

Kirill Lazarev

Internet of Things for personal healthcare


Study of eHealth sector. Smart wearable de-
sign.

Bachelor's Thesis
Information Technologies

December 2016



DESCRIPTION

		Date of the bachelor's thesis 2-December-2016
Author(s) Kirill Lazarev	Degree programme and option Information Technology	
Name of the bachelor's thesis Internet of Things for personal healthcare. Study of eHealth sector. Smart wearable design.		
Abstract Technologies are not still and Internet of Things concept introduces a lot of new possibilities for innovation, new products and user applications. All devices become truly personal and medical sector is not an exclusion. Telemedicine is a new approach to diagnostic and treatment, while smart healthcare solutions provide the user an ultimate health control. The purpose of my study is to understand what eHealth sector is and to provide clear guidelines for business and IT specialists on how to enter the smart healthcare market. I analyzed the current market situation, made an audience research in Finland and prepared a whitepaper with basic rules, which can help to develop and design a valuable, secure product for personal use, which gives maximum profit for the company and ultimate usage convenience and experience for selected consumers. Following topics are covered in the paper: needs and requirements of healthcare IoT, regulations, adoption, IoT user experience, security and so on. I hope my work will help specialist from different fields to understand personal healthcare Internet of Things and to open new operating areas. Finally, I applied all collected theoretical knowledge and designed a smart insulin pump, what is an innovative and new product on today's market.		
Subject headings, (keywords) Internet of Things, healthcare, eHealth, wearables, telemedicine, diabetes		
Pages 91	Language English	URN
Remarks, notes on appendices All appendices are very important for understanding the whole paper. Do not avoid opening them when there is a reference in the text.		
Tutor Matti Juutilainen	Bachelor's thesis assigned by Mikkeli University of Applied Sciences, Digital Archiving and eServices project	

CONTENTS

1.	INTRODUCTION.....	2
2.	IOT OVERVIEW AND THEORETICAL BACKGROUND	6
2.1.	IoT history at a glance	6
2.2.	Definitions and concept	9
2.3.	General architecture and characteristics of IoT	12
2.4.	General IoT peculiarities and challenges.....	14
2.4.1.	Automation vs. smartness.....	14
2.4.2.	Problem of standards	19
2.4.3.	Traditional vs. digital economics	21
2.4.4.	Security.....	24
2.5.	Telemedicine, healthcare and medical IoT	26
2.5.1.	Architecture of healthcare IoT.....	27
3.	PERSONAL HEALTHCARE IOT STUDY	29
3.1.	Motivation for healthcare IoT and study	29
3.2.	Wearables and the user study	31
3.3.	Exploring new audience	35
3.3.1.	Principles for delivering personal telemedicine	40
3.4.	Analysis of positive contribution and risks	44
3.4.1.	Smart healthcare security concerns	45
3.4.2.	Risk sources, recommendations for regulations and security	48
4.	STUDY OUTCOMES AND RESULTS	56
5.	DESIGNING A SMART HEALTHCARE DEVICE.....	57
5.1.	Introduction and motivation	57
5.2.	Diabetes	59
5.3.	Bracelet design and technologies.....	61
5.3.1.	Model and features	61
5.3.2.	Mechanisms.....	63
5.3.3.	Control and communication	64
5.4.	Application design	66
5.5.	Business aspects.....	66
5.6.	Conclusions and future work	67
6.	CONCLUSION	68
	BIBLIOGRAPHY	70
	APPENDICES	74

1. INTRODUCTION

Internet of Things (IoT, Internet of Everything, ubiquitous computing, ubiquitous Internet) and its services are becoming a huge part of modern life and ways of conducting businesses (Internet of Things Russian research center, 2013). Things that were just in our imaginations, like a digital assistant, smart home, smart car and the smart environment are now becoming real with the help of mobile devices, modern electronics and the network connecting everything into a huge infrastructure of Internet of Things.

Consider a situation, where you wake up in the morning and a sleep tracking wristband has already managed to write down how you slept and uploaded the data to some cloud service. A coffee machine and microwave received data from that cloud service and understood that you had woken up and started cooking breakfast for you. Following the data of the same band, light is going down in your bedroom. When you walk out of the room to the kitchen, all lamps are switched automatically. In the kitchen, you already expect a cup of coffee. When you leave the house and go to work, the robot vacuum cleaner starts to tidy up rooms.

This is the world based on the concept of IoT. Some of the smart IoT features do already exist, some of them are just automation. But anyway, Internet of Things is going to change the world dramatically, affecting all businesses and modes of life.

The rapid development of IoT was geared by continuous reduction in the cost of technology. In the last couple of years, we have continuously noticed the decrease of costs for different devices, starting from 3D printers to smartwatches and fitness trackers. Dramatically reduced prices of Bluetooth and Wi-Fi modules (e.g. around EUR 1 per item for the BLE module) allow connecting more and more devices to Internet of Things. (Sklyar, 2016)

Electronic sensors cost nearly nothing, but they can measure absolutely everything from temperature and humidity, and up to pressure, distance, sound power, the level of light, gravity and motion, sending all of the recorded indications to installed software. The price of computing power dropped most noticeably, making it possible to embed computer chips in practically every device. This has led to the elimination of the traditional barriers of the market for new products and companies, however, producing new ones.

Internet of Things is a logical step in the development of the worldwide network, which originally gave the ability to view static pages. Nowadays, it is leading to interconnected systems with artificial intelligence used to adapt to the whole environment to permanent changes and human needs. Modern IoT is still not developed, and 99% of all the objects possible to be connected are not connected at all. This means that the evolution of the Internet has started, but nothing is clear and architectures are still in development. Metcalfe's law states: "The value of a telecommunications network is proportional to the square of the number of connected users of the system (n^2). Imagine the situation when all new connected objects (sensors, actuators, devices, etc.) and people would add their value to the equation, raising the efficiency of the Internet dramatically. (Evans & Annunziata, 2012)

According to different studies, a number of connected devices in 2020 is going to be up to 50 billion, which is an enormous number for today (Cisco, 2016). Such fast development raises a lot of problems in the technical and business spheres. No one knows how to conduct businesses in the Internet of Things era: technologies are not clear, consumers' needs are still not stated, and even users themselves have no understanding of what they want to buy. All these troubles prevent managers from investing in IoT because of huge risks and unclear scope of work. Product developers have no idea how the final device or solution should work and what the requirements for the project are. Even the market situation is unclear. All in all, Internet of Things is something novel and undefined.

