportunities to live safer and longer at home more independently and thus, improve the life quality of the elderly. (Cho & Kim 2014, 141). As the demand of these solutions increases constantly, it creates new possibilities for businesses around the world among the health care industry.

The development of electronics, medical services and computer science has led to significant technological advancements in the form of IoT realization (Dey, Ashour & Bhatt 2017, 8). Cloud computing and IoT have had a huge effect on several industries, including on the health care sector. The new technologies enable quick and effective data sharing. (Peek, Holmes & Sun 2014, 45) A service provider can be defined as the company that offers the service based on the customer requirements and if needed, utilizes other services as well and resources of sub-contractors (Selviaridis & Norrman 2014, 154). The health care providers are service providers that offer services for patients and when necessary, they purchase services from other companies. At the moment, they face big challenges around the world, like the ageing of people. In order to meet the needs of this growing group of the elderly, the resource utilization and efficiency of health care services must be improved. IoT makes health service more effective, smart and ubiquitous. Constantly growing amount of ageing people require more health care services and combining IoT and health care can be the answer to this problem. Through these new solutions health care

can become more effective and smarter. Also, new supporting assistive technologies enable more personalized and patient-centric health care. There are many technical solutions that can be used in IoT services which makes them very interesting from a business point of view as the customer segment is constantly growing. (Pang et al. 2015, 86-88; Plaza, Martín, Martin & Medrano 2011, 1985) Therefore, the fast development of health care services and mobile devices offers a big market for IoT applications and possibilities will increase in the future. (Li, Xu & Zhao 2015, 255)

Individual health data can nowadays be collected through IoT systems. New analytic tools and IoT data are able to give more detailed and real-time information about patients' health than ever before which enables also more personalized health care. Receiving data about patients' everyday life, behavior and health can make the health care more effective and accurate. The integration of IoT, improved analytic tools and health care can lead to reduced health care costs while still achieving better results than before. (Lee & Lee 2015, 434; Dey et al. 2017, 4) As aging of people also has led to a more personalized model of health care, more and more intelligent applications are developed that assist independent living of the elderly. IoT increases the quality of assisted living solutions. There can be medical or wearable sensors that collect data around the clock. The collected data is sent remotely to, for example, medical centers, nurses or doctors. New technologies can improve the life quality of elderly very much and also prevent possible accidents or other health related problems. (Plaza et al. 2011, 1981; Li et al. 2015, 254) Behavioral, social and biological characteristics of people are the basis of personalized health care which makes health care more cost-efficient. Supportable services that can be executed with the help of IoT concentrate on the early disease detection and on homecare instead of clinics as is possible to connect in-home measuring equipment to hospital-based imaging systems through sensor nodes. The IoT solutions enable achieving the professionals' health recommendations remotely. (Dey et al. 2017, 7)

Better availability of data and new intelligent solutions supports the revolution of health care, enables personalization of management and treatment options and leads to decreased costs of health care (Dey et al. 2017, 4). From a business point of view, the growing number of users and matured ecosystem of mobile internet services have accelerated the development and deployment of IoT solutions in health care. However, the adoption of these solutions is challenging because of the lack of interoperability and integration. Thus, efficient device and service integration is very important for a successful IoT solution. Also, the collaboration between health care service providers and other internet and platform providers is in a key position in these solutions. Therefore, the health care service providers

do not have to develop new infrastructures, like servers or software, that enable deployment of IoT. Utilizing the existing infrastructures of other providers is more efficient. There are some strict privacy regulations and public authentications that affect the health care service providers and it is important to apply these rules to other service providers as well. In addition to the legislative demands, ensuring that only authorized users are able to access private data is critical. These requirements are the basis of the security architectures of an IoT system. (Pang et al. 2015, 88, 92)

3 MANAGING IOT SUPPLY CHAINS

This chapter presents published literature and researches about the most important subjects that support the empirical part of this thesis. The aim is to examine the subjects broadly in order to gain an extensive understanding about service supply chains, their management and risks that may occur. Also, IoT and its supply chain, the impact of machine learning, artificial intelligence and big data to IoT will be presented. Finally, the risk management concerning IoT supply chains from different points of view are discussed.

3.1 Service supply chain

The fact that internet can be reached almost anywhere at any time has led to the development of digital markets. This has offered companies new and fascinating strategic possibilities. (Abaidi and Vernette 2018, 676) The significance of services has grown a lot during the past decades and the shift from production-based to service-dominant value creation has changed the importance of services around the world (Vilko & Ritala 2014, 114). Globalization has many effects on companies' operations, like growing competition, borderless markets and huge advances of technology as well as increases in wages and institutional development all had an impact on the nature of service sector. The organizational structures of service industries are becoming more complicated and the whole service sector is diverse while still going through drastic changes. (Baltacioglu et al. 2007, 107, 121) The objective of service supply chain processes is to create competitive service offerings from heterogenous resources (Boon-itt, Wong & Wong 2017, 1).

Compared to traditional supply chain, the service supply chain is different because of the unique characteristics of services. The management of services is often decentralized. In addition, services are usually harder to visualize and to measure (Ellram, Tate & Billington 2004, 18). Intangibility of services is one of the biggest characteristic differences compared to traditional goods. Intangibility of services means that there is no physical flow in service supply chain. Therefore, the flow of information is crucial for the successful functioning of service supply chain. (Baltacioglu et al. 2007, 109, 113; Giannakis 2011, 1810) One of the biggest challenges of service organizations is the ability to react quickly to the changing demand of the customer. There are several parties included in the service production and they need to collaborate effectively. In order to co-create value in complicated value chains or networks, the service providers, the companies that provide other services or resources

used for the planning and delivery of these services, and the service customers need to work together. (Sakhuja, Jain, Kumar & Chandra 2016, 272) Nowadays collaborative buyer-supplier relationships are more common. Joint decision-making refers to a model which means that the parties try to find answers to supply chain related question together. This is based on mutual trust and transparency. (Biehl, Cook & Johnston 2006, 2) All of the actors form a service supply chain that aims to perform a sequence of operations in order to deliver services to customers. (Baltacioglu et al. 2007, 112)

Technical innovations are one of the reasons why service sector has grown significantly during the past decades. More companies want to focus on their core competencies and outsource other functions to experts which converts the enterprise's operations into procured services. (Baltacioglu et al. 2007, 106-107, 112; Ellram et al. 2004, 19) Especially, outsourcing IT services has become more popular lately, even though many companies have earlier wanted to keep it in-house (Demirkan, Cheng & Bandyopadhyay 2010, 120). As there are usually several organizations involved when producing services, the importance of coordinating and cooperating is emphasized in order to offer services at the highest possible level (Sakhuja et al. 2016, 271). In order to adding customer value in the supply chain, actions should be proactive and customer centered, and knowledge should be shared between parties. (Matthyssens and Vandenbempt 2008, 326) Service supply chain management is according to Baltacioglu et al. (2007, 112) "the management of information, processes, resources and service performances from the earliest supplier to the ultimate customer". Ellram et al. (2004, 23) have built a service supply chain model that describes the processes in the service supply chain that need to be managed. The model is presented in the figure 3.

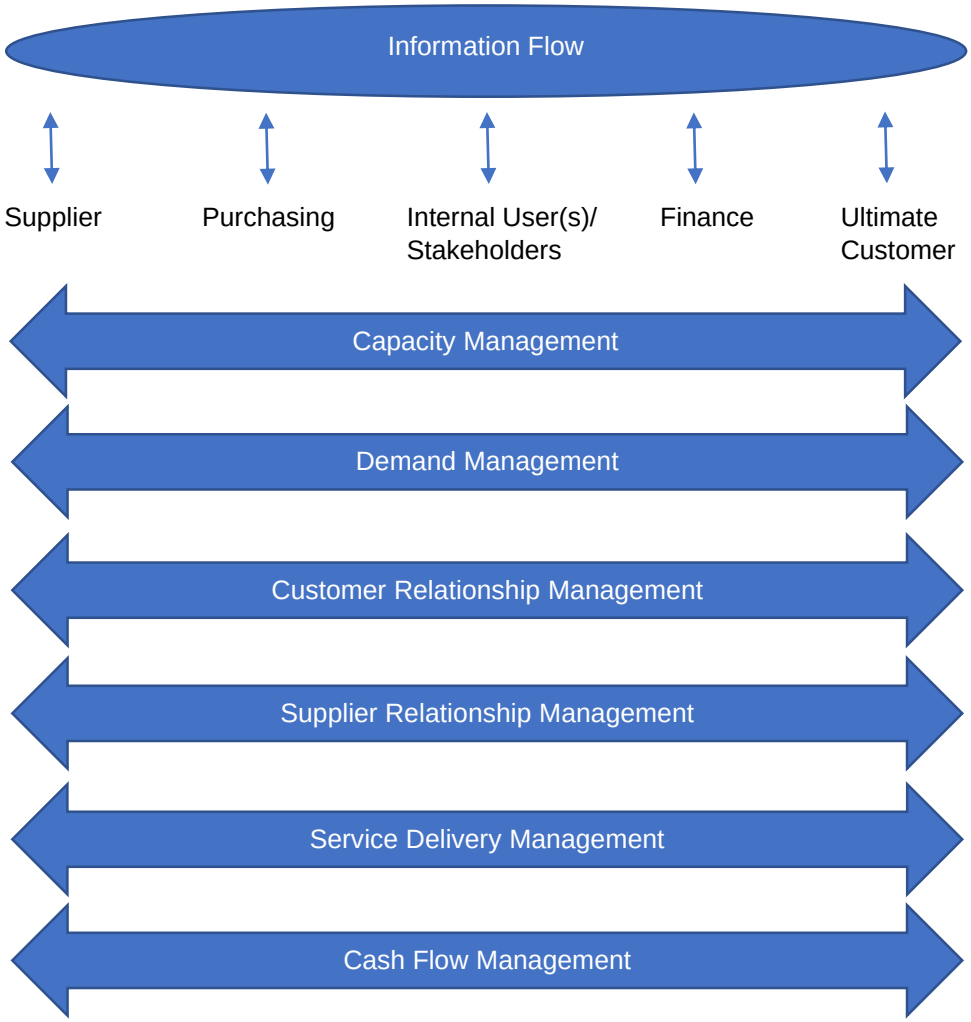

Figure 3. Service supply chain (Ellram et al. 2004, 24)

Information flow is important for the functioning of the service supply chain, as information sharing is crucial for supply chain partners and as it can provide the company, for example, feedback on their performance and knowledge about demand. Capacity management refers to the fact that the service provider needs to invest in its organization, processes and employees. Demand management concentrates on how to meet customer demand and how to react on changes that may occur. Customer relationship management includes, for example, identifying customers, creating customer knowledge and forming relationships with them. The following two processes are from the service buyer's point of view. Supplier relationship management consists of buying services which starts with identifying and clarifying a need, then negotiating contracts and executing them. Often service level agreements are made which may decrease the amount of uncertainty in performance expectations. Supplier relationship management and service delivery management are closely related as the latter makes sure that contracts and service level agreements are

met. Cash flows are the payments that occur between the parties. Managing them includes, for instance, deciding the timing and amounts of payments. When these service processes are performed successfully, the uncertainty in the supply chain can decrease which can lead to better results. (Ellram et al. 2004, 25-27; Srivastava, Shervani & Fahey 1999, 169)

Nowadays, it is recognized that efficient marketing and management of services differs from the marketing and management of traditional goods because services are so different in nature. The demand for services increases all the time and therefore, they need to be efficiently managed while taking into consideration the special characteristics of services. Through efficient management of a supply chain, companies can reach many benefits like, decreased costs, boosted revenues, higher customer satisfaction as well as improvements in service quality and delivery. Supply chains are crucial for companies as nowadays it is not possible to be successful when operating isolated from others. Globalization has led to a situation where many companies operate in several countries which increases the need for effective supply chain management. High involvement in the supply chain and tight relationships with the suppliers and customers are important for creating synergy advantages of collaboration that are in a key position in order to manage the supply chain successfully. (Baltacioglu et al. 2007, 106-108, 121-122)

3.2 IoT supply chain

Due the rapid evolvement of IoT, completely new markets are enabled. This means companies need to create an ecosystem of partners where risks can be shared, and beneficial win-win situations can be created. (Sinha & Park 2017, 2) There are no vendors who could be able to take care of the whole IoT end-to-end solution. IoT market can be characterized by complicated partnerships of several parties, like device manufacturers, software suppliers and retailers. Developing an IoT solution happens in a multidimensional partnership in order to develop a functioning system that combines IoT objects, networks, platforms and applications. (Rayes & Salam 2019, 259) Companies, which can be large multinational companies or governments, have usually several suppliers which may make the whole supply chain quite complex. As being involved in an IoT supply chain can mean that critical data needs to be shared with others, some may be reluctant to do this due to, for instance, legal or contractual reasons. Networks connect several locations and units and pursue to ease a safe exchange of data. The number of IoT devices is expected to grow fast in the future which will increase the number of parties in the IoT supply chains as well (Omitola & Wills 2018, 445, 449). As there are a lot of devices involved in IoT, all of the

devices aren't from the same supplier. Therefore, there might be differences between the standards. The heterogeneity of the devices can affect many things, like the information exchange and processing or communication between units. (Li et al. 2015, 249) The world becomes more and more connected and companies are becoming parts of complex business ecosystems (Westerlund, Leminen & Rajahonka 2014, 6). Instead of vertically integrated companies, networks of connected companies are replacing these traditional markets. For instance, technological innovations, globalization and better availability of information have led to a situation where the number and complexity of business networks have increased. They are usually flexible by nature which enables them to react quickly to change when needed. (Halinen & Törnroos 2003, 1285-1286) In ecosystem model the value capture and creation is done in cooperation instead of company level (Westerlund et al. 2014, 9). The IoT ecosystem includes all the parties that are involved in the IoT solution. These parties can be device suppliers, platform and other possible service providers, application developers and end-users. (Mineraud, Mazhelis, Su & Tarkoma 2016, 13)

The framework of this thesis describes how data is moved from the first layer to the last one and for the customer to be used. The traditional four-level model has several advantages. First of all, it separates the IoT components into smaller pieces which facilitates the development and troubleshooting. Standardized IoT components facilitate the development of joint solutions by multiple suppliers. Module engineering enables several types of IoT hardware and software systems to interact with each other. The model also advances the interoperability between suppliers in order to assure that the technology building blocks function together without problems. And finally, the model enhances new innovations as it enables developers to concentrate on a specific problem without the need to worry about the basic functions. (Rayes & Salam 2019, 8) Communication and co-operation in the IoT supply chain can happen between people, between people and object or between objects. (Lee & Lee 2015, 434) Providers are also dependent on each other as all of the parties need to provide their services on time. This is typical for supply chains and therefore, may lead to a situation where the parties try to control others in order to achieve maximum advantage. (Demirkan et al. 2010, 121) The four-level model is most often presented in technology focused articles. As the customer is in a key position in the IoT supply chain, it was added to the framework.

Technology stack is a combo of different technologies that allow these processes and provides seamless connections at all times and everywhere by anyone and anything. IoT solutions are based on combining smoothly several technologies. (Čolaković & Hadžialić 2018, 19) The first layer in the IoT supply chain is the device layer which takes care of the

data acquisition through different kinds of devices that usually have a sensor or a tag. All the IoT objects have a unique digital identity which is important if they need to be tracked as the IoT network is huge. (Li et al. 2015, 247) The sensors enable the connections between people and the physical measurements, for example, for real-time decision-making. (Dey et al. 2017, 5). The objects collect data and communicate with each other at the same time which means that a huge amount of data flows into the network. (Phan, Nurminen & Di Francesco 2014, 117)

The network layer in the IoT supply chain connects all the devices and people. Through the network layer devices are able to send data forwards which is crucial for the whole IoT system. (Li et al. 2015, 248) The network layer is responsible for processing, controlling and managing huge amounts of data moving across the network (Lee et al. 2017, 2). Outsourcing network's management and operations has become more popular lately. It gives companies a chance to concentrate on their core business and leave the more complex IT solutions to professionals. It also allows the network owners to test new solutions and technologies fast. They can also utilize the collected information to developed better and customized products for their customers. Almost all of the data networks that are used nowadays are founded on the Open Systems Interconnection (OSI) standard. The OSI is a model which describes how numerous components communicate in data-based networks. The model uses a concept that divides the network communication responsibilities into smaller functions, known as layers, which makes the development of them easier. (Rayes & Salam 2019, 37, 263)

The platform layer is between the application and network layers. The IoT platform provides a place for data processing and it supports the functioning of the IoT applications. IoT platforms are fundamentally software products, that provide wide-ranging sets of application-independent functionalities that can be used to make IoT applications. There are different platforms available as a standard configuration of an IoT platform doesn't exist. (Wortmann & Flüchter 2015, 222-223; Ullah, Nardelli, Wolff & Smolander 2020, 1) There are many different analytics methods that can be used to find useful information from huge data sets so that it can be processed at a faster rate (Dey et al. 2017, 5). The communication between the IoT platform and IoT objects is critical in order to construct a good platform. One of the key components of this communication are Application Programming Interfaces, also known as APIs. (Lee et al. 2017, 2, 4) APIs facilitate the controlling of the functionalities of the IoT and smart objects to ensure the common standards are followed in order to secure interoperability which may sometimes be difficult because of the variability of the device

technologies. (Rayes & Salam 2019, 98; Karolewicz, Bebn, Batalla, Mastorakis & Mavromoustakis 2017, 1).

Several firms develop different kinds of IoT platforms which help companies to quickly develop and utilize IoT services in their businesses. These platforms are especially important for companies that do not have employees that understand the different fields of IoT. New IoT platforms are emerging all the time and they offer possibilities for companies' IoT solutions. The small size, easiness of using and low costs of hardware platforms have affected to companies' quick deployment of IoT. (Lee 2019, 2-3) Most of the IoT platforms provide heterogeneous ways to access IoT objects and the data collected by them. This may cause interoperability issues when developers pursue to create cross-platform and cross-domain applications which can prevent the emergence and functioning of IoT ecosystems. (Broring, Schmid, Schindhelm, Khelil, Kabisch, Kramer, Le Phuoc, Mitic, Anicic & Teniente 2017, 55)

The application layer is the one that is the most visible for a user as it provides the interface (Lee et al. 2017, 2). The layer includes a collection of problem-specific applications which are able to interact with users, solve and share issues and their solutions with other applications. The applications software coordinates the communication between people, systems and objects. This layer is also in charge of integrating data and information, as well as of displaying the them to the users in a convenient way. (Lee 2019, 7; Wortmann & Flüchter 2015, 222-223) Often numerous IoT platforms are used to develop domain specific IoT applications. Developing an IoT application is not a simple job. As the IoT systems are complex, the development process can be very time-consuming. Traditionally there are several things that need to be taken into consideration, like for example networks, routers, firewalls and scalability while making the system able to interact with all of the components. In addition, the developer has to take into consideration how the application could scale several geographically distributed users (Jiehan, Leppänen, Harjula, Ylianttila, Ojala, Chen, Hai & Yang 2013, 651; Lee 2019, 4), especially during times when most of the employees are remote working.

Developing IoT applications can be difficult because of several reasons. First of all, distributed computing causes high complexity. Second, there are no general guidelines about dealing with low level communication. Also, there are many programming languages available that can be used. Lastly, various communication protocols may cause issues as the developers need to simultaneously take care of the infrastructure as well as controlling the software and hardware layers. (Ammar, Russello & Crispo 2018, 8) The implementation

of an IoT product often requires merging various components into a multi-layer stack of IoT technologies (Wortmann & Flüchter 2015, 222-223).

3.2.1 Internet of Things

Technological leaps have led to big changes especially in the field of manufacturing and therefore, they are named as industrial revolutions (Lasi, Fettke, Kemper, Feld & Hoffman 2014, 239). The fourth industrial revolution or the digital revolution, is shaping the world and businesses right now. The first industrial revolution was about increasing the efficiency of manufacturing through water and steam power, the second was about bringing electricity to manufacturing industry, whereas the third industrial revolution focused on automation of operations. The fourth industrial revolution concentrates on digitization processes and increased usage of information technologies looking for better efficiency and productivity. Although the first three industrial revolutions had an impact mainly on manufacturing industry, the fourth industrial revolution is different compared to them because it affects all the fields of life and new emerging technologies speed up the change even more. (Chiţiba 2018, 72-73; Ślusarczyk 2018, 232; Roblek. Meško & Krapež 2016, 1; Weking, Stöcker, Kowalkiewicz, Böhm & Krcmar 2020, 2)

This fourth industrial revolution concentrates on digitization of the whole process and seeking completely integrated solutions that utilize technology as well as enhancing the whole value chain from customers to suppliers. IoT related technologies have been crucial for the creation of Industry 4.0. (Xu, Xu & Li 2018, 2942, 2945; Rojko 2017, 8) IoT is one of the main enablers and key components of Industry 4.0 as it is expected to provide new solutions for many different businesses, products and services. IoT technology enables developing new products and services practically in every industry. (Weking et al. 2020, 2; Roblek et al. 2016, 3, 8) With the help of IoT even traditional business can shift into a digital paradigm with better connectivity, ability to collect huge amounts of data and analyze it with the help of big data. (Aheleroff, Xu, Lu, Aristizabal, Velásquez, Joa & Valencia 2020, 2)

IoT is a major technology trend. The IoT revolution is known especially for its connectivity and providing end-to-end solutions. New innovations that combine fields of communications and computing can lead to developing new smart devices that can enable user-machine as well as machine-to-machine interactions. (Dey et al. 2017, 10) More and more products are built with embedded sensors that can collect and process data about the changes in its environment. These products are also connected to people via internet so that they can

communicate collected data to people and other products. (Strange & Zuccella 2017, 175; Lee & Lee 2018, 6860) IoT will have an effect on various fields of everyday life of everyone (Atzori, Iera & Morabito 2010, 2787). IoT and its applications become more popular all the time. Increasing number of IoT devices collect huge amounts of data and new applications are developed in order to offer more precise and better services. (Cui, Yang, Chen, Ming, Lu, & Qin 2018, 1399-1400) IoT is a crucial part of development of smart services (Ge, Bangui & Buhnova 2018, 601). Health care is among smart cities, smart inventories and smart homes one of the most potential application fields of IoT technologies (Miorandi et al. 2012, 1509). Utilizing open source solutions has gained popularity over the years. It means publishing a code or hardware design that can be reused, altered, improved and possibly even used in commercialization. The open source development speeds up the whole development of IoT over a longer period of time. (Rayes & Salam 2019, 315-316)

IoT is often considered to consist of “Internet” and “Things”. Also, data as well as processes and standards can be added to this concept. Things can actually be anything from cars to people and trees. Internet obviously connects these several things in order to exchange data by utilizing standards that ensure interoperability and allowing the system to use mostly automated processes. With the help of analytics, data becomes knowledge. (Rayes & Salam 2019, 3-4) Based on this IoT is presented the figure 4 below.

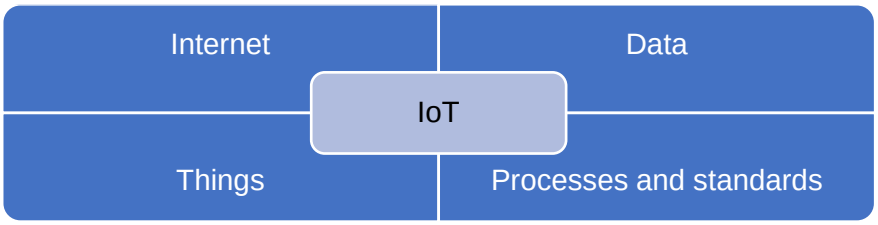

Figure 4. Internet of Things (Rayes & Salam 2019, 3-4)

Devices that are connected to IoT and have memory are known as smart objects which are able to interact with each other (Weking et al. 2020, 2). Smart objects are the basis of IoT. They have a unique identity and the ability to sense the environment and store the data. They are also able to communicate through internet with other objects and make autonomous decisions and thus, provide different kinds of services. In order to manage complex IoT services, the IoT infrastructure should be well-designed. (Sánchez López, Ranasinghe, Harrison & McFarlane 2012, 295; Lee et al. 2017, 1) IoT devices collect large amounts of data and then transfer it to different kinds of analytics tools. With the help of

these tools enterprises can understand the collected data better which can help them in decision-making. It is possible to control IoT objects remotely through internet which enables better integration between physical objects and computer-based systems. (Rayes & Salam 2019, 2)

Different technologies need to be integrated efficiently in order to achieve success with IoT. The most popular sensing solutions are RFID (Radio Frequency Identification) or sensors embedded in the objects. They are in a key position in IoT systems as they offer the possibility to identify objects and track their condition as they sense the environment and provide output for applications. RFID is based on tags and readers. The tags have a microchip and an antenna which together capture, store and process data and transfer signals. Sensors on the other hand often acquire data by using physical interfaces, known as inputs, which observe the surroundings and then, transform the input signals into electrical signals, outputs, that are read by the computing devices. There are different kinds sensors that can be used to measure almost anything. (Sánchez López et al. 2012, 291-293; Rayes & Salam 2019 70; Lee & Lee 2015, 432)

Lee and Lee (2015, 433-434) have identified three IoT applications for companies. First of them is monitoring and controlling systems that acquire data which give companies a chance to follow the IoT devices in real-time anywhere which enables, for example, identifying potential improvement possibilities and optimizing functions. The second application is big data and business analytics that can be used to discover changes in the measured object and to understand the collected data. The last application is information sharing and collaboration which is crucial for IoT because the objects need to be able to exchange information either with each other or with several people in different locations. IoT solutions can facilitate information sharing which can assist, for instance, avoiding delays in supply chains and increase situational awareness. IoT has several unique characteristics which make it such a successful concept that can be applied to almost any field of business nowadays. These characteristics enable versatile usage of IoT. The most important characteristics of IoT are presented in the figure 5.

Figure 5. Characteristics of IoT (adapted from Patel & Patel 2016, 6123; Čolaković & Hadžialić 2018, 20; Atlam & Wills 2019, 26-28; Ray 2018, 295)

The most important characteristic of IoT is its connectivity: the ability to be connected anywhere anytime with anything or anyone through a worldwide network. IoT is based on sensing and gathering information about the environment using an integration of various technologies. Therefore, sensing is also one of key elements of IoT. IoT is known for its large scale because there are billions of devices connected to the internet. Also, intelligence is a big part of IoT as the goal is to get the devices to make autonomous decisions. IoT devices are able to function in dynamic environments and to react to changes. Unique identification of IoT refers to the unique identity and identifier, like IP address, that all the IoT devices have. There are different kinds of platforms and networks that IoT devices are based on and thus, several authors describe them and the IoT data created as heterogenous. In addition, IoT devices are self-configuring. (Patel & Patel 2016, 6123; Čolaković & Hadžialić 2018, 20; Atlam & Wills 2019, 26-28; Ray 2018, 295)

IoT has led to an increased number of collaborative relationships due to its inter-connected nature. These relationships may be across different industries which on the other hand, can also make them more complex. As IoT enables carrying out new tasks that have not been

possible before through data collection and sharing, it also enables creating new business models. (Ju et al. 2016, 883, 889) An important part of IoT infrastructure is the applications provided by it. Through those applications users are able to access data, analytics and visualizations. (Dey et al. 2017, 6) Visualization of the data is an important part of IoT applications as it helps to extract useful information from the collected data. Touch screen technologies have become better and therefore, accessing applications has become easier and it is possible almost anywhere. (Gubbi et al. 2013, 1649) The number of companies that utilize IoT solutions in their businesses is increasing faster than ever before and more companies are expected to start utilizing IoT technologies in the near future. IoT is considered as one of the most influential of future technologies and therefore, it has gained more attention among different industries as well as researchers. (Lee & Lee 2015, 431, 434-436)

Companies often want to adopt IoT systems because of the benefits that they wish to achieve. First of all, it enables collecting and analyzing data in real-time for decision-making and faster response times. Companies can also provide more flexible services because of better quality of analytics they can perform. Increased amount of data allows better understanding of the object that is measured. Through IoT it is also possible to improve forecasting and the accuracy of analyses. Better planning is possible due to this. Diverse data sources can give new insights and help to prepare better for possible unexpected events. Also, automation of decision-making can lead to significant time savings. In addition to time savings, IoT can lead to cost savings, increased efficiency of operations and services. However, sometimes adaptation of IoT may cause unwanted structural changes. (Brous, Janssen & Herder 2020, 1-4, 12; Rayes & Salam 2019, 2) One of the biggest issues regarding IoT is the full interoperability of the devices which enables higher intelligence of the system which facilitates their adaptation and usage (Atzori et al. 2010, 2788). Standardization is in a key position in the development of IoT (Li et al. 2015, 255). A problem is that nowadays many firms develop IoT systems for their customers based on their wishes without paying attention to the company's system's ability to communicate with other similar systems (Ganzha, Paprzycki, Paelowski, Szmeja & Wasielewska 2018, 103).

3.2.2 Cloud computing

Cloud computing is an Internet-based IT service model through which computing services are provided to customers on-demand. (Madhavaiah, Bashir & Shafi 2012, 163; Marston, Li, Bandyopadhyay, Zhang & Ghalsasi 2011, 177) There are numerous" as a service"

models available in the market. Together with big data, cloud computing enables these new service models. The trend is called everything as a service, also known as XaaS. (Duan, Fu, Zhou, Sun, Narendra & Hu 2015, 621) Cloud computing provides solutions for issues that IoT may face, like problems with data storages or communications between things. Nowadays it is important that employees are able to access company's applications and services anywhere through the internet. This has increased the demand of cloud-based solutions. Cloud computing has practically endless capabilities regarding, for example, data storage and processing power, it is more mature technology which has most of the IoT problems at least somehow solved. Therefore, cloud computing is a crucial technology for the delivery of these services. (Botta, de Donato, Persico & Pescapé 2016, 684, 687; Lin & Chen 2012, 534)

A cloud service consists of the software and the computing infrastructure on which it operates (Jhang-Li & Chang 2016, 631). It provides a virtual infrastructure that combines monitoring devices as well as analytics and visualization tools. WiFi and other internet connections become all the time more popular which enables collecting and accessing ubiquitous information. (Gubbi et al. 2014, 1645) As IoT applications need large data storages, high processing speed to ensure that real-time decision-making is possible and quality networks to stream the acquired data in order to function, cloud computing offers a good back-end solution to beat these challenges. (Lee & Lee 2015, 432) In general, cloud is considered as a good way to compensate the technological constraints of IoT. (Botta et al. 2016, 687) Cloud computing offers companies a chance to outsource their computing infrastructure completely or parts of it to cloud service providers that rent access to their computing resources (Rayes & Salam 2019, 19; Lin & Chen 2012, 534). Four service provision strategies will be presented in the table 2.

Table 2. Service provision strategies (Solberg Søilen 2006, 43; Marston et al. 2011, 178; Maresova & Klimova 2015, 3909; Padilla, Milton & Johnson 2015, 1; Femminella, Pergolesi & Reali 2018, 512; Botta et al. 2016, 687)

Cloud service model	Description
Data as a service (DaaS)	Companies can buy or rent data as a service. The users may see only the analytics based on the data instead of the raw data.
Software as a Service (SaaS)	Applications can be utilized on the cloud which means there is no need to install application on the customer's computer.
Platform as a Service (PaaS)	Allows companies to use a third-party platform in order to control, develop and manage applications within the cloud infrastructure.
Infrastructure as a Service (IaaS)	Storage, processing and networking resources can be bought as a service. Subscribers are able to use the cloud infrastructure to adapt and run operating systems as well as several applications.

A common factor for all of the strategies is that data is a key resource. When buying data as a service, it needs to be evaluated how to measure the value of rented or bought data and how to maximize it (Solberg Søilen 2006, 43). Among cost reductions, SaaS can offer strategic mobility and better quality of service. SaaS has potential to become bigger than traditional IT service delivery because of its convenience and flexible cost structure. Especially, the usage-based pricing attracts smaller companies. As SaaS is a complex solution, there are usually multiple parties involved in the production of the service. Therefore, some big global companies, like Oracle and Amazon, have cooperated in order to produce software services. (Yan, Guo & Schatzberg 2012, 96; Jhang-Li & Chang 2017, 650). PaaS facilitates the usage of platforms as there is no need to build and maintain the platform infrastructure. A lot of time and money can be saved. (Rayes & Salam 2019, 20) IaaS on the other hand provides users the possibility to customize more as they have full control over virtual machines (Li & Li 2013, 867). Companies can achieve many benefits through cloud computing, like for example, cost reductions, better hardware resources, new innovations and delivering services that they haven't been able to deliver before. Cost

reductions can be achieved through decreased infrastructure and maintenance costs as well as energy savings as those costs are usually quite high when having a traditional server. Perhaps the biggest concern about cloud computing is losing control over company's critical data. (Marston et al. 2011, 178, 181)

There are public, private and hybrid clouds available. Public clouds are provided by a third party through internet. Costs are smaller than private clouds and thus, they are usually utilized by small and medium sized companies. For instance, Google provides public cloud services. Private clouds offer better flexibility and control over the infrastructure, and therefore they are suitable for bigger companies. (Marston et al. 2011, 180) Hybrid cloud is a combination of the private and public clouds. It gives companies a chance to exploit the infrastructure of a public cloud, but they retain control over their critical data. (Rayer & Salam 2019, 20)

Padilla et al. (2015, 14-16) have identified five components that create value for customers in B2B cloud services. First of them is service quality which refers to service reliability and consistency. The second component is service equity which includes i.e. brand reputation. The reputation of the service provider is important also for the customer company. Confidence benefits is the third component that creates value. It refers to provider's trustworthiness, e.g., whether the customer can trust the service provider with their sensitive data. The fourth component is perceived sacrifices which is about the cost and time that customer needs to use in order to use the service. The final component is cloud service governance, which is about, for instance, data migrations and security as well as service level agreements.