Internet of Things suggests a lot of possibilities across the healthcare industry where proper information is a deposit of fast and safe cure. Nowadays, IoT principles are already applied to some aspects of human health care, improving the quality and dramatically reducing the costs. However, not all possible applications and target patients are covered, of course. As the methods and solutions for collecting, sending and analyzing data are improving all the time, we will notice a larger number of Internet of Things driven medical solutions for monitoring patients. (Niewolny, 2014)

The purpose of my thesis work is to understand what IoT is, to define the right ways of conducting businesses in the telemedicine sector and designing a product for personal healthcare market based on performed study. I will focus on consumer-oriented healthcare to analyze the concept, architecture and technical aspects of IoT as well as business perspectives, market situation, development problems and future consumers. **This analysis would help me to prepare a whitepaper with guidelines for developers and managers in the medical**

business, which will summarize my study. The study covers key digital medicine issues, such as perspectives, security, regulations, the patients' user experience and so on. It will help IT people as well as managers without a technical background. The output should guide readers to the world of IoT healthcare, explaining minorities and possible difficulties in the medical Internet of Things business segment.

Why is my research useful? Internet of Things is a hot topic today, and many companies want to enter the market. Wide possibilities and huge target audience make the healthcare segment extremely profitable. However, it is the most difficult area to operate in because of enormous needs and regulations. It is crucial to investigate the current situation before any product development and planning because it would help to adapt the project to meet the technological and economical requirements. Target audience study would show the interest in the field. Moreover, it will outline the expected features and all possible problems and fears. Finally, I will analyze, if people are ready for modern IoT healthcare devices and what they expect from them. All in all, I would like to study healthcare IoT deeply, because it is not efficient (and not required in case of healthcare) to jump into business without proper knowledge of the whole field.

My thesis study is a part of a big research work performed at Mikkeli University of Applied Sciences. The purpose of the project is to strengthen the field of expertise in digital archiving and eServices at Mikkeli University of Applied Sciences and support the internationalization of it. Developing R&D activities in this field bolsters the regional competitiveness according to the regional strategy of smart specialization. Identifying know-how and needs of knowledge support the wellbeing of people, environment and economy. Research and development activities that are beneficial for local, national and international levels are performed at the project. As a result, the project will develop new research-based knowledge of digital solutions of everyday life, user-oriented digital services as well as information management and digital preservation, applied methods of user studies and visualized information and practically oriented publications of productization and commodification processes of digital services. The project maintains and generates new innovative research, publication and project activities as well as guidelines for the stakeholders. (Lampi, 2016) As I focus on personal healthcare, the thesis covers the user-oriented modeling of digital services research question.

The structure of the document is as follows: after the current introduction, Chapter 2 provides background information about Internet of Things, architectures, and usage cases, as well as a brief explanation of healthcare IoT and telemedicine. This is followed by personal smart

healthcare study presented in Chapter 3. The results of this study are then reported in Chapter 4. Chapter 5 shows how research from Chapter 3 could be applied for developing a personal healthcare product. Chapter 6 finishes the research by overviewing conclusions and providing directions for future work.

2. IOT OVERVIEW AND THEORETICAL BACKGROUND

In this section I am going to introduce general Internet of Things concepts. Moreover, I will discuss how it was developed and how became popular. Challenges and development barriers are also explained in following chapters. Finally, I will introduce eHealth and explain the differences of healthcare, medical Iot, telemedicine and its architectures.

2.1. IoT history at a glance

To understand what Internet of Things is, I would like to recall the history of telecommunications and Internet, firstly (Postscapes, 2015):

- 1844 – Samuel Morse sends the first morse code.
- 1926 – Nikola Tesla for Colliers: *“When wireless is perfectly applied the whole Earth will be converted into a huge brain, which in fact it is, all things being particles of a real and rhythmic whole... and the instruments through which we shall be able to do this will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket”*.
- 1964 – Marshall McLuhan: *“...by means of electric media, we set up a dynamic by which all previous technologies -- including cities -- will be translated into information systems”*.
- 1969 – ARPANET was developed.
- 1974 – TCP/IP started its operations.
- 1989 – Tim Berners-Lee proposes the World Wide Web.
- 1990 – First connected object was created (toaster by John Romkey).
- 1991 – First web page was hosted.
- 1995 – First e-commerce service started (Amazon and Echobay, or Ebay).
- 1998 – Mark Weiser: *“Ubiquitous computing is roughly the opposite of virtual reality, where virtual reality puts people inside a computer-generated world, ubiquitous computing forces the computer to live out here in the world with people.”*
- 1999 – the actual start of something called IoT. The executive director of the Auto-ID Center, Kevin Ashton, proposed the “Internet of Things” term: *“I could be wrong, but I'm fairly sure the phrase "Internet of Things" started life as the title of a presentation I made at Procter & Gamble (P&G) in 1999. Linking the new idea of RFID in P&G's supply chain to the then-red-hot topic of the Internet was more than just a good way to get executive attention. It summed up an important insight which is still often misunderstood”*.

- 2000 to 2004 – IoT is under discussions in Guardian and Scientific American. Some companies try to imagine the devices of future, and the term starts to appear in books and publications. RFID is deployed on a massive scale.
- 2005 – The Internet of Things topic is greatly highlighted by ITU (International Telecommunications Union), and the first report is published: “*A new dimension has been added to the world of information and communication technologies (ICTs): from anytime, anyplace connectivity for anyone, we will now have connectivity for anything. Connections will multiply and create an entirely new dynamic network of networks – an Internet of Things*”. (Internet Telecommunications Union (ITU), n.d.)
- 2006-2008: EU recognized the term and European IoT conference is held, IPSO Alliance (biggest members: Intel, Ericsson, Google, Cisco, SAP, Sun, Fujitsu, and Bosch) opened to study and promote the IP network of smart objects and to empower Internet of Things. (IPSO alliance, n.d.)
- 2011 – IPv6 was launched.
- 2011-today – Europe shows their continued interest and support in the subject with ICT-FP7 Work Programme, IoT-A, and digital future directives. The UK government invests £5m in developing IoT in the country. China continues to fund and support developmental research in the field at institutions. Internet of Things Global Standards Initiative started. It promotes a unified approach to the development of technical standards enabling Internet of Things on a global scale. New products are developed. Standards become common and open.