3.2.3 Data characteristics

As the data sources are heterogenous, it is important to develop IoT platforms that can handle different kinds of data. (Lee & Lee 2018, 6860) In addition, the data collected by IoT devices is raw and it can be structured, semi-structured and unstructured; data can be as, e.g. text, photos or videos. The different types of data are described in the table 3. Furthermore, the amount of collected data is enormous. As the data is raw, there needs to be techniques to transform this raw data into knowledge. It should be "extracted, classified, abstracted and analyzed". (Cai, Xu, Lihong & Vasilakos 2017, 76) Data mining provides one possible tool to create valuable information from the collected data. It is a big challenge to

handle the amount of data produced by IoT devices efficiently and to meet all the other requirements, like timeliness. (Stankovic 2014, 5; Phan et al. 2014, 117)

Table 3. Types of data (Loose 2006, 441)

Type of data	Definition
Structured data	Data is in a highly regular form, like in tables.
Semi-structured data	Data contains the same information as structured data, but the regularities do not apply to all of the data.
Unstructured data	Data can be in the form of, for example, text or images. It contains some kind of information but doesn't have an explicit structure.

The amount of data collected by IoT devices is large, but the quality is also quite good compared to data that is collected using traditional practices. There are several reasons for it. First of all, the data is usually more accurate and real-time. The data also has higher heterogeneity as it is collected from various sources. Multisource data needs to be combined in order to achieve a complete and broad view of the data. The process of combining data from different sources is called "multisource data fusion". IoT allows data collecting to be effective and therefore, the volumes are high. Better timeliness and higher volumes of gathered data that IoT enables can improve the performance of a company and the capability to react faster to unexpected events. (Brous et al. 2020, 3; Cai 2017, 77) Data science is about finding tools and techniques to analyze huge amounts of data and to understand it better. Data science consists of various scientific fields, like data mining and machine learning, in order to discover patterns and regularities of data. With the help of data science, IoT applications can become more intelligent. (Mahdavinejad, Rezvan, Barekatain, Adipi, Barnaghi & Shetsh 2018; Ghosh, Chakraborty & Law 2018, 209)

As IoT devices collect data all the time, the IoT data needs large storage spaces (Cai 2017, 78). The huge increase of data means also tougher requirements on data storage and management. There are two important tasks for data storages: offering a reliable storage space and providing an efficient access interface for data queries and analysis of big amount of data. (Chen, Mao & Liu 2014, 189) Cloud storage is the most often used platform to store big IoT data (Ge et al. 2018, 605). Databases can be used for short-term or long-term storage. IoT systems often utilize unstructured databases which are called noSQL

databases. They offer a mechanism for storing and retrieving data. NoSQL databases do not have a schema which enables quick deployment of it, however some maintenance problems may occur. (Serpanos & Wolf 2018, 12; Cai et al. 2017, 76) There are several databases available on the market. Choosing the right one is a strategical question and it depends, for instance, on the data types and on the usage of the data (Phan et al. 2014, 124). As IoT becomes all the time more popular and it consumes more bandwidth, in order to improve effectiveness and response times, data centers are becoming more distributed (Lee & Lee 2015, 438).

3.2.4 Big data analytics and IoT

Among monitoring devices' environment, mining the information acquired by the IoT devices is one of the most important tasks of IoT. (Ahmed, Yaqoob, Hashem, Khan, Ahmed, Imran & Vasilakos 2017, 459). Companies need to have effective process in order to really understand the high-volume and diverse data. Therefore, big data is important. Gandomi and Heider (2015) divide big data into two parts: data management and analytics. The first one is about storing the collected data and preparing it for analytics which refers to techniques that can be utilized to analyze and understand data better in order to gain knowledge from it. (Gandomi & Haider 2015, 140) Big data technologies provide data storage and processing services for an IoT system. Big data can create remarkable value by making information easier to analyze and more usable to companies which can help them to improve their performance. (Ahmed et al. 2017, 465-466) There is no one specific big data technology for IoT domains. Thus, choosing the right technology depends on the situation and needs. For instance, in IoT health care decision trees and feature extractions are often used. The integration of big data and IoT has led to development of new, more complex, businesses and services like smart cities. (Ge et al. 2018, 602, 606)

IoT devices can be used in almost any industry which means that the role of IoT will grow significantly in future. IoT can be seen as one of the largest sources of big data as well a big market share of big data applications and analytics. (Ahmed et al. 2017, 468; Ahmed, Choudhury & Al-Turjman 2019, 124). Nowadays, the amount of data produced by IoT is huge and the complexity of it means that it cannot be handled utilizing the traditional data analytics tools. Even small delays in the data processing can cause massive damage to companies' businesses. (Peek et al 2014, 42; Rayes & Salam 2019, 19). According to Ahmed, Choudhury and Al-Turjman (2019) the success of IoT is based on the efficient

integration of big data analytics. As deploying IoT has become more popular, more data is produced all the time which enables development of big data. (Ahmed et al. 2019, 109)

The importance of data analytics is nowadays emphasized more than ever and its meaning for IoT is undeniable. Companies are interested in data and the knowledge that can be extracted from it. (Ahmed et al. 2019, 118) The goal of big data analytics is to help companies understand the collected data better and based on it to make well-informed decisions. There are various big data analytics methods, like clustering and classification. IoT data differs from normal big data that is collected by other systems as the characteristics of IoT data are different. The data is very heterogeneous and increases at a high speed which also makes the size of big data grow rapidly. Integrating IoT and big data processes can help to solve data storage and analytics problems. Utilizing big data in IoT has become quite essential. (Marjani et al. 2017, 5248-5251, 5259) The possibility of online analysis is very important for IoT as the embedded sensors are collecting data all the time and as the sensors are possibly in various locations. (Ahmed et al. 2019, 119).

The main computational challenge of big data sets is the size of them (Peek et al. 2014, 44). Data, especially data, which is collected by sensors, has a high level of redundancy which needs to be reduced in order to achieve trustworthy results from analyses. Therefore, the presentation of data is extremely important. If the data is not represented in a proper way, it can have remarkable effects on the quality of data analysis and therefore, it can even have an impact on the company's operations. (Ahmed et al. 2019, 112) One of the most important key requirements of IoT is to enable combining and integrating huge volumes of heterogenous data (Ahmed et al. 2017, 463). Quite often the data is transferred to a cloud storage (Rojko 2017, 77). Adopting cloud services can lead to cost savings as there is less infrastructure to support, even though the deployment process may be expensive. Good education and training courses of employees can ease the implementation process. (Jhang-Li & Chang 2016, 651)

3.2.5 Utilizing machine learning in IoT applications

Artificial intelligence, AI, can be used to interpret external data properly and to gain information from it. The information can be used to achieve goals and other responsibilities. It is a technology that aims at getting computers to do human-like reasoning which will increase the usage of technology in many industries. AI utilizes external data collected by the IoT devices or other possible sources of big data for identifying hidden rules and patterns

based on approaches from machine learning, ML, which includes methods that assist computers to function without actually being precisely programmed. ML is one of the subfields of computer science. (Kaplan & Haenlein 2019, 17; Mahdavinejad et al. 2018, 165; Ghosh et al. 2018, 208) AI can be used in IoT for pursuing independence of the machines which can lead to saving time and money. The complete control over the machine should not be lost but the goal is to achieve a situation where there is no need for round-the-clock supervision. Adding AI to IoT systems makes the devices become intelligent. (Poniszewska-Maranda & Kaczmarek 2015, 1346, 1348)

Machine learning is often used for analytics for the IoT applications. Machine learning is one of the most used technologies of intelligent network management and operation. IoT solutions have become more dynamic, heterogenous and complicated which also makes the management of them harder. Machine learning can be used to find valuable information and features hidden in the collected data which gives users a chance to obtain deep analytics and build smart IoT applications. (Cui et al. 2018, 1400, 1414) ML can create possibilities to help forward devices' ability to make autonomous decisions. Machines are being develop all the time and they are more capable of performing less-routine jobs. (Ghosh et al. 2018, 208)

3.3 Risk management

Companies that utilize IoT faces different kinds of risks, for instance, related to its proper use, management and the data acquired through growing number of interconnected things. The risks that will be handled here are service supply chain, IoT security, business and data management risks. These aspects were chosen as they are the most essential risks that are studied in several researches. (Brous et al. 2020, 6, 14, Lee & Lee 2015, 438) One of the most important part of a company's strategy is how they cope with uncertainty in their environment. Their strategic choices have an impact on the company's exposure to uncertainty within the organization and its environment which on the other hand, has an effect on their performance. (Miller 1992, 312) IoT deployment is a challenging process while the company needs to harness the economic value and identify multiple risk factors at the same time. These new technologies may create new types of risks that existing risk management methods are not able to predict or mitigate. (Radanliev, De Roure, Nicolescu, Huth, Montalvo, Cannady & Burnap 2018, 14)

Service supply risk management can be defined as “identification, analysis, and mitigation of risks in the service supply chain, involving the whole service supply chain system”. There aren’t many studies about service supply chain risk management as the subject is quite new. If the processes of the service supply chain are not understood, it makes understanding the risks more difficult. Vilko and Ritala (2014) divide the service supply chain risk analysis into three perspectives: service process, service offering and service system. As these levels are more intertwined than those in traditional supply chains, the importance of risk management increases. Service process is about supply chain activities and the risks that may escalate from this level to other levels. The risks need to be efficiently identified, analyzed and controlled. Service offering concerns the supply chain actors. The risk management needs to identify and examine the customer-specificity and how value is created for their clients. Service system focuses on the risks of supply chains and networks. In risk management, a coherent approach towards clients, paying attention to the intangible nature of services, understanding the heterogeneity of actors involved and the complexity of offered services are important. These different perspectives will be taken into consideration in the following chapters. (Vilko & Ritala 2014, 114-118)

3.3.1 IoT security

The security issues related IoT are widely recognized and addressed in the literature. Security is an important aspect when adopting IoT technologies and applications especially in situation where there are several actors involved in producing an IoT solution. The IoT system is only as secure as its weakest parts are (Serpanos & Wolf 2013, 13). According to Miorandi et al. (2012, 1505) security problems of IoT can be divided into three aspects: data confidentiality, privacy and trust. More information about these security problems is provided in the table 4.

Table 4. Security problems of IoT (Miorandi et al. 2012, 1505)

Aspect	Description
Data confidentiality	Only authorized people and objects should be able to access data. This is especially important in health care as the data can be very sensitive.
Privacy	The rules defining who can access data that includes information about individual users.
Trust	The dynamic nature of IoT makes the trustworthiness challenging. In addition to trusting the other actors involved in the supply chain, also people should be able to trust the objects as well.

Data confidentiality is one of the biggest issues concerning IoT applications as there may be several actors that can access data. It ensures that the messages in the network can be understood only by the users who are allowed to do so. Controlling access to data is extremely important. Privacy refers to defining who are able to access data concerning individual users. Privacy issues are important to take into consideration because there might be data about, for example, users' locations and especially in health care applications as the devices may collect personal and sensitive information. Trust is about whether the parties involved in the IoT supply chain have mutual trust towards each other, especially when the nature of IoT is so dynamic which can make the trust relationships hard. (Miorandi 2012, 1505-1509; Lee & Lee 2015, 439; Li et al. 2015, 253) Also, authentication, integrity and availability are important security requirements for IoT. Authentication means that the actors involved in any operation are who they claim to be. Integrity is about ensuring that the exchanged messages are not altered by external parties. Availability ensures that there are no interruptions in the services. Forward secrecy means that when an object is removed from the IoT system, it will not be able to understand the communication that happens in the system anymore. Backward secrecy makes sure that if a new object joins the network, it cannot understand the communication that has occurred before joining the network. Both of them should also be taken into consideration when managing an IoT system. (Rayes & Salam 2019, 214)

The number of IoT devices in the network grows continuously which increases also the security risk. IoT can enhance the performance of firms and improve the quality of life but at the same time IoT provides cyber criminals a surface for attacks. (Lee & Lee 2015, 439) The security risks are critical especially when an IoT system is a part of company's operations. If someone is able to hack a smart object in the system, the sensing capabilities can be used to spy the company and to steal some extremely valuable and sensitive information. Also, impersonation attacks can occur which means that someone claims to have another identity than their own. Protecting individual users' privacy is also very important as the collected data can tell a lot about people's lives. (Rayes & Salam 2019, 212, 214) It is critical for organizations to include cyber security measures and processes that minimize cyber risk regarding IoT products, platforms and services in their strategies (Radanliev et al. 2018, 14-15). Even though the characteristics of IoT devices make it successful, they also make the network more vulnerable than traditional networks. The devices often have low battery and micro-controller and therefore, can be easily flooded. IoT devices communicate, for example, through Bluetooth, WiFi or 4G which are vulnerable to attacks. (Cui et al. 2018, 1406) Each of the IoT layers should include a security solution in order to protect them from possible safety hazards (Lee et al. 2017, 3).

3.3.2 Business risks

Privacy and safety related risks are not the only ones that companies may face. There are other business-related risks as well. Business risks are related to the parts of business value proposition where there is considerable uncertainty (Anderson 2014, 11). As deploying an IoT solution can be such a big change, it can create a lot of uncertainty. Business risks are diverse and depend, for instance, on company's industry and the size of it, competitors and government measures. They are mainly affected by the management's ability of assessing company's resources and making successful decisions. Business risks can be divided into four groups: technical risks, social risks, financial risks and political risks. Technical risks are related to, for example, raw materials or production. Social risks can be caused by, for instance, boycotts towards company's products. There are many factors that can cause financial risks. For example, decreased profits due to changes in demand. Terrorism or other unexpected accidents that have huge effects can be defined as political risks. (Suominen 2003, 51-53)

IoT affects the business models between companies and the relationship between them becomes tighter and more dialogue-based instead of unidirectional and short-term

relationships. However, one possible risk related to these relationships is unbalanced power relations between the actors involved in the service supply chain. This unequal power distribution can lead to a situation where the supplier is highly dependent on the buyer, or vice versa. These kinds of situations create uncertainty especially for the one having less power. (Boehmer, Shukla, Kapletia & Tiwari 2020, 213-214) There might occur some lack of acceptance towards IoT which means that companies need to develop trust in the new systems. The more users have trust in the new system, the more they are willing to participate in the adaptation. Even though utilizing IoT can lead to great economic benefits, for instance, due to automation of different kinds of processes, the adaptation process can also demand high investments causing a major financial risk for the company. Employees may need to be reassigned and re-educated which can increase costs. Also, there is a large variety of different kinds of devices with diverse capabilities make designing an IoT solution and communication protocols a challenge. Therefore, planning and deploying a new solution may take a lot of time and other resources as well. (Brous al. 2020, 5,13)

3.3.3 Data management risks

IoT is one of the most significant sources of big data among social media sites, sensor networks and machine-to-machine solutions. Sivarajah, Kamal, Irani & Weerakkody (2017) present in their research three main challenges regarding big data that are data challenges, process challenges and management challenges. Data challenges are caused by the characteristics of data. Process challenges are related to handling the data and preparing it for usage. Management challenges deal with issues regarding for example the governance and the safety of IoT. (Sivarajah et al. 2017, 263, 265) More information regarding these challenges is provided in the figure 9.

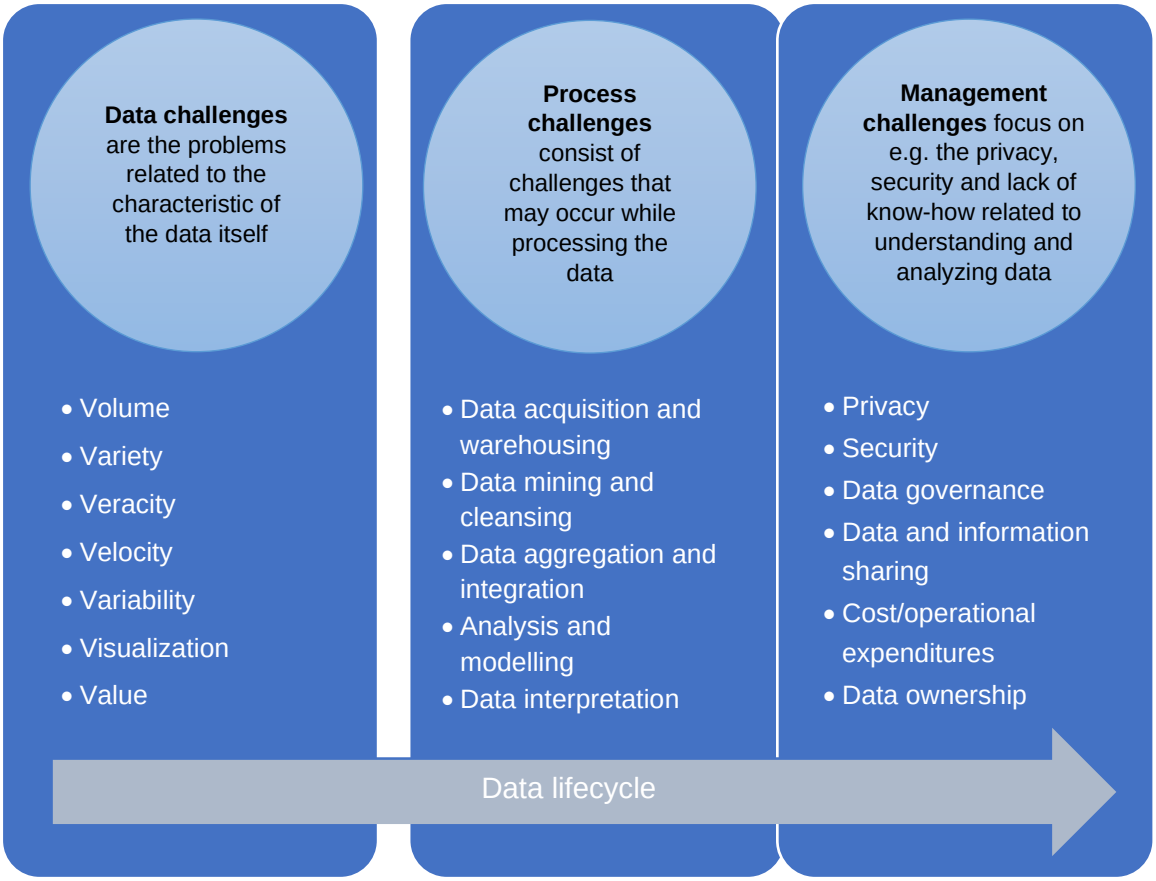

Figure 9. Data management challenges (adopted from Sivarajah et al. 2017, 265)

The characteristics of big data make it successful, but they also create some challenges around it. In this thesis 7 V's of data are used to describe the big data. The amount of data collected through IoT devices is enormous which creates different kinds of challenges. Also, the variety of data sources leads to a situation where the collected data is heterogenous and the possible interoperability issues caused by them can affect the adaptation of IoT and the integration of new systems to existing processes. The data may lack binding information that complicates the data processing and usage. Thus, the expected benefits can be significantly smaller than planned. In addition, the heterogeneity of data can lead to, for example, data quality issues and therefore, misleading information. Veracity issues refers to the fact that both, structured and unstructured data, can have reliability issues. Velocity is about the fast rate of data inflow with non-homogenous structure. Variability of data, referring to the constantly and rapidly changing meaning of data, creates big challenges for example, the analyzing processes. With the help of visualizations, the collected data can become easily readable and therefore, make the data related processes more efficient. However, the visualization of data can be difficult due to the large sizes of the data sets.

Finally, extracting knowledge from data can create value for companies. This makes data such an important asset for them. (Sivarajah et al. 2017, 269, 273-274; Brous et al. 2020, 5, 13)

The collected data is often so raw that it is hard to understand as such. In addition, the data can be different in terms of subjectivity and importance, and it can be anything from individual opinions to specific measurements. Examining, understanding and finding data patterns is crucial when huge volumes of data from several different sources are collected. The key challenge of IoT solutions is the intelligent integration of these large data sets in order to create new knowledge. Combining data from several data sources is beneficial as the same information may not emerge from analyzing separately the data sources. The data needs to be pre-processed through data cleansing. Having data from multiple sources can also cause noise and uncertainty which needs to be handled properly. The main objective of these processes is to help companies and users to utilize multi-source data to find useful information through mining and analysis. Structuring data in a way that it is easily and efficiently available for queries and different analysis tools is very important. (Karacapilidis, Tzagarakis & Christodoulou 2013, 227-228)

Based on the Sivarajah et al. (2017) research the process challenges are data acquisition and warehousing, data mining and cleansing, data aggregation and integration, data analysis and modelling and data interpretation. There challenges are mainly caused of the 7V's of big data. Data acquisition and warehousing problems are mainly caused by diverse data sources and the volume of data. Data mining, cleaning and analyzing can be challenging especially because of the noisy, dynamic and heterogenous nature of the data. The growing amount of unstructured data sets can cause integration challenges for companies. (Sivarajah et al. 2017, 273-274; Chen, Chen, Du, Li, Lu, Zhao & Zhou 2013, 161)

The sensitivity of data requires careful management. Besides privacy and security challenges there are other management challenges as well. The usage of data continues to increase which leads to growing need of data governance. Data governance means assuring data quality and ensuring that the value of data remains as a company asset. At the same time, the volume of data increases, leading to higher demand for data centers and thus, the workload in them is going to increase. The growing amount of data can lead to, for instance, security, privacy, management and server technology challenges. Data storage and processing costs can be very high. Data ownership challenges are complex, and they need to be solved in order to unleash the full potential of data. Data ownership

issues are often discussed, for example, in social media context as users create the content but basically the social media platforms can have rights to it. Information sharing is beneficial for service supply chains. Companies usually have their own data warehouses based on different kinds of platforms and technologies. The diversity of these systems and privacy regulations may lead to a situation where the actors are reluctant to share their data. (Sivarajah et al. 2017, 274-275; Otto 2011, 61; Lee & Lee 2015, 436)

4 METHODOLOGY

Before the empirical part of this research, in this chapter the used methodology is presented. First, the research context and more information about the testbed project will be presented. This study is conducted as a qualitative research and therefore, the method will be shortly explained. In addition, the data collection and analytics processes are introduced. The interviewees and case companies are going to remain anonymous in order to guarantee openness in the discussions. However, short case company and interviewee presentations will be given in order to provide some background knowledge about them. Also, the secondary data sources will be described. Finally, the process of evaluating the research quality will be examined.

4.1 Research context

The research context of the study is the network of actors delimited to companies that are involved in the ELSA testbed project and to companies that already offer solutions in the health care sector. The project is run by South Karelia Social and Health Care District, LUT University and LAB University of Applied Sciences. The goal is to develop an innovation hub that allows fast innovation, development, and prototyping especially for out-of hospital products through providing testing and other supporting services for companies. Other supporting services can be, for example, analyzing customer value or helping to develop the idea into a product or service. Testing services provide companies a possibility to test their solution within authentic environment with real customers. In this testbed also the users take part in the product and service development, and it is done where the end-user is. Thus, they get feedback from the end-users and also from health care professionals which can help them to develop their solution. Testbeds are also beneficial for health care providers as they get a chance to gain knowledge about solutions they may want to utilize in the future. Testbeds improve the cooperation between the private and public sectors and decrease the market risk of new solutions. One of the goals of testbeds is to provide also small enterprises a chance to develop their solution and test it with real users. Health care providers also have a possibility to network with other companies which can be very valuable for them.

4.2 Research method

Qualitative research method was used in this thesis. The data used in qualitative researches is usually nonquantitative in nature. This means the data can be, for instance, interviews, papers or videos. (Saldaña 2011, 3) The most common way to collect data is to do theme interviews within a few months. It is typical for qualitative researches not to pursue to find relationships between variables. Instead, the goal is to understand for example, how people feel about certain phenomenon. It pursues to provide a lot of information about a precise case. (Koskinen, Peltonen & Alasuutari 2005, 31, 44, 278) The qualitative method was chosen for the thesis as the aim is build an understanding about a fairly new phenomenon of IoT supply chain.

A case study examines a current phenomenon in depth and using a real-world context. Case study aims at explaining real-world phenomena, “cases”, that are too complex for surveys, enables illustrating different themes in a descriptive mode and offers a chance to enlighten a situation that doesn’t have a single set of outcomes. (Yin 2015, 16-19) A case study is one of the most popular research methods used in qualitative business researches (Koskinen et al. 2005, 154). One of the biggest benefits of case studies is that it provides a many-sided view of different situations. Based on these characteristics of a case study, it is clear that it is a good option for a research about business network. It enables studying the dynamics between the actors. One of the most fundamental questions of a case study is how to form the studied network as it is not possible to study the whole network. The general guideline for setting the network boundaries is the content of the research problem. The objectives of the study affect crucially the way a study should be delimited. (Halinen & Törnroos 2003, 1286-1288) The focus in this research is delivering and buying an IoT solution, so the previously described network limitations were made.

4.3 Data collection

Primary data is data which is collected specifically for a certain research through methods that fit best for the research. Often, the material that is created is published and made available for other researchers to use. (Hox & Boeije 2005, 593) The primary data for this thesis was collected through interviews which were done online in Teams due to restrictions caused by COVID-19. The benefit of interviews is their flexibility as they enable repeating the questing and having a conversation with interviewees. In this research the interviews were conducted as theme interviews. Theme interviews are semi-structured interviews

where the conversation is built on chosen themes. The advantage of theme interviews is the possibility to react better to interviewee's answers because it is possible to even add questions if needed. The effectiveness of theme interviews is based on interviewer's possibility to guide the interview without completely controlling it. (Tuomi & Sarajärvi 2018, 85-89; Koskinen et al. 2005, 104-105) The case companies are placed on different stages in the IoT supply chain which enables getting a broad perspective for the study. Also, their IoT solutions differ from each other which makes the setting for this research even more interesting. Especially having representatives from both customer and supplier companies provides a broad understanding about delivering and buying an IoT solution. In addition, the positions of the interviewees are different which enables getting diverse points of view about the subject. In total six interviews were done. The interviewees' positions in their companies and the used interview template are presented in table 4.

Table 5. Interviewees of the case companies

Interviewee	Position in the company	Company	Interview questions
Interviewee A	Product Manager	Company A	Template 1
Interviewee B	Owner	Company B	Template 1
Interviewee C	Chief Engineer	Company B	Template 1
Interviewee D	Director of Energy Business Line	Company C	Template 1
Interviewee E	Project Manager	Company D	Template 2
Interviewee F	IT Manager	Company D	Template 2
Interviewee G	CEO	Company E	Template 1

The interviews were done in September and October 2020 and each of them lasted from half an hour till one hour. The questions were sent to the interviewees via email in advance. The interviews were conducted in Finnish in order to have in-depth discussions as all of the interviewees were native Finnish speakers. With the interviewees' permission the interviews were recorded and partially transcribed afterwards. There was no need to transcribe them precisely as the goal was not to, for example, examine the interviewees' behavior. All of the interviewees were interviewed separately except for the interviewees B and C who were interviewed at the same time. The questions differed a little depending on the company's

position in the IoT supply chain. The list of questions can be found in the appendix 1 and appendix 2. The questions in template 1 (appendix 1) were presented to the suppliers of IoT solutions and the questions in template 2 (appendix 2) were presented to the buyers of these solutions. The question template 1 was divided into four themes: IoT service supply chain, testbed experiences, IoT technology and risk management. The template 2 was altered a little because the health care service provider doesn't have experience about delivering an IoT solution.

Company A offers cloud-based AI-solutions that are meant for monitoring, supporting health and well-being. Company B's IoT solution is mainly based on collecting real-time information about people's living environment. Company C does not yet operate in the health care sector, but they are very interested in the possibilities the field may offer in the future. It is an industrial manufacturing company which currently offers their clients, for instance, software development services and they are looking for opportunities to use this knowledge in health care services. They took part in the testbed project together with another company. They had workshops where product development ideas were discussed with professionals. Company D is a public social and health care service provider and was one of the organizers of the whole testbed project. Company E provides smart solutions made especially for enhancing homecare. Additional information about the case companies is provided below in the table 5. Information about operating revenue and number of employees in table are based on data on Amadeus database. The newest available data was used. The operating revenues are rounded up to nearest ten. In addition, case companies are divided into three groups based on the services they offer.

Table 6. Information about case companies

Company	Operating revenue (in thousands)	Number of employees	Group
Company A	180 EUR (2018)	2	Service provider
Company B	100 EUR (2019)	2	Service provider
Company C	24 000 EUR (2019)	323	Technology provider
Company D	525 EUR (2019)	5000	Customer
Company E	60 EUR (2019)	3	Service provider

The possibility to use several data sources is a major strength when collecting data for a case study (Yin 2015, 119), which is why in this study besides the interviews, also additional data will be used. Usually qualitative secondary data sets include documents, videos or audio tapes (Hox & Boeije 2005, 594). Several data collection methods are used in order to get more perspective and therefore, improve the credibility and trustworthiness of the study (Saldaña 2011, 31). The secondary data used in this thesis are the documentation written during the project and one lecture video. The material includes more specific information about this testbed project, tests that have been done and the companies involved in the project. More information about the secondary data and the case company the material is about is provided in the table 6.

Table 7. Information about secondary data

Data source	Case company
Lecture video	Company C
Testbed contract	Company D
Testbed safety contract	Company D
Measurement results	Company B
Final report of a testing process	Company B
Workshop report	Company C

4.4 Data analysis

Content analysis is most often used in qualitative researches in order to analyze the collected data. In content analysis the collected material is systematically studied. Traditionally either inductive or deductive reasoning has been used in researches, but there is also a third method that combines these two, abductive reasoning, which was chosen for this thesis. (Tuomi & Sarajärvi 2018, 103, 121; Saldaña 2011, 3) In inductive reasoning there may not even be a theoretical framework and the research is based on empirical data. The goal is to make generalizations about the studied subject and possibly to create new theory. Deductive research is strongly based on theory and aims at drawing conclusions based on it and then testing hypotheses in an empirical setting. (Kovács & Spens 2005, 137) As there is no clear theoretical background about the subject and the aim was not to create such, abductive reasoning is suitable for this research as it can be used to find new insights to a phenomenon. There are many researches and a lot of knowledge available

about IoT and service supply chains but combining these two forms a new phenomenon that has not been studied yet. The abductive research process is presented below in the figure 6.