The timeline of Internet of Things can be divided into several stages depicted in Figure 1. It is clearly seen that the development of IoT is not super fast but the first huge step was taken and some studies started. Briefly, the current situation may be described as follows: increase in the number of devices which interact not only with the users but also with each other (M2M). So, each thing has a possible access to the network, but what is the need for it, is the question to be solved.

To conclude the history dive, Figure 2 depicts the popularity of “Internet of Things” search query in Google engine from 2004. The popularity is marked from 0 to 100, where a value of 100 is the peak popularity of the term. A value of 50 means that the term is half as popular. Likewise, a score of 0 means the term was less than 1% as popular as the peak. It can be seen with no difficulties that interest grows exponentially. As I speak about countries most interested in IoT, top five places are taken by Singapore, India, South Korea, Hong Kong and Ireland.

Nordic countries are in top twenty. For instance, Finland is eighth. This means that Internet of Things is a very relevant topic in all countries driving the technologies and IT revolution. (Google Trends, 2016)

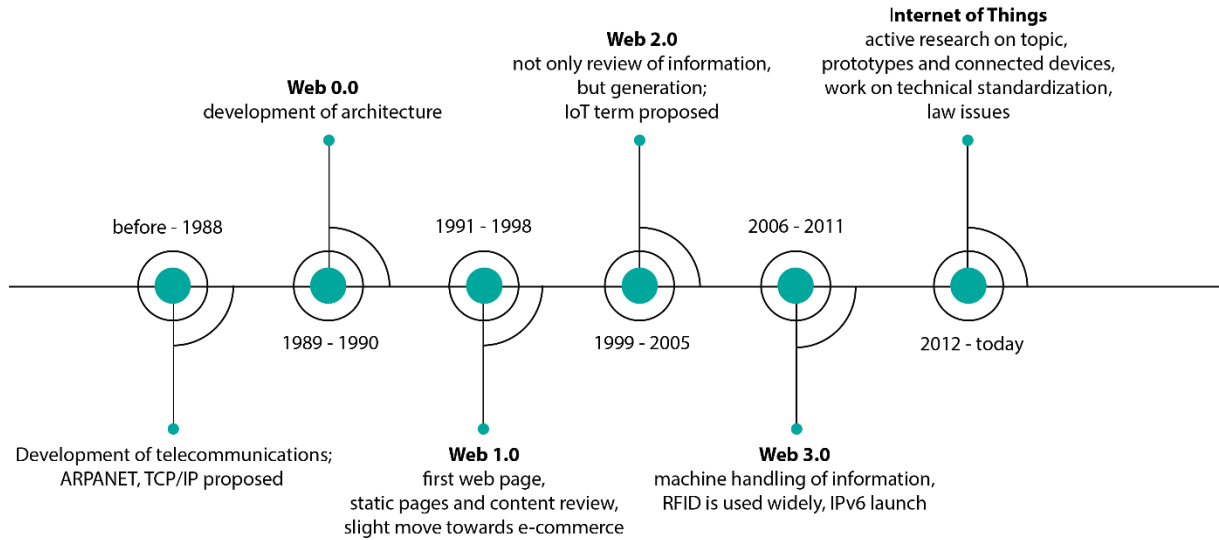


FIGURE 1. Stages of Internet development

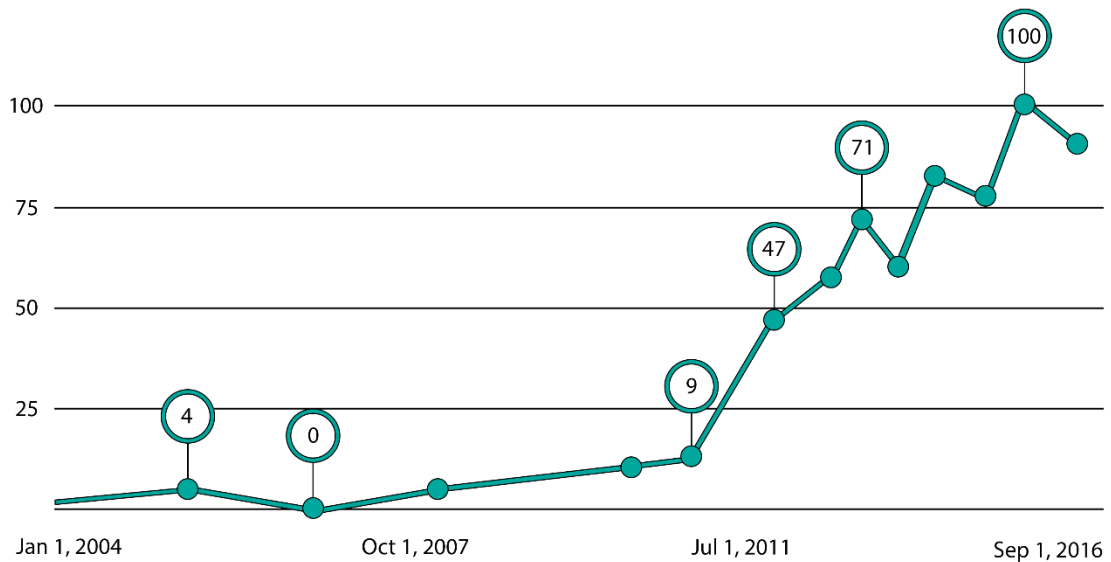


FIGURE 2. “Internet of things” term Google search popularity

2.2. Definitions and concept

Apart from Kevin Ashton's definition, there are some modern explanations on what Internet of Things is:

"Internet of Things is a kind of network form based on the Internet, extending and expanding its client into any goods and materials (M2M) information exchange and communication". (Kiritsis, 2011)

"The expression Internet of Things is wider than a single concept or technology. It is rather a new paradigm that involves a wide set of technologies, applications, and visions. Also, complete agreement on the definition is missing as it changes with relation to the point of view. It can focus on the virtual identity of the smart objects and their capabilities to interact intelligently with other objects, humans, and environments or on the seamless integration between different kinds of objects and networks toward a service-oriented architecture of the future Internet". (Vermesan, et al., 2011)

"Internet of Things (IoT) is an integrated part of Future Internet including existing and evolving Internet and network developments and could be conceptually defined as a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual "things" have identities, physical attributes, and virtual personalities, use intelligent interfaces, and are seamlessly integrated into the information network." (Iera, et al., 2010)

The term has many definitions quite similar to each other but with some differences. Out of all clarifications, I would like to propose mine, which would be used as a concept of IoT defined in this paper:

Internet of Things is a network connecting people, real and virtual objects together adding a digital layer to all sides of life. It produces clear benefits for users. The whole Internet of Things infrastructure is the concept of space in which all of the analog and digital worlds can be combined, changing our relationship with objects and properties, and the essence of the objects themselves in core. Internet of Things is not just a lot of different 'things' (instruments, devices, and sensors) connected to each other by wires or wirelessly, but it is an integration of real and virtual worlds in which communication is performed, and

everything is controlled by users. The environment is a smart and permanent adaption to events occurring is done, consequently, IoT could be believed to be an artificial intelligence.

The next issue to be explained is the term thing:

According to my IoT definition, the thing is any real or virtual object that exists and moves in space and time, and can be uniquely determined. It is expected that in the future, “things” become active participants in business, information and social processes where they can interact and communicate with each other by sharing information about the environment, responding to and influencing the processes occurring in the real world without human intervention.

Every “thing”, starting with the tiny sensor and ending with the robotic manufacturing arm, has the following characteristics, showing its belonging to IoT infrastructure:

- Sensors (embedded or the sensor itself) – Devices and systems have sensors that track and measure activity in the real world.
- Connection – There is a straight connection to the device or it is indirectly connected via a hub, smartphone (in the case of wearables, for example) or base station, while the whole local IoT system is connected further to the Internet in any case. These connections between devices could be implemented by the use of other wireless technologies (to be discussed in 2.5.2. “Foundational technologies overview” section), instead of IP connections.
- Processing unit – As any calculating unit, the device in the IoT environment has some processing power for analyzing data and sending it. There are some exclusions here, and several remotely manageable appliances or sensors have no calculating capabilities. However, they still have logic for handling received or sending data.
- Energy efficiency – All IoT devices should be efficient enough to perform the required task without big electricity consumption.
- Economic efficiency – Of course, big solutions, like smartphones or smart home appliances are expensive, but sensors and small actuators must be cheap in manufacturing and support.
- Quality and reliability – IoT devices should be able to work in aggressive environments, in open air, in water and for long periods of time. Even user devices must be robust and well built.

- Security – Devices should be able to transfer data reliably and securely. Protection and privacy are big issues. For example, in the case of medical monitoring data could not be caught or changed.

Internet of Things is considered to have four layers of operational areas (not to mix with architecture concepts) (Iera, et al., 2010):

- Layer 1 – identification of each object
- Layer 2 – services for people’s needs (for example smart house)
- Layer 3 – digital urbanization, the concept of smart city
- Layer 4 – sensory planet

Nowadays, humanity is more or less ready with only two layers of Internet of Things, so the full potential of these technologies is not experienced yet. These layers show that IoT is a network of small networks, connected together (for example your device in a smart home and your smart home in a smart city). To meet the idea of IoT, everything should be involved, which is shown in Figure 3. The question is in the necessity and logic of connections as well as management of huge amounts of data. Some manageable and ordered system is needed, which is today’s engineering challenge.

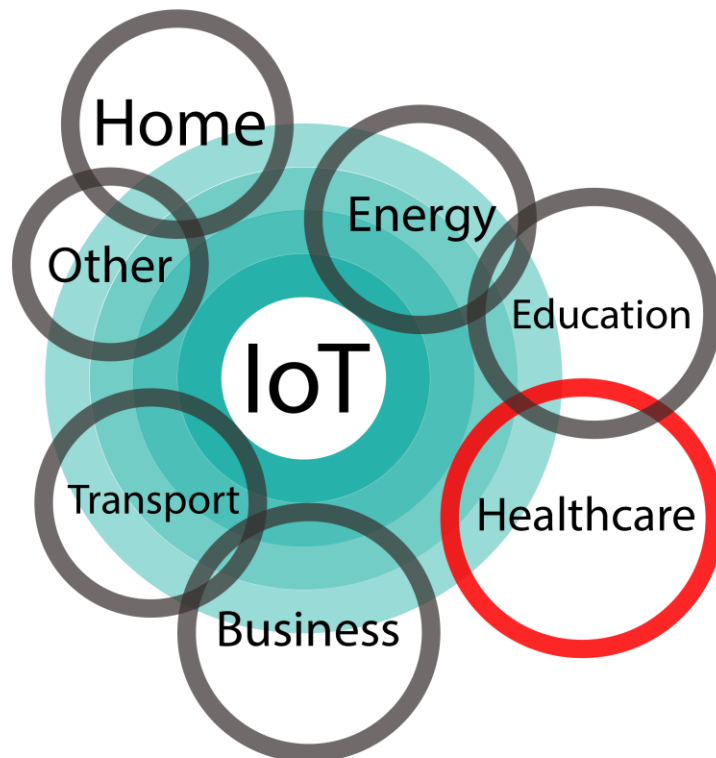


FIGURE 3. Internet of Things scope

2.3. General architecture and characteristics of IoT

Internet of things is quite different from common Internet in communication aspect. For us the normal that communication could be established at any time and from everywhere, however Internet of Things has additional dimension – “anything”. So, the concept of IoT has some characteristics that demonstrate multi-dimensional comprehensiveness, information sharing, and intelligent processing:

- Interconnected. Internet of things facilitates people to devices and devices to other devices.
- Smart sensing. The majority of devices and actuators have embedded or connected sensors to detect current conditions.
- Intelligence. IoT devices have some calculating units and software used for smart decisions, predictions and automation control.
- Energetical efficiency. All IoT devices have to be efficient and able to use recyclable energy, boost own energy harvesting, if the application of device requires and allows it.
- Expressing (or data sharing). IoT connected devices have the capability to express and share their current state to all other connected devices. It allows better communication flow between user and machines.
- Safety. Internet of Things devices should help ensure the safety of individual life. All medical smart devices are a good example of this characteristic.