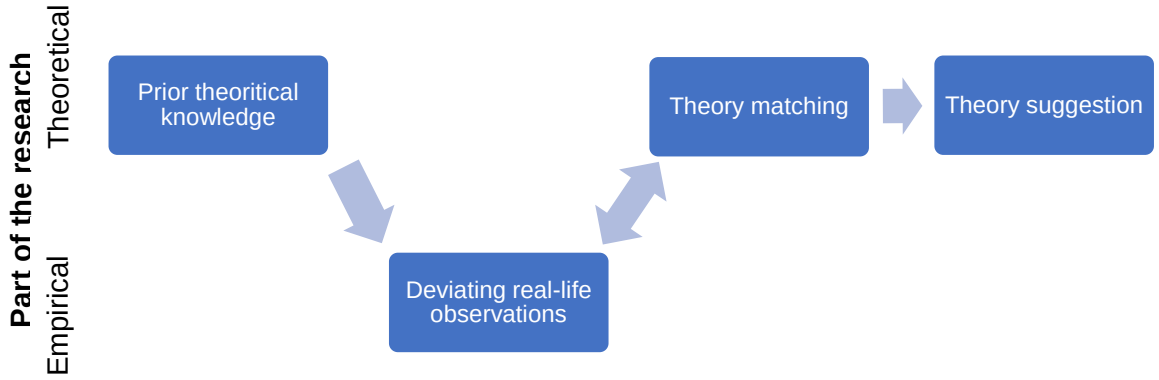

Figure 6. The abductive research process (Adopted from Kovács & Spens 2005, 139)

The research process begins with examining the previous studies made about the subject and overall the theoretical background. Dozens of articles were examined for the theoretical part of this study in order to gain broad understanding about the subject. The goal is to gain understanding about the research area and identify possible gaps there. Theoretical framework is chosen for the study. After studying the background, the research process proceeds to the empirical part which consists of real-life observations, in this thesis it consists of case company interviews and other material about the testbed project. The interview questions were made based on the theoretical part. The following step is theory matching, or systematic combining, which aims at matching theory and reality. Going back and forth between the theoretical and empirical parts helps to understand the studied phenomenon more deeply. Having several data sources can help to expose and understand new dimensions of the research problem. This will be done in the following chapters. After theory matching it is possible to make new theoretical suggestions. (Kovács & Spens 2005, 139-140; Dubois & Gadde 2002, 555, 559)

4.5 Evaluating research quality

Reliability and validity are extremely important ways to estimate the quality of the research. Reliability refers to the fact that if the same study was conducted again later, the results should be similar. In order to ensure the reliability of a study, the research procedures should be clearly documented. (Yin 2015, 48-49) Therefore, in this methodology chapter

the steps of this research process and the reasons for choosing them are presented. However, it is good to take into consideration that when studied phenomena and companies change over time, it would naturally also affect the results of a research. Stuart, McCutcheon, Handfield, McLachlin & Samson (2002, 430) divide analyzing the validity of a case research into three parts: construct validity, external validity and internal validity. The first one means that used data sources should be described. Having several data sources improves construct validity and therefore, interviews and additional materials about the project will be used. External validity refers defining the domain to which research's results can be generalized. A problem that often occurs in qualitative researches, is that it's often difficult to generalize the results because of the small sampling. However, often a small sampling is chosen because the goal is to have a very deep understanding about the studied subject and that is why qualitative research method was chosen for this study. Internal validity is not that suitable for descriptive studies and therefore, it will not be used to evaluate this research. (Koskinen et al. 2005, 258, 263-265; Stuart et al. 2002, 430; Yin 2015, 46)

5 EMPIRICAL FINDINGS

In this chapter the findings based on the interviews and the secondary data are presented. First, the summary of the findings will be presented. After this, there are three subchapters based on the services the case companies offer and the findings will be more deeply examined. The first of these subchapters is about IoT service suppliers. The following is focused on technology providers. The third subchapter is based on the answers by the IoT solution buyers. One of the goals of this testbed project was to build an innovative environment to the area which enables testing solutions in the future after the project as well. All of the case companies agree that it is okay for a third party, like the university, to utilize the data produced in a testbed process because it most likely benefits everyone. One of the main tasks of universities in testbeds is to provide companies product development ideas. In general, case companies considered testbed projects very beneficial.

Before the actual questions about the IoT and its supply chain, the interviewees were asked to tell a little bit about their main responsibilities and company. The case companies are founded between the years 1999 and 2018. They offer very versatile IoT solutions which enables getting a broad understanding about the subject. In addition, the interviewees are in very different positions in their companies, for example a CEO, a chief engineer and a project manager were interviewed, which provides different points of views for this research. All of the interviews began with a discussion about the framework of this study. The framework was shortly presented, and the different layers were explained to the interviewees. It was enhanced that the customer in the framework is the health care provider. After this, the interviewees were asked whether they would add or remove any stages on the framework. Interviewee A pointed out that big companies which offer IoT platforms also have a lot of focus on device management, like for instance, remote controlling of devices and software updates. However, as the company A operates in a specific application area, he doesn’t consider this kind of stages necessary for them. Company B representatives pointed out that technical and other support is provided to customers when needed. However, this can be seen to be included in the customer layer when the service is delivered to the client. Other interviewees considered the framework accurate and did not have ideas of additional stages which could be added.

5.1 Summary of empirical findings

The summary of the empirical findings is divided into three categories: IoT security, business risks and data challenges based on the risk management chapter. A summary of the most important findings is presented in the table 7.

Table 8. Summary of empirical findings

Aspect	Description
IoT security	The security of IoT solutions aroused concern among the interviewees. All of them regarded it as a very important issue that needs to be taken into consideration by all actors that are involved in the supply chain. The handled data in health care systems is very personal and therefore, the information security of the whole IoT supply chain is crucial.
Business risks	Deploying an IoT solution can be very expensive and lead to radical changes in health care organizations. Therefore, when making these investments, they need to make sure that the investments are reliable and ideally the relationship with the supplier becomes interactive and long-term. The uniqueness and complexity of the solutions may make it hard to replace them which can increase buyer's dependence on the supplier. Unbalanced power relations are not ideal for the business. Also, the nurses' and doctors' acceptance towards the new technology affects the usage of IoT solutions.
Data challenges	Almost anything can be measured nowadays. Identifying proper data sources and making sure that the devices function properly can be a challenge. There are several actors involved in acquiring the data which can result in data ownership issues. These issues can be solved through detailed contracts. Also, the willingness to share data with companies involved in the supply chain is an interesting topic.

Interestingly, all of the interviewees had similar opinions about the security and privacy issues. Of course, all of the stages in the IoT supply chain have different kinds of information security protocols. However, the same laws and regulations affect them all and therefore, they have to take the security aspect of IoT solutions very seriously. A common goal for all case companies is to ensure the privacy of the health care providers' customers. On the other hand, opinions about business risks and data challenges seem to depend on the company's position on IoT supply chain. The customer's biggest business risks are related to, for example, the investment, challenges if the supplier needs to be changed and making sure that employees and customers feel comfortable with the new technology. They were also more concerned about the data ownership issues. For the solution providers, for instance, mobile coverage, the reliability of devices and the accuracy of analyses and predictions can create challenges. Their answers will be analyzed more closely in the following chapters.

5.2 Service providers

Company A provides a cloud-based solution and they utilize a lot of different as a service-solutions, for example, database related services. Company B has about 5 to 10 suppliers. They buy, for example, special IoT networks as a service from another company. Traditional mobile networks can also be used for IoT solutions and they can be bought as a service from operators. Company B also utilizes cloud services in their solution. They purchase, for instance, sensors for their devices as well. Company E buys IT services, different kinds of cloud services, like platforms, and also networks. All of the companies have some requirements for their suppliers, depending on the bought product or service. However, there is something that is common for them all. As the health care related data is very sensitive, there are laws and regulations that affect the health care sector and their supplier network as well. General Data Protection Regulation, known as GDPR, regulates data usage in every company in Europe. In addition, in Finland a law concerning the handling of information about patients affects companies that operate in this field.

The service layer is especially important for the health care professionals. The systems should be easy and fast to use. It would be important that the new systems would be able to communicate with existing systems. Having data in several systems is inconvenient and difficult for the employees. When the data is provided for nurses and doctors in a visualized form which makes it easier and faster to utilize. For example, company B provides their

customers alarms via email, text messages and web services. The system is flexible as it enables users to set the limits for the alarms which improves the user experience.

Interviewee G points out that understanding both, the customer organization's and patients' needs, requires a lot of know-how. They need to understand the needs of their customer, meaning a health care organization, but also, for instance, the life of the elderly who still live at home. This can be especially challenging as combining IoT and health care is still on a fairly early stage of development. Even though they already have experience about the subject, understanding these needs is still going to require work in the future as well. Interviewee A states that there can be data compatibility issues regarding all machine-to-machine solutions, also IoT:

"As long as there have been computers, the same problem has existed, and it still has not been solved."

One of the biggest issues is ensuring whether the same data means the same thing in every context. However, the situation has gotten a lot better with new solutions as most of them are built with such features that they can be connected. Several interviewees said that security related issues are the most critical issues in IoT solutions. However, the security aspect of IoT came up somehow in every interview. All of the interviewees agree that security problems are significant, and a lot of attention should be drawn to the issue especially because the data is so sensitive. Interviewee A points out the consumer devices that collect data all the time have become more popular and especially in these devices there might be serious lack of security. According to the interviewee G there are bigger risks in solutions that are still being developed compared to solutions that are already in the market. If there is some kind of problem in the development stage of a solution and it is not noticed, it can cause big problems in the future and it can be harder to fix. The same interviewee also pointed out that one risk related to, for instance, automatic medicine dispensers is that the patient is given a wrong amount of medicine which can be extremely dangerous or even life-threatening.

Communication between a supplier and a buyer is crucial. When a smaller start-up company communicates with a large enterprise, getting feedback may take time. Companies should have clear processes in order to communicate efficiently. The communications between companies B and D improved when company D assigned a

specific person to take care of the communication with company B. Interviewee C also points out that mobile coverage is one of the most important requirements for their supplier. As their solution includes a device that is taken to the patient's home, it needs to function as efficiently in a city center as well as in the countryside. Interviewees B and C agree that information security has gotten a lot better lately. However, the development of it is still ongoing, and they believe that there is room for improvement, for example, regarding GDPR.

Developing an IoT solution for health care is definitely not an easy job. It requires a lot of time and other resources, like money, as well. For example, company B had their systems in testing environment for several months. During this time tens of thousands of measurements were made. These systems generate a lot of new data. Companies' job is to find the most important information from the data sets and ensure the quality of analyses. Interviewee G finds testbeds extremely useful and states that it has been essential for their solution development. Especially understanding the customers' needs and gaining knowledge about the health care sector have been crucial for the company. Also, learning to discuss more professionally is something that can be utilized in the future with other companies as well. One of the biggest benefits according to the participants is the opportunity to understand what the real needs of health care sector are right now and what kind of solutions are desired. It helps to realize how the solution should be developed and to which direction should the company aim next. In addition, several participants in testbed agree that gaining better understanding of the operations of customer organizations is useful and can possibly be utilized in public tenders as well.

One aspect regarding testbeds that came up in the interviews was the pricing model of them. In testbeds the companies that want to develop their solutions pay for the health care provider because the health care provider offers them valuable knowledge and even possibilities to test their solutions with actual customers. This might be an issue for smaller companies that do not have a large financial capital. This can lead to a situation where only bigger companies are able to develop their products and therefore, strengthen their position in the market. However, all in all the experiences about the testbed project has been very positive.

5.3 Technology providers

Company C has been involved in this testbed project in cooperation with other company. Together with professionals they were examining the possibilities of the IoT market and what kind of solution could be designed. Company C differs from other case companies also because of its size. At the moment they do not buy services from other companies. In case their clients need something that company C does not offer, they simple buy it somewhere else. Company C has a lot of experience of IoT and therefore, the challenge is not any more how to collect data and connect different systems. Nowadays the challenge is to figure out what to do with the data and how to utilize it as much as possible. They see the IoT system as bidirectional: data is collected and analyzed which can then help to optimize and control the devices in the field. The role of AI will be bigger as well in the future. They think it would be an ideal situation if different parties collected data and utilized it mainly themselves, but others could also use it in their decision-making. However, many companies are not interested in sharing their data with other and in some cases, there can be contracts that even prevent it.

Company C uses open interfaces as much as possible in order to avoid vendor lock-in situations where the customer becomes very dependent on their vendor. This gives their customers a chance to use services from other providers as well. As a big company it is understandable that there may not be enough resources to produce everything that their customers need. Interviewee D hopes that majority of interfaces could be standardized to ease the building process of IoT systems. Standardization would enable combining several systems from different companies and therefore, having a more efficient IoT system. Technology providing companies could concentrate completely on few products or services and let other firms to focus on other things. At the moment, most vendors are used to having their own interfaces.

People from case company C attended workshops with a company that could be a potential cooperation partner in the future. In the workshop there were representatives from the case company C, case company D and the university. The workshop included discussions about the utilization possibilities of the potential solution and what kind of problems could be solved with the help of this solution. Also, the possible risks were discussed. These kinds of workshops can cut down the problems that companies may face in the future in service supply chains when the solution is actually in usage. When experts from different fields innovate together, they can come up with more imaginative business ideas. Developing the

solutions together can help to avoid possible pitfalls and challenges caused by them in the future.

Interviewee D sees testbeds as an interesting concept and specially a good opportunity to gain understanding about the sector. He thinks that the need for IoT and AI in health care will grow in the future. Health care becomes more digitalized all the time and IoT and AI are part of this digitalization. They enable, for instance, visualization of data and knowledge management. Big part of work related to AI processes is about cleaning and modifying data in order to be able to run machine learning algorithms. IoT and AI are going to affect the work of doctors and nurses on a daily basis, for example, making reporting easier and providing them real-time information which can also enhance planning of workdays. More efficient processes may even give the professionals more time to meet their patients which can lead to improved customer satisfaction. In addition, families can receive real-time information about the patients which can be very useful. Interviewee D points out that taking care of information security in pilot projects is extremely important. Even though a solution is only tested or developed, the information security cannot be ignored.

5.4 Customer

Both of the interviewees E and F agree that main criteria for choosing IoT solution is to have a clear need for the solution. Financial benefits are not the only ones that can be achieved through IoT solutions, for example, the goal might be to improve the life quality of the patients. Having some certificate requirements is one way to ease the supplier selection process. In addition, a factor that affected choosing the service provider for testbeds has been the motive of the service provider. Testbeds are organized especially for testing and developing new services and products. Therefore, when choosing companies for testbeds, it is important to make sure that the companies have a genuine desire to improve their solution. Testbeds should not be considered as a way to enter the market. As a public authority company D needs to take the act on public procurement into consideration. In case there was a functioning solution in the testbed that could be utilized in the future, they would still have to put the solution out to tender. Also, the information regarding, for instance, the service’s content and price should be clear and achievable. Careful planning is the first step in the process. Proper contracts need to be done in order to ensure the commitment of companies. The project plan should be done with all the parties that are involved. The evaluation of resources needed for a testbed project was noticed to be

extremely important. Lastly, employee commitment is an essential part of the project which requires time but is very rewarding.

Based on the interviewees' experiences, communication with different solutions providers depend a lot on the size of a supplier. Cooperation with huge multinational companies is usually pretty formal and they have clear processes for communications. Communicating with small and local companies can be closer and faster. Customizing services may be easier with smaller companies. However, these smaller companies may not have as strong and well-planned information security and data protection processes, especially if the solutions are still in a very early stage of development. Therefore, communication during the development processes is important as the health care provider can offer support and their expertise for the solution providers. Company D representatives feel like the communication with other companies, especially in the region they operate in, is quite open and honest.

The IoT solution buyers also consider the role of IoT and AI in health care to be significant in the future. However, they emphasize the fact that it should not replace humans and their knowledge. New technologies can be used to support the work of nurses and doctors. They state that IoT has a lot of potential and there are a lot of expectations towards it, but it still has not been utilized as much as it could have been. Especially in homecare, these solutions enable noticing changes in patient's habits in a longer term. It would be ideal if data could be collected before people actually need health care services. Thus, it is easier to customize the services for them when there is valuable data already available. When having a lot of data of a population, AI can enable making prediction models which can help preventing severe diseases. Interviewee F sees that IoT and AI have three main aspects: more efficient processes, customer point of view and financial benefits. Efficient processes mean that, for example, when assessing patient's service needs all possible information is available. Customer point of view means that the health care is available for everyone who needs it within a reasonable time and that the solutions can ease customers' life in many ways. The final one refers to possible cost reductions that can be achieved through IoT solutions.

The employees of a health care service provider may feel that using new technologies may be time consuming. It would be good to remember that these new technologies can replace some older practices and systems which may not respond to their needs anymore. Informing and educating employees is in a key position when deploying new technologies and solutions. Also, interviewee E points out that employees' commitment and motivation

affect the success of the whole process. Usually, older people are less familiar with new technology than younger people. Therefore, younger people might be more accepting towards new technologies. It was emphasized that it would be good if the health care professionals familiarized themselves with these technologies already during their studies in order to ensure nurses' and doctors' ability to utilize technology on a daily basis in their work.

Information security processes need to be precisely planned in a health care provider organization. While adding new companies to the service supply chain, they need to make sure that data regarding their clients' is handled in a proper way. There are numerous data sources that a health care provider can utilize. If there is a patient in home care, it is possible to measure, for instance, their circadian rhythm and changes in them. In addition to making decisions for individual patients, it would be ideal to also make analyses on a populational level. This would require anonymization of data. However, laws do not yet enable this kind of data utilization between industries. Open data is not utilized at the moment but there are interesting possibilities that it could offer. For example, weather forecasts could be used examine how changes in weather affect nurses' driving routes and thus, their schedules. It is common for health care providers to have several systems in which they document information about patients. When choosing solutions that generate new data, it would be ideal that they saved the data to the same place and to the same form. Interviewee F also points out that currently health care providers in private and public sectors have separate systems for storing data which means that all information about patients may not be available when needed. This is an issue that needs to be solved in the future. The ownership of data came up in one of the interviews. The ownership issues have an impact on the procurement process of an IoT solution and they need to be taken into consideration carefully. As the health data is extremely sensitive, there are several regulations that affect the health care provider and several companies may be involved in collecting data which can make managing the supply chain more complicated. Interviewee E commented on the subject:

"It is clear that when we purchase a product and data related to it, the data is ours. We are obligated to archive the data and store it, of course in that point when purchasing a product or a device, we have to think in advance who owns it."

Neither of the interviewees E or F knew exactly what kind of supplier evaluation tools the company has in use, however both agreed that there are some. When buying a solution that can be significant for patient's health care and also an expensive investment, it can be a really challenging situation if the provider, for example, goes bankrupt or is sold to another company. These kinds of unexpected events should be taken into consideration when making contracts with suppliers even though it might be difficult to prepare for them. As a large and significant health care provider in their area, it is not ideal to be dependent on other companies.

Interviewees E and F do not consider that there are significant risks related to testbeds. Proper contracts are done and all of parties should engage in the project. In addition, a specific safety contract is done with every actor that is involved in the project which ensures the handling of personal data should be carried out lawfully, appropriately and transparently. If needed, the companies in testbed project are allowed to use the data in company D's data lake but they will only access to anonymized data. This is done in order to minimize risks related to data security and secure people's privacy. As the usage of IoT solutions in homecare is still little, it is not clear how the services will be organized in the future. There are many questions that still need to be solved, like are health care service providers going to offer devices for their customers as a service or should everyone buy their own devices. In addition, it important to make sure that customers are still able to meet, for instance, doctors in person as well.

Succeeding in a testbed project depends on many things. Company D representatives noticed that a successful testbed project requires information flows both ways. The more honest the discussion between the actors is, the easier the development process is. Having a specific contact person for companies seemed to help and speed up the communications between parties and also having a schedule for the communications has been noticed to be useful. Being regularly in contact through meetings and reports with the other companies has been important and improved the quality of cooperation. Regular, clear and open discussion are in a key position in successful testbed projects which enable building new networks with new companies. Clarifying the goals and requirements to each other have an impact on the engagement of parties. In addition, it is important to inform the health care customers and their families about the executed testbed project in order to make sure that the devices are used correctly.

Obviously, the reliability of the solutions is crucial because there might be lives depending on them. There needs to be a back-up solution or at least a plan what to do in case the

solution stops working. When developing a solution, getting real-time feedback from a testbed environment is important in order to build a secure solution. The testing period needs to be long enough to get enough data. As the solutions are tested with real customers of company D, possibly in their own homes, it is important to pay attention to communication with them when planning the testing process. The customer segments are different so their differing needs should be taken into consideration. The customers must to be told why and how the process will be executed by the professionals who know the solution providers and their customers the best.

6 DISCUSSION AND CONCLUSIONS

Especially during the past few decades IoT has created new possibilities for products and services which has created many new innovations and will continue doing so in the future as well. In just 20 years it has become a megatrend that is expected to change the world drastically. The growing number of aging people creates challenges for health care. IoT solutions can be used to make processes more efficient and to enhance the life quality of people. The expectation towards IoT in health care has grown during the past years but most of the solutions are still in their development stage. It will take a few years before the solutions become more common and change health care.

Producing a high-quality IoT solution usually requires several actors to be involved in the service supply chain. Nowadays it is more common for the actors in a service supply chain to form a supplier network that enhances collaboration and information exchange. Combining the expertise of companies which operate in different fields enables creating a solution that is more innovative. Testbeds offer opportunities for the supplier and buyer to develop these solutions together which is beneficial for both. Supplier gets a chance to truly understand the needs of their potential customer. Buyer on the other hand may have a chance to affect what kind of solutions will come to the market when they are involved in the development process. As usually in business, there are risks associated with IoT solutions as well. Perhaps the biggest risk of IoT are the security related risks. The networks become more vulnerable as more devices are attached to the systems. The data acquired by IoT health care solutions can be very sensitive which is why the actors involved in the service supply chain need to be careful.

The aim of this study was to examine the service supply chain of IoT, especially in the health care sector. The previous studies about IoT concentrated mainly on IoT technologies. This thesis addresses a research gap concerning the IoT supply chain, how it functions, and the risks related to it. In this final chapter of this thesis a short summary about the results will be made and the answers to research questions and possible implications will be presented. In addition, limitations, reliability and validity of this thesis will be evaluated in order to examine the quality of it. Lastly, possible future avenues of the research subject are pondered.

6.1 Summary

The unique characteristics of IoT solutions makes the management of service supply chain challenging. Many companies are examining the possibilities that IoT could offer and some are still learning how to utilize these solutions. Based on this research, the main factors that affect the success of an IoT supply chain are presented in the figure 7. These are factors that the management of companies involved in the supply chain, both buyers and suppliers, should pay attention to in order to deliver high quality services.

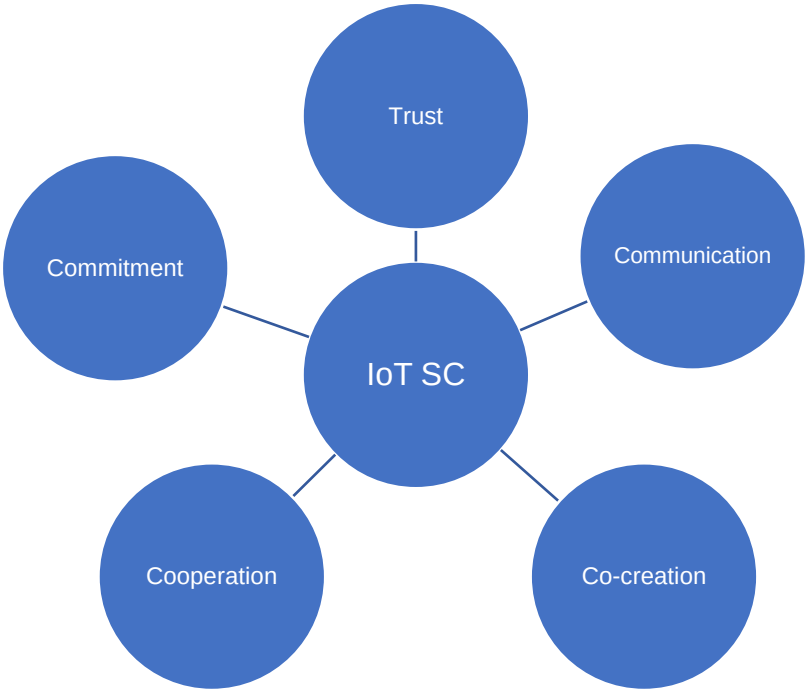

Figure 7. Factors affecting IoT service supply chain

The importance supply network's co-creation of value has been acknowledged in many researches before (Giannakis 2011, 1810). One of the biggest goals of service supply chain is to produce value for the customer, which can be either an organization or a private person, and it is more efficiently done when all of the parties collaborate. As providing IoT solutions, especially providing IoT solutions for social and health care, requires huge amount of knowledge and cooperation between several parties is necessary. When health care providers offer their knowledge for solutions providers, they can also have an impact on the IoT market which can be very valuable. Therefore, cooperation leads to co-creation of value. In addition, co-creation also refers to co-creation of innovations that working together enables. When professionals from different fields and enterprises combine their

know-how, it offers possibilities for creating solutions that are more innovative than solutions which are developed within just one field.

Commitment to the testbed project and afterwards on providing the solution is one of the key factors of a successfully functioning service supply chain. If there are actors that commit to the IoT supply chain less than others, it can lead to unbalanced power relations. Also, corporate acquisitions can create uncertainty in the relationship. All of the parties and their employees should engage in delivering the service for the end-customer. Commitment of service supply chain actors and their management is important, but employees also need to be ready to engage in delivering the service to customers. The engagement process of health care providers employees may be challenging as they may be afraid that the machines take over their jobs. Some may also feel that the new systems are difficult to use and take a lot of time. The managers' job is to educate the employees and ease the integration process. Sharing information and communication between the management and employees is important for the process. The goals should be clearly stated for everybody. Even though IoT might change how people work on a daily basis, the machines cannot replace humans in health care. The solution providers also need to engage in handling the sensitive data in a proper way.

Trust in the figure refers to trust in other actors in the supply chain but also trust in the solutions. Social and health care customers usually have trust in the service provider as they share sensitive and private things with the experts. Therefore, when having more companies in the supply chain, health care providers need to be very careful that their customers' privacy is secured. Communication and information sharing are in the key position when building long-term relationships where the actors rely on each other. Two-way communication is important. The health care service provider also needs to be sure that the solutions function reliably at all times. In addition, the analyses made based on the collected data should be trustworthy and accurate. If the systems do not work properly, it can lead to serious damage. Based on this summary it is fair to conclude that all of these factors have an impact on the IoT supply chain, but also on each other and how successful each factor is.

6.2 Conclusions and answers to the research questions

The main goal of this thesis was to find answers to research questions that were presented in the first chapter. There was a clear gap in research concerning IoT as a service and the supply chain related to it. Therefore, the main research question was:

How the IoT supply chain can be described from the perspective of customer needs?

Nowadays, service supply chain management is focused on the customers and their needs. It is important to create value for clients and therefore, the customer aspect was chosen for this research question. At all of the IoT stages of the whole process, or at least in an ideal situation, things should be happening based on the needs of the customer and in order to serve the customer as well as it is possible. Customers' opinions are highly appreciated, especially as operating in the social and health care sector requires expertise. Čolaković & Hadžialić (2018, 34) state in their study about IoT that there is lack of coordination between standards and technologies. This came up in the interviews as well. The services are usually designed and executed based on the customer's wishes instead of standardized solutions. However, some kind of standardization could be done in order to ease the usage of multiple systems at the same time.

IoT creates value for companies when the devices can communicate with each other and integrate with other systems which can, for example, make analyses (Lee & Lee 2015, 431). Nowadays companies clearly acknowledge the value of data and they are ready to invest in it. The IoT supply chain is based on this value creation process. It has been proven in many studies (e.g. Baltacioglu et al. 2007, 107) that very often companies decide to outsource some of the services in order to focus on their core competencies. This is also common for the companies that were involved in this study because providing an IoT solution requires knowledge from many different fields. It is much more cost-efficient to outsource some of the services. The service supply chain around IoT begins from the device layer that collects the data. The companies can either produce the devices by themselves or purchase them from their suppliers, depending on their expertise. The devices should be easy for health care customers and employees to use. The less the devices need to be maintained, the better it is. For example, changing the batteries would increase employees' workload too much. The following stage is the network layer. Enterprises can utilize either traditional mobile networks or special IoT networks. None of the case companies provide network connections, so they need to buy them from other companies. One of the most

crucial requirements for these network suppliers is mobile coverage. Having a secured network is crucial especially as the data in the health IoT systems can be very sensitive.

The third layer is the platform layer. It is used for analyzing and storing the collected data. There are companies that are focused on providing just IoT platforms or companies can offer the complete IoT solutions. Cloud based solutions have become more and more popular. Some companies have implemented IoT platforms and if they decide to buy new services, these new service providers should be able to connect their systems to existing platforms from another companies. The fourth and fifth layers, services and customer, are intertwined and affect each other a lot. Services are the most visible parts of IoT solutions for the customer: the data can be, for instance, visualized for users. Visualizations are made in order to make it easier for application users to understand data. Different kind of applications can be build based on the collected data depending on customer's needs. Being able to customize the application interface for each customer is definitely a benefit. Alarms can be given to health care professionals, for instance, via emails or text messages. Services should also include support services, like IT support in case the systems stopped working. IoT solutions for health care need to be easy for health care customers to use, they should not add the workload of nurses and doctors and they need to be extremely reliable.

One of the most crucial things for the IoT supply chain is whether the different layers can be smoothly combined and how well the systems communicate with each other. All of the layers are critical for the functioning of an IoT solution. If there are problems in data acquisition, the rest of the solutions cannot function properly. If the network layer has issues, the data will not be transferred to the platform. Possible challenges in the platform can be, for instance, inaccurate analyses which can lead to severe outcomes, especially in health care. In case there are problems in the service layer, like in user applications, solving these problems can take users' valuable time. Finally, issues in the customer layer can occur, e.g., if the customers do not know how to use the application properly. As a conclusion, if there are difficulties in one of IoT supply chain layers, the whole solution may stop working. If there are problems, they should be quickly located and fixed. Producing health care services can be challenging as understanding customer needs can be difficult sometimes and in addition, laws regulate the sector a lot. Information sharing and good relationship between the supplier and buyer is important for understanding the customer. The solution needs to be suitable for the health care providers but also for their customers. It requires

resources to truly understand customer needs and testbeds provide good opportunities to learn to understand them better.

Three sub-questions were developed in order to help answering the main research question. These sub-questions are:

1. *How data sources are identified based on the needs of customers' intended applications?*

One of the best-known challenges regarding IoT is the amount of data sources, the volume of data collected by them and the heterogeneity of them (Čolaković & Hadžialić 2018, 21). In health care, there are numerous measurement possibilities. Identifying data sources and deciding what should be measured depend strongly on the health care providers' needs. The process begins when the health care provider has some kind of problem that needs to be solved. The problem can be related to, for example, enhancing a process or improving the life quality of their customers. Identifying data sources often happens together with an IoT solution provider as they have more precis knowledge about possible measurements and how their solution functions. Therefore, communication and discussions between the buyer and supplier is critical at this point. Understanding customer needs eases identifying data sources. Customer organizations may not always have a lot of knowledge about IoT, especially if they have not used IoT solutions before. However, in this case the customer organization had good understanding about the IoT which helped the solution providers to identify useful data sources.

Karacapilidis et al. (2013, 228) stated that integrating diverse data sources can be a challenge but it should be done in order to generate new knowledge which is one of the most important goals of IoT. The health care organizer in this study has an IoT platform in usage and their supplier should be able to integrate their devices to this platform. As the number of consumer smart devices grows all the time, this could provide new possibilities and data sources for health care providers as well. These smart devices collect different kinds of data, some even 24 hours a day. Data about people's sleep, training or heart rate can be measured all the time. Maybe some health care providers could be able to utilize the information as well. However, this would require making contracts with smart device providers and some way to ensure the quality of data. This would also rase a question about the ownership of data which may create challenges.

2. *How the roles of different actors can be defined in the IoT supply chain within intended applications?*

There are several companies involved in delivering an IoT solution as there are no companies that could odder the whole end-to-end solution by themselves (Rayes & Salam 2019, 259). Thus, the different roles of the actors were examined. Traditionally supply chain actors have been considered as separate parties but nowadays the companies can be seen as a cooperative network that aims at providing their customer the highest possible value (Normann & Ramírez 1993, 66). The roles are interesting to examine as the companies' roles change depending on the point of view. Nearly all of the companies are at some point the supplier and at other point the buyer. In this study the focus was especially on the B2B IoT services, so the health care provider was considered as the customer and the companies that produce these IoT services as the suppliers. Vendors of solution providers were shortly discussed in order to understand the supplier network better, but the main focus was on the firms that deliver a complete IoT solution directly to the health care provider.

The role of the actors in IoT solutions depend heavily on the purpose of the solution. Some of the solutions require more intense cooperation than others. The health care provider is in a key position in IoT supply chain because they work between the IoT solution provider and their clients. Their role is to deliver a service to their customers and based on their customer's needs they have to find suitable solutions. The role is not easy as they have to balance between being cost-efficient and providing the best possible services for their customers. Health care providers need to be able to recognize the best possible solutions that could improve the life quality of, for instance, elderly that still live at home. The role of IoT solution providers is to help health care providers in this. When developing the solution, the health care provider can offer their expertise in health care and supplier can offer their expertise in technology. The suppliers need to be able to produce a reliable solution as the devices may measure, for example, vital functions. There should be a back-up solution in each layer that ensures the functioning of the IoT solution at all times and the system should alarm if there are problems.