Moreover, Internet of Things has functional peculiarities:

- Function to get information from things
- Function to exchange information
- Function to process and control information intelligently
- Function at large scale

Internet of Things is determined by its architecture, which is able to collect all the characteristics and functions and make them operate correctly and smoothly in one unique architecture. There are two types of known architectures, 3-layer and 5-layer ones. I would take a look at extended architecture, as it covers business issues also.

Figure 4 shows the architecture and it includes following layers (Gang, 2011):

- Perception layer (sometimes device layer or data collector and coordination and collaboration). This layer deals with data collected from things. For example, sensing devices. Analog of the physical layer in OSI networking model.

- Network layer (sometimes transmission layer). Transfers information from the things to other things and information processing systems.
- Middleware layer. This layer is responsible for information processing and producing decision based on analytics performed.
- Application layer. Provides the applications based on the object information processed in the middleware layer.
- Business layer. Responsible for the management of the whole IoT ecosystem.

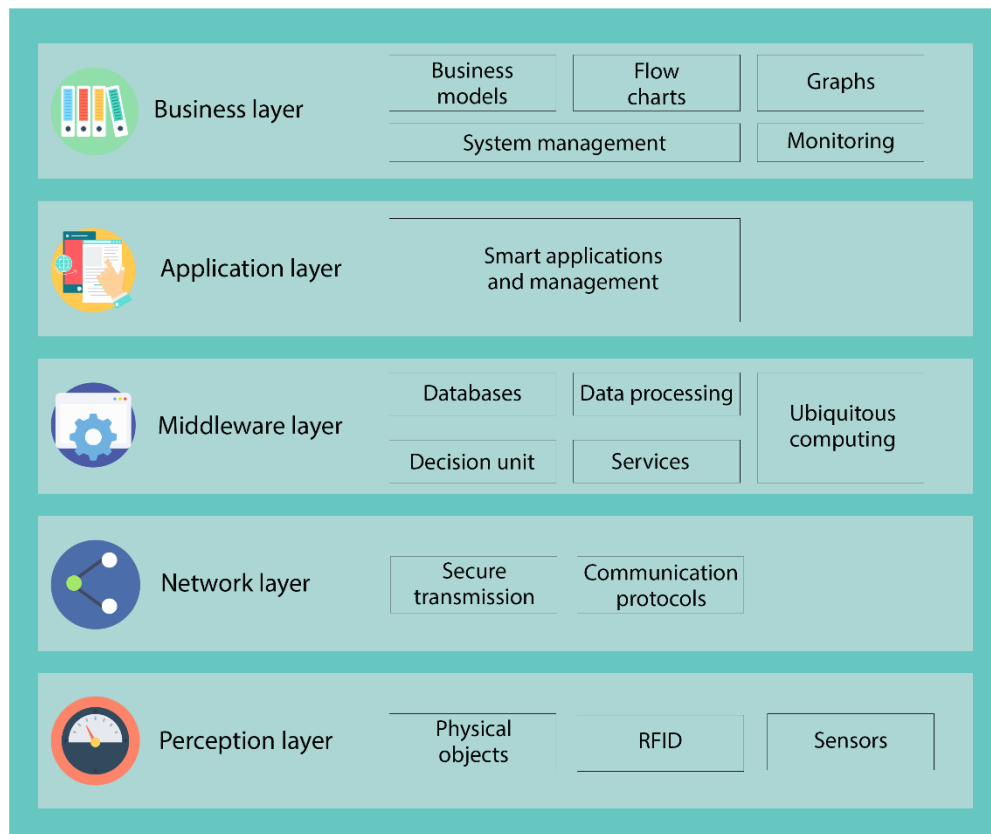


FIGURE 4. Internet of Things architecture

It was stated a lot of times that things are permanently connected with each other for communication but they are not necessarily able to transfer data between each other. This ability depends on the similarity of the services they are assigned to do. Single thing lacks the ability to reason on its environment and to subsequently make smart decisions and actions to achieve objectives. While the entire system can do it, so the whole system could be represented as something intelligent but not a single device in it. Here are some more features of Internet of Things that are important for understanding the concept:

- A single thing is not smart, but ecosystem is
- Decision making and all actions are service-dependent

- Things communicate in IoT infrastructure only if it is needed and/or they are designed for it

2.4. General IoT peculiarities and challenges

This chapter is about non-evident IoT development barriers. Of course, developing batteries of huge capacity is a big challenge, however, there are some more general and core troubles, which must be solved to enter the era of IoT.

2.4.1. Automation vs. smartness

It is not possible to develop Internet of Things rapidly in our existing environment because the current view on IoT is not clear and root approach should be changed completely to achieve exactly intelligent technological world. Most often, the concept of IoT is inseparably linked with something “smart”: smart homes, smart blood sensors, smart transport, smart businesses, however, when we look at that intelligence closely, we understand that remote control lamp in the house is just an automation, but not the clever or smart house and even digital syringe controlled from smartphone is not smart solution, as there is no intelligence and further connections in the system. It seems that nowadays Internet of Things is not intelligent and it is not clear what smartness is.

The emergence of Internet of Things is an expected step because laziness is the engine of progress. Moreover, people want to benefit from existing technologies at full power. Around 20 years ago the air conditioner at home was switched on by the user when it was too hot or cold. After some evolution of computing, we have some device in between, which is programmed by the user to turn on heating or cooling automatically, depending on the connected sensor. Finally, the house turned out not "smart" because such an approach slightly changes the situation, but the user still should control everything. It turns out to be automation.