3. *How risk management approaches differ between actors which represent different parts of IoT supply chain or utilize varying data sources?*

The companies that are involved in the IoT supply chain may face different kinds of risks depending on their position in the chain. However, one of the main concerns that arose among all of the interviewees, regardless of their position in the IoT supply chain, was the safety of data and the customers' privacy. This is not a surprise considering that the safety of IoT has been studied quite a lot during the past few years. The trustworthiness of devices and other systems connected to them is crucial as people's lives can depend on them. This is an aspect that will gain attention in the upcoming years as the solution will become more common. Sivarajah et al. (2017, 274) also discuss about data privacy and security and how they are crucial data management challenges. IoT solution providers can try to mitigate the risks related to information security, one possible way to do this is to handle and analyze the data in the same place where it is collected. Therefore, sensitive data would not need to be transferred over the network, which can be vulnerable, to another location. Health care provider on the other hand can try to mitigate risks by controlling carefully who can access their customers' personal data. Also, having some kinds of certification requirements for their vendors can help buyer to mitigate risks.

According to Sivarajah et al. (2017, 274) data ownerships issues of IoT are often discussed in social media context. Interestingly, similar questions arose during the interviews as well. The situation can become complicated when the device is placed in the customer's home, solution provider delivers a device and other possible systems, and health care provider buys the service. One possible risk that health care providers may face, that differs from the risks that solution providers face, is their employees' reluctance to use new technology. Earlier, Brous et al. (2020, 5) have stated that the more the users trust the system, the more willing they are to take part in the projects. Open communication between the management and employees, making sure that everybody is informed about the possible changes and offering proper training on using new systems are ways to increase trust in new technology. The solutions are deployed in order to help employees' work, not to replace them. As the testbed organizer, the health care provider representatives did not actually see that there are major risks related to testbeds. When developing solutions, they pursue to offer the IoT solution providers anonymized and pseudonymized data whenever it is possible in order to maximize their patients' privacy. Sometimes smaller companies with a new solution still need help with information security issues and testbeds provide good opportunities to develop security protocols.

Whereas health care providers need to take into consideration how their stakeholders react to deploying new technology, IoT solution providers mainly encounter risks that complicate delivering their services. Some of the devices can collect data around the clock. Thus, the data volumes can be very large. Karacapilidis et al. (2013, 227) have already stated earlier that data can be different in terms of subjectivity and this issue was acknowledged by the case companies as well. Finding accurate knowledge from the large data sets and having enough storage capacity can be challenges. Making incorrect analyses and predictions based on them can lead to severe problems. The IoT solution providers had some differing opinions about the risks related to testbed projects and overall IoT solutions. Interestingly, some thought that there are bigger risks in solutions that are still in their developing stages and some thought there are no differences between solutions that are in the market and that are still being developed. The biggest risk when developing solutions is that there is a small problem that remains unnoticed. This small problem may become bigger over time and harder to fix.

6.3 Implications

This thesis provides information about IoT supply chain for both, buyers and suppliers of IoT solutions. Studies about IoT usually focus on technological aspect of it. The goal of this study was to provide information about the subject from a business point of view. Nearly all of the articles, books and other materials used in this thesis are published within 20 years. Therefore, the information used in this research is fairly new and up to date which eases the utilization of it. The results of the study support the previous researches made about subjects and succeeded in bringing new insights especially about IoT supply chain in health care.

Especially managers in health care providing organizations need to be careful when choosing supplier as they have a broad customer base and their services affect people's lives. The study provides additional information particularly about IoT solutions in health care and what to take into consideration when selecting new IoT services. Having better understanding about the processes makes it easier to manage them. This knowledge is valuable because health care providers are going to need IoT in the future when the number of aging people increases faster than ever. IoT can help to cut down costs and improve the service quality. IoT solution providers can also utilize the research as the results can help to understand their potential customers and their needs. In health care sector this is very important because offering social and health care services require a lot of know-how. In

addition, risk management approaches were studied, from supplier and buyer point of view. It is very important for all of actors regardless of their position in the supply chain to ensure that information security issues are taken into consideration.

6.4 Reliability and limitations

There are some limitations concerning this research that need to be taken into consideration. First of all, as the health care provider only operates in one part of Finland, there could be different results in other social and health care districts or in different countries. It is also good to remember that all of the case companies are Finnish, and the situation could be different if, for example, a supplier is from another country. GDPR regulates the companies in European Union, but there might be other regulations and laws in different areas. Secondly, examining companies that have cooperated for a longer time could have provided different kinds of results. However, as IoT is still quite new and companies are examining the possibilities IoT could offer, there are not many health care providers that have a longer history utilizing IoT solutions. IoT solutions have special requirements in this field of business and therefore, generalizations to other branches can be difficult.

In general, reliability of this research is quite good. Suitable research method was chosen for this study and the research process was described thoroughly which enables repeating the research. Construct validity and external validity can be considered to be fairly good as well. Several data sources were used. The case companies and additional material that was used were described providing the reader as much information as it was possible while ensuring the anonymity of the case companies. Examining buyers and supplier provides good understanding from different aspects. However, there some factors that may reduce the reliability and validity of the research. The sampling is small and is focused on a specific field of business and on one supplier network. Therefore, generalizing these results truly is difficult. As using IoT in health care is still a new phenomenon, it can be expected to change already in the near future which can also have an impact on the results of the study. Thus, even if the research was done again, the results could be different. It is difficult to say how exactly IoT is going to affect health care but it is clear that it will.

6.5 Suggestions for further research

As IoT and the service supply chain around it have not been studied much earlier, there are many interesting research possibilities. The experiences and thoughts of nurses and doctors regarding the growing usage of IoT solutions in health care could be studied. Also, examining how customers of the health care provider feel about their daily lives being measured could offer interesting insights to the subject. As the goal of deploying an IoT solutions usually is to make processes more efficient, studying the economic impact could be interesting, too. The resources were limited, so only a small part of a supplier network was examined. Thus, it could be interesting to observe the bigger part of the supplier network by studying also, for example, how the IoT devices are built and how many companies are involved in that process.

REFERENCES

Abaidi, I. & Vernette, E. (2018) Does digitalization create or reduce perceived global value? Journal of Consumer Marketing, Vol. 35(7), pp. 676-687.

Aloi, G., Caliciuri, G., Fortino, G., Gravina, R., Pace, P., Russo, W. & Savaglio, C. (2017) Enabling IoT interoperability through opportunistic smartphone-based mobile gateways. Journal of Network and Computer Applications, Vol. 81, pp. 74-84.

Aheleroff, S., Xu, X., Lu, Y., Aristizabal, M., Pablo Velásquez, J., Joa, B., & Valencia, Y. (2020) IoT-enabled smart appliances under industry 4.0: A case study. Advanced Engineering Informatics, Vol. 43, pp. 1-14.

Ahmed, M., Choudhury, S. & Al-Turjman, F. (2019) Big Data Analytics for Intelligent Internet of Things (pp. 107-128). In Artificial Intelligence in IoT. Cham: Springer International Publishing.

Ahmed, E., Yaqoob, I., Hashem, I., Khan, I., Ahmed, A., Imran, M. & Vasilakos, A. (2017) The role of big data analytics in Internet of Things. Computer Networks, Vol. 129, pp. 459-471.

Ambore, B. & Suresh, L. (2018) Assessing trends of existing research contribution towards Internet-of-Things. International Journal of Advanced Computer Science and Applications, Vol. 9(9), pp. 172-184.

Ammar, M., Russello, G., & Crispo, B. (2018) Internet of Things: A survey on the security of IoT frameworks. Journal of Information Security and Application, Vol. 38, pp. 8-27.

Anderson, E. (2014) Business risk management: models and analysis. John Wiley & Sons.

Assunta Barchiesi, M. & Fronzetti Colladon, A. (2019) Big data and big values: When companies need to rethink themselves. Journal of Business Research. pp. 1-9.

Atlam, H. & Wills, G. (2019) Technical aspects of blockchain and IoT. Role Of Blockchain Technology In Iot Applications, Vol. 115, pp. 1-39.

Atzori, L., Iera, A. & Morabito, G. (2010) The Internet of Things: A survey. Computer Networks, Vol. 54(15), pp. 2787-2805.

Baltacioglu, T., Kaplan, M., Yurt, O. & Cem Kaplan, Y. (2007) A New Framework for Service Supply Chains. The Service Industries Journal, Vol. 27(2), pp. 105-124.

Biehl, M., Cook, W., & Johnston, D. (2006) The efficiency of joint decision making in buyer-supplier relationships. Annals of Operations Research, Vol. 145(1), pp. 15–34.

Boehmer, J. H., Shukla, M., Kapletia, D., & Tiwari, M. K. (2020) The impact of the Internet of Things (IoT) on servitization: an exploration of changing supply relationships. Production Planning & Control, Vol. 31(2-3), pp. 203-219.

Boon-itt, S., Wong, C., & Wong, C. (2017) Service supply chain management process capabilities: Measurement development. International Journal of Production Economics, Vol. 193, pp. 1-11.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016) Integration of cloud computing and internet of things: a survey. Future generation computer systems, Vol. 56, pp. 684-700.

Braziotis, C., Bourlakis, M., Rogers, H., & Tannock, J. (2013) Supply chains and supply networks: distinctions and overlaps. Supply Chain Management, Vol. 18(6), pp. 644–652.

Broring, A., Schmid, S., Schindhelm, C., Khelil, A., Kabisch, S., Kramer, D., Le Phuoc, D., Mitic, J., Anicic, D., & Teniente, E. (2017) Enabling IoT Ecosystems through Platform Interoperability. IEEE Software, Vol. 34(1), pp. 54–61.

Brous, P., Janssen, M. & Herder, P. (2020) The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations. International Journal of Information Management, Vol. 51, pp. 1-17.

Cai, H., Xu, B., Jiang, L. & Vasilakos, A. V. (2017) IoT-Based Big Data Storage Systems in Cloud Computing: Perspectives and Challenges. IEEE Internet of Things Journal, Vol. 4(1), pp. 75-87.

Calbimonte, J-P., Sarni, S., Ebere, J. & Aberer, K. (2014) XGSN: An Open-source Semantic Sensing Middleware for the Web of Things. 7th international workshop on semantic sensor networks. Riva del Garda, Trentino, Italy.

Chandler, J., & Lusch, R. (2015) Service Systems: A Broadened Framework and Research Agenda on Value Propositions, Engagement, and Service Experience. Journal of Service Research, Vol. 18(1), pp. 6–22.

Chen, J., Chen, Y., Du, X., Li, C., Lu, J., Zhao, S. & Zhou, X. (2013) Big data challenge: a data management perspective. Frontiers of Computer Science, Vol.7(2), pp. 157-164.

Chen, H., Chiang, R. H., & Storey, V. C. (2012) Business intelligence and analytics: From big data to big impact. MIS quarterly, Vol.36 (4), pp. 1165-1188.

Chen, M., Mao, S. & Liu, Y. (2014) Big Data: A Survey. Mobile Networks and Applications, Vol. 19(2), pp. 171-209.

Chernyshev, M., Baig, Z., Bello, O. & Zeadally, S. (2018) Internet of Things (IoT): Research, Simulators, and Testbeds. IEEE Internet of Things Journal, Vol. 5(3), pp. 1637-1647.

Chiţiba, C. (2018) INDUSTRY 4.0. Knowledge Horizons. Economics, Vol. 10(2), pp. 72-75.

Cho, M.E. & Kim, M.J. (2014) Characterizing the interaction design in healthy smart home devices for the elderly. Indoor and Built Environment, Vol. 23(1), pp. 141-149.

Choudhury, T., Paul, S., Rahman, H., Jia, Z. & Shukla, N. (2020) A systematic literature review on the service supply chain: Research agenda and future research directions. Production Planning and Control, pp. 1-22.

Čolaković, A. & Hadžialić, M. (2018) Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues. Computer Networks, Vol. 144, pp. 17-39.

Cui, L., Yang, S., Chen, F., Ming, Z., Lu, N. & Qin, J. (2018) A survey on application of machine learning for Internet of Things. International Journal of Machine Learning and Cybernetics, Vol. 9(8), pp. 1399-1417.

Demchenko, Y., Grosso, P., de Laat, C. & Membrey, P. (2013) Addressing big data issues in Scientific Data Infrastructure. Collaboration Technologies and Systems (CTS), 2013 International Conference on 48–55.

Demirkan, H., Cheng, H. & Bandyopadhyay, S. (2010) Coordination Strategies in an SaaS Supply Chain. Journal of Management Information Systems, Vol. 26(4), pp. 119-143.

Dey, N., Ashour, A. S., & Bhatt, C. (2017) Internet of things driven connected healthcare. In Internet of things and big data technologies for next generation healthcare (pp. 3-12). Springer, Cham.

Díaz, M., Martín, C. & Rubio, B. (2016) State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer Applications, Vol. 67, pp. 99-117.

Dlodlo, N., Foko, T., Mvelase, P. & Mathaba, S. (2012) The State of Affairs in Internet of Things Research. Electronic Journal of Information Systems Evaluation, Vol. 15(3), pp. 244-258.

Duan, Y., Fu, G., Zhou, N., Sun, X., Narendra, N. C., & Hu, B. (2015) Everything as a service (XaaS) on the cloud: origins, current and future trends. In 2015 IEEE 8th International Conference on Cloud Computing, pp. 621-628.

Dubois, A., & Gadde, L. (2002) Systematic combining: an abductive approach to case research. Journal of Business Research, Vol. 55(7), pp. 553–560.

Ellram, L., Tate, W. & Billington, C. (2004) Understanding and Managing the Services Supply Chain. Journal of Supply Chain Management, Vol. 40(3), pp. 17-32.

Ellram, L., Tate, W. & Billington, C. (2007) Services Supply Management: The Next Frontier for Improved Organizational Performance. California Management Review, Vol. 49(4), pp. 44-66.

European Strategy and Policy Analysis System (2020) Welcome to 2030: The Mega-trends. [Web page] [Accessed 25.6.2020] Available: https://ec.europa.eu/assets/epsc/pages/espas/chapter1.html

Femminella, M., Pergolesi, M. & Reali, G. (2018) IoT, big data, and cloud computing value chain: Pricing issues and solutions. Annals of Telecommunications, Vol. 73(7), pp. 511-520.

Finnish institute for health and welfare (2019) Prioritizing home care. [Web page] [Accessed 18.6.2020] Available: https://thl.fi/en/web/ageing/prioritising-home-care

Gandomi, A. & Haider, M. (2015) Beyond the hype: Big data concepts, methods, and analytics. International Journal of Information Management, Vol. 35(2), pp. 137-144.

Ganzha, M., Paprzycki, M., Pawlowski, W., Pawel S. & Wasielwska, K. (2018) Towards Semantic Interoperability Between Internet of Things Platforms (pp. 103-127). In Integration, Interconnection, and Interoperability of IoT Systems. Springer International Publishing.

Gartner (2020) Hype Cycle for Supply Chain Strategy, 2020. [Web page] [Accessed 28.10.2020] Available: https://www.gartner.com/en/newsroom/press-releases/2020-09-09-gartner-2020-hype-cycle-for-supply-chain-strategy-shows-internet-of-things-is-two-to-five-years-away-from-transformational-impact

Ge, M., Bangui, H. & Buhnova, B. (2018) Big Data for Internet of Things: A Survey. Future Generation Computer Systems, Vol. 87, pp. 601-614.

Ghasemaghaei, M., Ebrahimi, S. & Hassanein, K. (2018) Data analytics competency for improving firm decision making performance. Journal of Strategic Information Systems, Vol. 27(1), pp. 101-113.

Ghosh, A., Chakraborty, D., & Law, A. (2018) Artificial intelligence in Internet of things. CAAI Transactions on Intelligence Technology, Vol. 3(4), pp. 208-218.

Giannakis, M. (2011) Conceptualizing and managing service supply chains. The Service Industries Journal, Vol. 31(11), pp. 1809-1823.

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

Halinen, A & Törnroos, J. (2005) Using case methods in the study of contemporary business networks. Journal of Business Research, Vol. 58(9), pp. 1285-1297.

Hox, J. J., & Boeije, H. R. (2005) Data collection, primary versus secondary. Encyclopedia of Social Measurement, Vol. 1, pp. 593-599.

International Data Corporation (2019) The Growth in Connected IoT Devices Is Expected to Generate 79.4ZB of Data in 2025, According to a New IDC Forecast. [web page] [Accessed 12.8.2020] Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213219

Jhang-Li, J. & Chang, C. (2017) Analyzing the operation of cloud supply chain: Adoption barriers and business model. Electronic Commerce Research, Vol. 17(4), pp. 627-660.