So, what is smart IoT? This is a set of technologies, which will change the paradigm of achieving the result so that user should set the target, not the means of achieving it. Those are the characteristics of smart IoT:

- a) Permanent support of user by objects
- b) Clear processes and result orientation
- c) Request to do instead of rules on how to do

In the case of medical instrumentation, let's define characteristics of a smart insulin pump:

- a) Active CGM monitoring and permanent insulin delivery
- b) Data analytics based on collected data and connected medical APIs
- c) Request to keep normal glucose level

The biggest question now is how to achieve goals described above and the possible numerously discussable solution is the multi-agent architecture. The foundation of multi-agent approach is the concept of a mobile software agent, which is implemented and operates as an independent specialized computer program or an element of artificial intelligence. The essence of multi-agent technology is a completely new method of solving problems. In contrast to the classical method, when a search is carried out by a well-defined (deterministic) algorithm, which allows finding the best solution for given problem, in the multi-technology result is obtained automatically as an outcome of the interaction of many separate software modules (so-called agents). (Wei & Toenjes, 2012)

Each user and each device in the real world are assigned to a software agent - an object with a certain degree of intelligence, which represents its interests in the virtual world. The virtual world can be called somewhat improved copy of real world with same parties that often follow pre-established and well-known rules, providing reliable answers to questions. The relationship of real and virtual worlds is bidirectional. It means that solutions from the virtual world are given to reality for execution and all the unintended events of the real world affect the virtual world. (Mzahm, 2012) Figure 5 depicts the multi-agent communications system implemented in IoT infrastructure.