Jiehan, Z., Leppänen, T., Harjula, E., Ylianttila, M., Ojala, T., Chen, Y., Hai, J & Yang, L. (2013) CloudThings: A common architecture for integrating the Internet of Things with Cloud Computing, In Proceedings of the 2013 IEEE 17th International Conference on Computer Supported Cooperative Work in Design, pp. 651–657.

Ju, J., Kim, M. & Ahn, J. (2016) Prototyping Business Models for IoT Service. Procedia Computer Science, 91, pp. 882-890.

Kaplan, A. & Haenlein, M. (2019) Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. Business Horizons, Vol. 62(1), pp. 15-25.

Karacapilidis, N., Tzagarakis, M., & Christodoulou, S. (2013) On a meaningful exploitation of machine and human reasoning to tackle data-intensive decision making. Intelligent Decision Technologies, Vol. *7*(3), pp. 225-236.

Karolewicz, K., Beben, A., Batalla, J., Mastorakis, G., & Mavromoustakis, C. (2017) On efficient data storage service for IoT. International Journal of Network Management, Vol. 27(3), pp. 1-14.

Kemppainen, K., & Vepsäläinen, A. (2003) Trends in industrial supply chains and networks. International Journal of Physical Distribution & Logistics Management, Vol. 33(8), 701–719.

Koskinen, I., Peltonen, T., & Alasuutari, P. (2005) Laadulliset menetelmät kauppatieteissä. Vastapaino.

Kovács, G., & Spens, K. (2005) Abductive reasoning in logistics research. International Journal of Physical Distribution & Logistics Management, Vol. 35(2), pp. 132-144.

Lasi, H., Fettke, P., Kemper, H., Feld, T. & Hoffmann, M. (2014) Industry 4.0. Business & Information Systems Engineering, Vol. 6(4), pp. 239-242.

Lee, I. (2019) The Internet of Things for enterprises: An ecosystem, architecture, and IoT service business model. Internet of Things, Vol. 7, pp. 1-13.

Lee, S., Bae, M. & Kim, H. (2017) Future of IoT Networks: A Survey. Applied Sciences-Basel, Vol. 7(10), pp 1-25.

Lee, D. & Lee, H. (2018) IoT service classification and clustering for integration of IoT service platforms. The Journal of Supercomputing, Vol. 74(12), pp. 6859-6875.

Lee, I. & Lee, K. (2015) The Internet of Things (IoT): Applications, investments, and challenges for enterprises. Business Horizons, Vol. 58(4), pp. 431-440.

Legner, C., Eymann, T., Hess, T., Matt, C., Böhmann, T., Drews, P., Mädche, A., Urbach, N. & Ahlemann, F. (2017) Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. Business & Information Systems Enginerring, Vol. 59(4), pp. 301-308.

Li, C., & Li, L. (2013) Efficient resource allocation for optimizing objectives of cloud users, IaaS provider and SaaS provider in cloud environment. The Journal of Supercomputing, Vol. 65(2), pp. 866–885.

Li, S., Xu, L. & Zhao, S. (2015) The internet of things: A survey. Information Systems Frontiers, Vol. 17(2), pp. 243-259.

Lin, A. & Chen, N. (2012) Cloud computing as an innovation: Percepetion, attitude, and adoption. International Journal of Information Management, Vol. 32(6), pp. 533-540.

Lycett, M. (2013) ‘Datafication’: Making sense of (big) data in a complex world. European Journal of Information Systems, Vol. 22(4), pp. 381-386.

Madhavaiah, C., Bashir, I. & Shafi, S. I. (2012) Defining Cloud Computing in Business Perspective: A Review of Research. Vision: The Journal of Business Perspective, Vol. 16(3), pp. 163-173.

Mahdavinejad, M., Rezvan, M., Barekatain, M., Adibi, P., Barnaghi, P. & Sheth, A. (2018) Machine learning for internet of things data analysis: A survey. Digital Communications And Networks, Vol. 4(3), pp. 161-175.

Maresova, P. & Klimova, B. (2015) Investment evaluation of cloud computing in the European business sector. Applied Economics, Vol. 47(36), pp. 3907-3920.

Marjani, M., Nasaruddin, F., Gani, A., Karim, A., Hashem, I. A. T., Siddiqa, A. & Yaqoob, I. (2017) Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges. IEEE Access, Vol. 5, pp. 5247-5261.

Marston, S., Li, Z., Bandyopadhyay, S., Zhang, J. & Ghalsasi, A. (2011) Cloud computing — The business perspective. Decision Support Systems, Vol. 51(1), pp. 176-189.

Matthyssens, P. & Vandenbempt, K. (2008) Moving from basic offerings to value-added solutions: Strategies, barriers and alignment. Industrial Marketing Management, Vol. 37(3), pp. 316–328.

Miller, K. (1992) A Framework for Integrated Risk Management in International Business. Journal of International Business Studies, Vol.23(2), pp. 311-331.

Mineraud, J., Mazhelis, O., Su, X., & Tarkoma, S. (2016) A gap analysis of Internet-of-Things platforms. Computer Communication, Vol. 89-90, pp. 5-16.

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

Normann, R., & Ramírez, R. (1993) From value chain to value constellation: designing interactive strategy. Harvard Business Review, Vol. 71(4), pp. 65-77.

Omitola, T. & Wills, G. (2018) Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain. Procedia Computer Science, Vol. 126, pp. 441-450.

Otto, B. (2011) Organizing data governance: Findings from the telecommunications industry and consequences for large service providers. Communications of the Association for Information Systems, Vol. *29*(1), pp. 46-65.

Padilla, R., Milton, S. & Johnson, L. (2015) Components of service value in business-to-business Cloud Computing. Journal of Cloud Computing, Vol. 4(1), pp. 1-20.

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, Vol. 9(1), pp. 86-116.

Patel, K. & Patel, S. (2016) Internet of Things-IoT: Definitions, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. International Journal of Engineering Science and Computing, Vol. 6(5), pp. 6122-6131.

Peek, N., Holmes, J. H. & Sun, J. (2014) Technical challenges for big data in biomedicine and health: Data sources, infrastructure, and analytics. Yearbook of medical informatics, Vol. 9(01), pp- 44-47.

Phan, T. A. M., Nurminen, J. K., & Di Francesco, M. (2014) Cloud databases for internet-of-things data. In 2014 IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom), pp. 117-124.

Plaza, I., Martín, L., Martin, S. & Medrano, C. (2011) Mobile applications in an aging society: Status and trends. The Journal of Systems & Software, Vol. 84(11), pp. 1977-1988.

Poniszewska-Maranda, A., & Kaczmarek, D. (2015) Selected methods of artificial intelligence for Internet of Things conception. In 2015 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1343-1348.

Radanliev, P., De Roure, D., Nicolescu, R., Huth, M., Montalvo, R., Cannady, S., & Burnap, P. (2018) Future developments in cyber risk assessment for the internet of things. Computers in Industry, Vol. 102, pp. 14-22.

Ray, P. (2018) A survey on Internet of Things architectures. Journal of King Saud University - Computer and Information Sciences, Vol. 30(3), pp. 291-319.

Rayes, A. & Salam, S. (2019) Internet of Things From Hype to Reality: The Road to Digitization (2nd ed. 2019.). Cham: Springer International Publishing.

Roblek, V., Meško, M. & Krapež, A. (2016) A Complex View of Industry 4.0. SAGE Open, Vol. 6(2), pp. 1-11.

Rojko, A. (2017) Industry 4.0 concept: Background and overview. International Journal of Interactive Mobile Technologies, Vol. 11(5), pp. 77-90.

Sakhuja, S.,Jain, V., Kumar, S. & Chandra, C. (2016) A Structured Review of Service Supply Chain Discipline: Potentials, Challenges, and Integrated Framework. Journal of the Academy of Business Education, Vol. 17, pp. 270-295.

Saldaña, J. (2011) Fundamentals of qualitative research. Oxford University Press.

Sánchez López, T., Ranasinghe, D., Harrison, M. & McFarlane, D. (2012) Adding sense to the Internet of Things. Personal and Ubiquitous Computing, Vol. 16(3), pp. 291-308.

Selviaridis, K., & Norrman, A. (2014) Performance-based contracting in service supply chains: a service provider risk perspective. Supply Chain Management, Vol. 19(2), pp. 153–172.

Serpanos, D. k. & Wolf, M. k. (2018) Internet-of-Things (IoT) Systems: Architectures, Algorithms, Methodologies. Cham: Springer International Publishing.

Sinha, S., & Park, Y. (2017) Building an Effective IoT Ecosystem for Your Business. Springer International Publishing.

Sintonen, s, & Immonen, M. (2013) Telecare services for aging people: Assessment of critical factors influencing the adoption intention. Computers in Human Behavior, Vol. 29(4), pp. 1307-1317.

Sivarajah, U., Kamal, M., Irani, Z., & Weerakkody, V. (2017) Critical analysis of Big Data challenges and analytical methods. Journal of Business Research, Vol. 70, pp. 263-286.

Ślusarczyk, B. (2018) Industry 4.0 – Are we ready? Polish Journal of Management Studies, Vol. 17(1), pp. 232-248.

Solberg Søilen, K. (2016) Users' perceptions of Data as a Service (DaaS). Journal of Intelligence Studies in Business, Vol. 6(2), pp. 43-51.

Spekman, R., Kamauff, J. & Myhr, N. (1998) An empirical investigation into supply chain management: a perspective on partnerships. International Journal of Physical Distribution & Logistics Management, Vol. 28 (8), pp. 630-650.

Srivastava, R., Shervani, T., & Fahey, L. (1999) Marketing, Business Processes, and Shareholder Value: An Organizationally Embedded View of Marketing Activities and the Discipline of Marketing. Journal of Marketing, Vol. 63, pp. 168-179.

Stankovic, J. A. (2014) Research Directions for the Internet of Things. IEEE Internet of Things Journal, Vol, 1(1), pp. 3-9.

Statista (2020a) Internet of Things (IoT) market revenue forecast in Europe in 2019 and 2022. [Web page] [Accessed 2.7.2020] Available: https://www.statista.com/statistics/1115774/iot-market-revenue-forecast-in-europe/

Statista (2020b) Number of internet of things (IoT) connected devices worldwide in 2018, 2025 and 2030. [Web page] [Accessed 24.6.2020] Available: https://www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

Statista (2020c) Internet of things (IoT) market size in the Nordic and Baltic countries forecast from 2017 to 2022, by category [Web page] [Accessed 19.11.2020] Available: https://www.statista.com/statistics/1121849/iot-market-size-in-the-nordics-and-baltics-by-category/

Strange, R. & Zucchella, A. (2017) Industry 4.0, global value chains and international business. Multinational Business Review, Vol. 25(3), pp. 174-184.

Stuart, I., McCutcheon, D., Handfield, R., McLachlin, R. & Samson, D. (2002) Effective case research in operations management: a process perspective. Journal of Operations Management, Vol. 20(5), pp. 419-433.

Suominen, A. (2003) Riskienhallinta (3. uud. p.). WSOY.

Tuomi, J. & Sarajärvi, A. (2018) Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos.). Kustannusosakeyhtiö Tammi.

Ullah, M., Nardelli, P., Wolff, A., & Smolander, K. (2020) Twenty-one key factors to choose an IoT platform: Theoretical framework and its applications. IEEE Internet of Things Journal, pp. 1-9.

van Kranenburg, R. & Bassi, A. (2012) IoT Challenges. Communications in Mobile Computing, Vol. 1(1), pp. 1-5.

Vilko, J., & Ritala, P. (2014) Service supply chain risk management. Operations and Supply Chain Management, Vol. 7(3), pp. 114-120.

Wang, P., Chaudhry, S., & Li, L. (2016) Introduction: advances in IoT research and applications. Internet Research, Vol. 26(2), pp. 239-241.

Wang, P., Valerdi, R., Zhou, S. & Li, L. (2015) Introduction: Advances in IoT research and applications. Information Systems Frontiers, Vol. 17(2), pp. 239-241.

Weking, J., Stöcker, M., Kowalkiewicz, M., Böhm, M. & Krcmar, H. (2020) Leveraging industry 4.0 – A business model pattern framework. International Journal of Production Economics, Vol. 225, pp. 1-17.

Westerlund, M., Leminen, S., & Rajahonka, M. (2014) Designing Business Models for the Internet of Things. Technology Innovation Management Review, Vol. 4(7), pp. 5-14.

WHO (2018) Ageing and health. [Web page] [Accessed 18.6.2020] Available: https://www.who.int/news-room/fact-sheets/detail/ageing-and-health

Whitmore, A., Agarwal, A. & Xu, L. (2015) The Internet of Things—A survey of topics and trends. Information Systems Frontiers, Vol. 17(2), pp. 261-274.

Wortmann, F. & Flüchter, K. (2015) Internet of Things. Business & Information Systems Engineering, Vol. 57(3), pp. 221-224.

Xu, L., Xu, E. & Li, L. (2018) Industry 4.0: State of the art and future trends. International Journal Of Production Research, Vol. 56(8), pp. 2941-2962.

Yan, J., Guo, Y. & Schatzberg, L. (2012) Coordination mechanism of IT service supply chain: An economic perspective. Electronic Markets, Vol. 22(2), pp. 95-103.

Yin, R. (2015) Case study research: design and methods (5th edition.). SAGE.

Ylijoki, O. & Porras, J. (2016) Perspectives to Definition of Big Data: A Mapping Study and Discussion. Journal of Innovation Management, Vol. 4(1), pp. 69-91.

APPENDICES

Appendix 1: Question template 1

General questions:

1. What is your position in the organization?
2. What are your main responsibilities?
3. Tell shortly about your company.

Theme 1:

1. To which stage/stages would you place yourself in the framework? What kind of knowledge is in the key position in your business?
2. How many companies are involved in providing your IoT solution? What kind of knowledge is bought?
3. What kind of demands do you have for your supplier network?
4. At what point do you start to communicate with your suppliers? How do you communicate with them? In your opinion, do you communicate enough?
5. What have been the biggest challenges when delivering your IoT solution to customers?

Theme 2:

1. What kind of meaning does testbeds have for developing your solution?
2. What kind of solutions are suitable for testbed projects? At what point do you contact a testbed organizer?
3. What kind challenges are there in testbeds?
4. Do you think that the knowledge gained in testbeds can be utilized in public tenders?

Theme 3:

1. What is the role of IoT and AI in your organization now and in the future?
2. Does IoT or AI add the need of education of employees? How about understanding the needs of a customer?

3. Are there ways to connect the needs of a customer, collected data and testbed solutions?
4. What kind of data sources do you offer? What kind of valuable information does your customer get from this service?
5. What kind of requirements do your customers have regarding the data sources?
6. How do you feel about third parties, like the university, utilizing the data gathered in testbeds?

Theme 4: Risk management

1. How do you evaluate the risks in testbeds? To what kind of risks have ran into? Do these risks differ from risks related to solutions that are already in the market?
2. What do you think is the biggest risk regarding IoT services?
3. What kind of risks are related to customers and how do you mitigate these risks?
4. What kind of information security risks are there in testbed? What kind of processes do you have to prevent these risks?
5. Are there data compatibility problems? If yes, what kind of problems are there? How can these kinds of problems be solved?

Appendix 2: Question template 2

General questions:

1. What is your position in the organization?
2. What are your main responsibilities?
3. Are there any possible stages you would add to the framework?

Theme 1:

1. What are the most important selection criteria for testing solutions?
2. At what point do you start to communicate with your suppliers? How do you communicate with them? In your opinion, do you communicate enough?
3. What kind of challenges are there when choosing IoT testbed solution providers?
4. Do you use some kind of supplier evaluation tools?
5. Do testbed projects affect market dialogue in public procurement?

Theme 2:

1. What is the role of IoT and AI in your organization now and in the future?
2. How much do you believe to benefit from IoT and AI in the future?
3. What kind of know-how is needed when utilizing different kinds of data storages?
4. Does deploying IoT solutions add the need for education? How do you believe your employees will react to increasing use of technology?
5. Do your suppliers have demands regarding openness of data?
6. Are there ways to connect the needs of a customer, collected data and testbed solutions?
7. What kind of data sources do you utilize?

Theme 3: Risk management

1. How do you evaluate the risks regarding testbed suppliers? To what kind of risks have ran into?
2. What kind of supplier evaluation tools do you use?
3. What do you think is the biggest risk regarding IoT services?

4. What kind of information security risks are there in testbeds? What kind of processes do you have to prevent these risks?
5. Are there data compatibility problems? If yes, what kind of problems are there? How can these kinds of problems be solved?