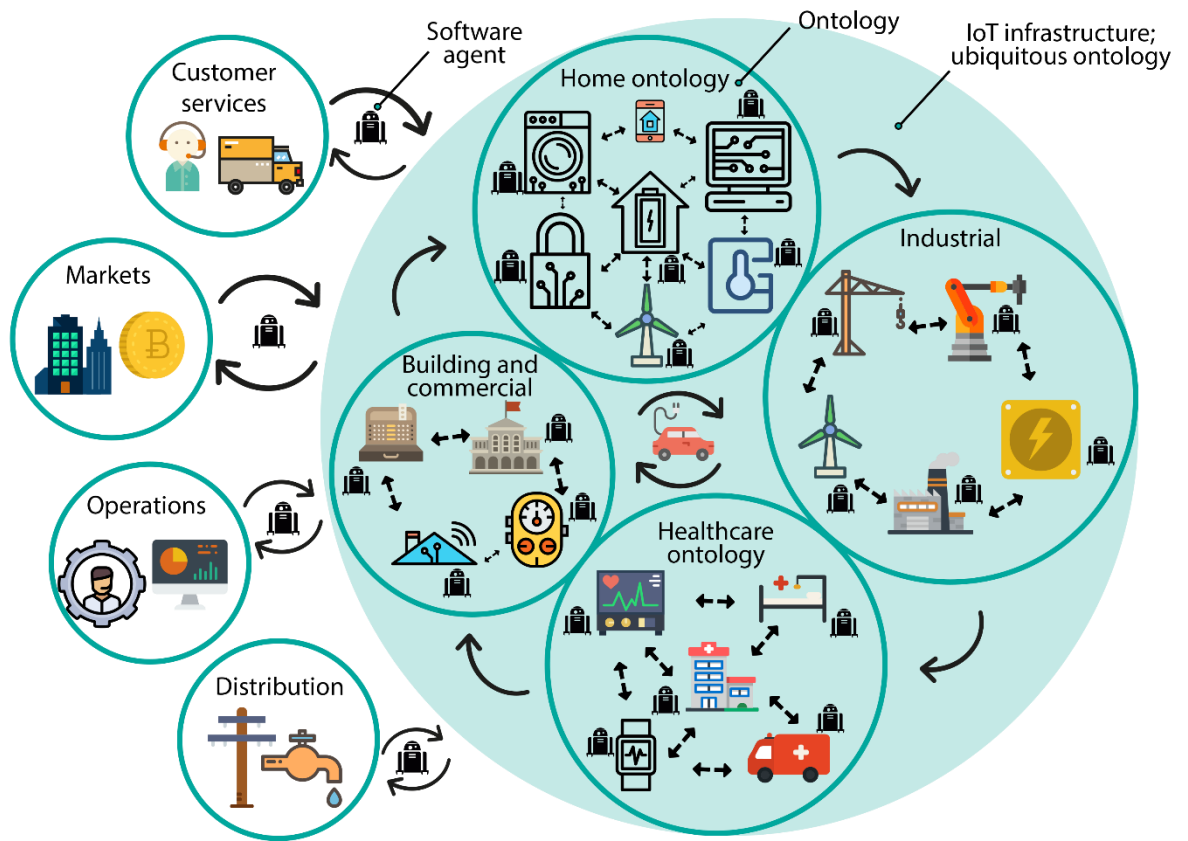


FIGURE 5. Scheme of multi-agent system communications in IoT

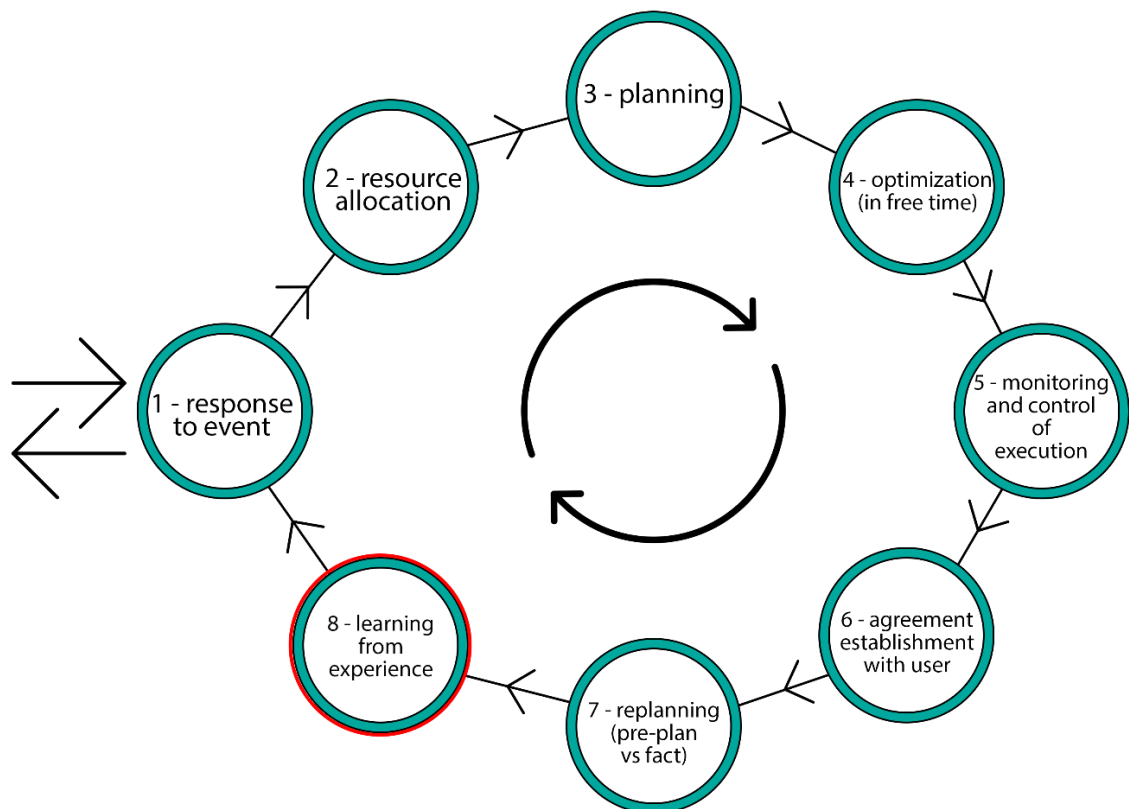


FIGURE 6. Processing an event by an agent

First of all, agents perceive information from the real world. Then it should be treated, so some actions are planned, which should be accomplished by giving the appropriate commands into the real world. Figure 6 shows the process in steps.

Let's look at such system by use of real examples (scheme on Figure 7). Consider a situation when the user wants to prepare a meal, and occasionally there is no more milk in the fridge. Now there are three possible paths. First one is applied in completely non-IoT infrastructure and user would go shopping to the grocery store. The second path is what we have today - automation in IoT. The user would order some milk by smartphone, for example. The third solution is about smart IoT, and it could be achieved only by use of multi-agent systems. Then fridge agent will ask to restock milk even before the reserves are exhausted, by putting the request in the queue of purchase agent.

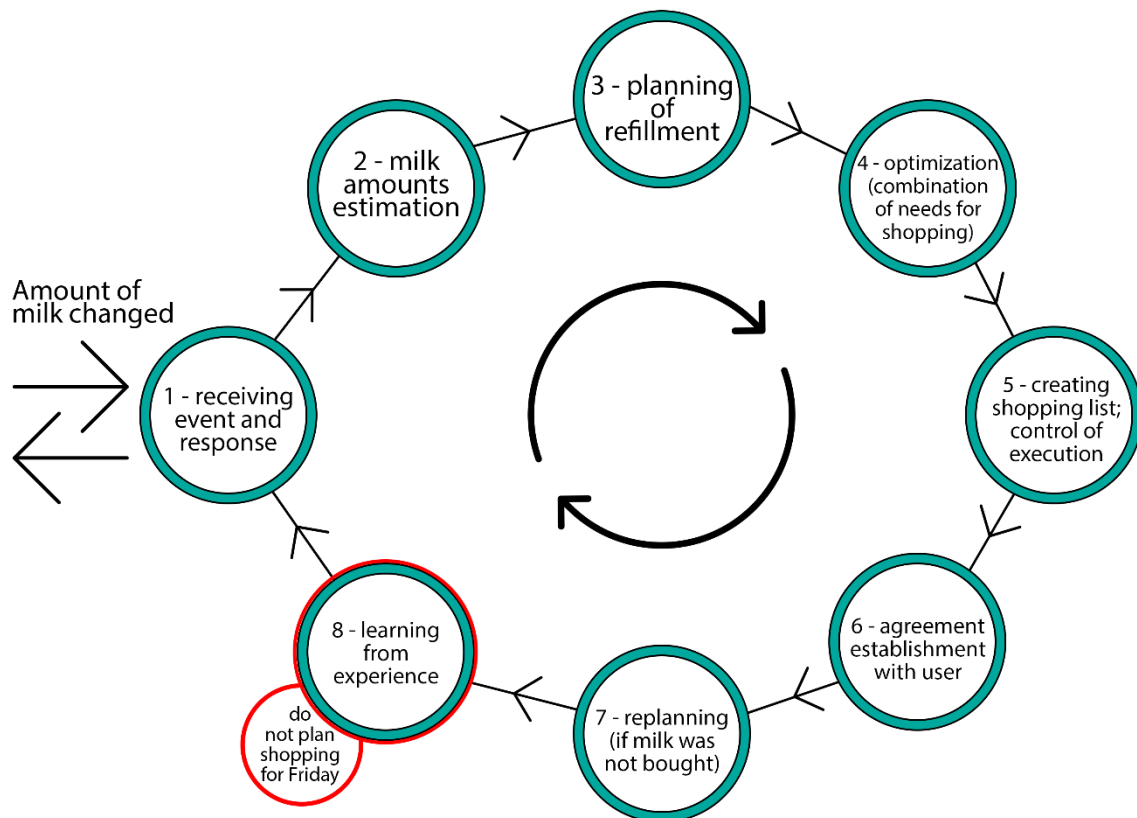


FIGURE 7. Process of fridge refillment (example based on Figure 6)

Next logical question is a storage area for agent information and its relations. Principles of ontology could be used for it. Ontology is a relatively versatile and machine-readable way to represent different knowledge. In ontology, we can describe important concepts and logical rules, while intelligent agents use this knowledge to achieve the objectives and for interaction.

It is quite difficult to develop an ontology for the whole Internet of Things environment due to its enormous size. The much simpler way is to develop one ontology per each sphere of living and matches between them. That way all things with their agents would be assigned to some ontology in a logical for human manner. (Wei & Toenjes, 2012)

As seen from above the main role of ontology is to store knowledge in a structured way. This knowledge contains the description of the physical essence of the world. But what if we go deeper and store the rules of relations and logic of IoT in the ontology. On practice, a newly connected device would automatically detect the sphere he is going to work in, his features and possible communications from the ontology. For example, if smart heart rate monitor is connected to IoT infrastructure, it gets an agent first, which is a part of healthcare system ontology. Then agent notifies the whole system about new device presence and its features, needs. Such as heart sensor can control rate and stability of pressure and heartbeat, it needs power and connection to medical APIs, also calibration is needed once per two years. Those messages would be received by all interested or responsible agents, like home-based health adapter, for instance.

To make the system completely intelligent, the agent of the smart monitor could request data from agents (again presented in the same ontology) of a glucose meter, meteorocenter. Possessing such data AC could predict the pick moments and notify the owner in critical situations beforehand, allowing avoidance of emergency.

In the described intelligent Internet of Things, the user is a full participant in all processes, and he always sees the latest information. Of course, all of our areas of life will be closely intersected. It is imperative that the intersection of these areas was viable and useful to the user. After all intelligence and self-operating environment people must benefit from technologies anyway. All the presented examples are about smart homes. However, multi-agent systems are needed to support every segment of the IoT environment, and healthcare is not an exception.

By now there is no clear understanding of how to achieve the goals described in the previous paragraph, but world-know institutes are working on the multi-agent approach design and artificial intelligence. My opinion is quite strong in this field – it is not possible to create true IoT without implementing multi-agent systems and machine learning. That's why I decided to move focus from the main topic and highlight that trend, as healthcare is also a very tightly connected system, which requires the correlation of sensors and medical actuators.

2.4.2. Problem of standards

Alongside clear IoT barriers, like creating efficient batteries, decreasing power consumption, implementing IPv6, creating extra efficient wireless technologies and so on, there are some unclear and questionable issues, which must be solved to boost Internet of Things development and final appearance of it in our lives. The rapid development of Internet of Things has begun to encounter the same problems that hit the revolution in the field of personal computers in the 1980s. At the moment, the problem is not how to bring a product to the market, but how to develop appropriate standards, without which the various devices will be just a heap of junk, unable to communicate with each other.

The careful examination of everything is critical, from hardware compatibility and up to the data storage methods in the cloud. Before progress goes too far, the market needs to develop applicable standards. To show the trouble, I present the current variety of different standards and alliances.

Qualcomm is one of the leaders in producing CPUs for phones and tablets. The company is also a major player in Internet of Things market since the development of AllJoyn protocol, which was the basis for creating AllSeen Alliance. The alliance was formed in 2013 and has already received the support of the largest manufacturers of home appliances, such as Electrolux, LG, Panasonic, Sony and the industrial giant Bosch.

A direct competitor of AllSeen Alliance is Open Interconnect Consortium (OIC). The consortium pursues the same objectives as the AllSeen, trying to create a standard for the synchronization of devices that form Internet of Things but without the use of Qualcomm's AllJoyn protocol. OIC Consortium was created in 2014 by such giants as Intel, Samsung (what is strange, because Samsung is working together with Qualcomm) and Broadcom. Soon, however, there was a rift between the parties, and in October 2014 Broadcom left the group.

Intel has also created a separate alliance Intel Internet of Things Solutions Alliance, which, obviously, is going to use a more integrated approach, promoting the brands of its members, such as Dell, Hewlett-Packard, Fujitsu, Microsoft, and Oracle.

It's obvious that games around standards and attempts to monopolize the market are creating a lot of noise around. Smaller companies and enthusiasts are not sure which protocol or framework to use, what produces more and more questions. At this stage, no one is going to make

any concessions, and, it seems that the market would choose the winner, but it will take some time, moving the beginning of a true IoT era to the indefinite future.

So, what should be done to finish the innovating/development stage and to focus on implementing the environment? In my opinion, the existing infrastructure should be used, and all new protocols should be based on the previous work done. By existing environment, I mean IP networks, which are the Internet. However, IP communication protocols are not applicable for transporting data from sensors and wearables to head devices and gateways.

According to Maciej Kranz, vice president and general manager of Cisco's corporate technology: "the industry is beginning to realize that the fragmented, closed model is not amenable to scaling and limits the benefits of the introduction of Internet of Things." (Kranz, 2016)

Again, according to Cisco, the work on standardizing of IoT is done in four directions (Cisco, 2016):

- 1) Development of existing IP and Ethernet: IEEE and IETF are focusing on it, creating requirements for such spheres of IoT as deterministic Ethernet, for example.
- 2) Managing industrial branch standards: main players in the industry make standards out of their proprietary protocols, creating contradictions, which hampers compatibility. To convert existing standards to IP and Ethernet technology, while ensuring compatibility with inherited protocols, IoT industry cooperates with big commissions.
- 3) Creating architectural models: the general model is being created by IoT World Forum to ensure mutual compatibility of all components in the whole environment. The suggested model has seven layers, which gives an ability to use open IoT systems with guaranteed unity:
 - a) Collaboration and processes (people and business processes)
 - b) Applications (reports, analytics, control)
 - c) Abstraction of data
 - d) Data storage
 - e) Analysis and calculations (data operations)
 - f) Communications
 - g) Physical devices and controllers (things of IoT)

- 4) Opening consortiums to manage the biggest problems: as discussed before, the situation is difficult here, because everyone wants to win the game with their proprietary standards. However, on the other hand, the truth (better solutions, in our case) emerges from the clash of opinions.

To conclude this topic, my opinion is so that IoT is seeking for open architectures on the IP base with open standards. It will boost mutual compatibility in IoT, therefore allowing to realize power solutions and business models, detecting monopolists and outsiders on the market. Of course, some companies would lose the race, but this is the price for customer satisfaction and IoT appearance. As moving towards the main focus of thesis, the multi-agent method could increase the efficiency of telemedicine at least twice, as all monitoring systems would be connected to hospitals and with any other smart devices, databases, etc., while all logic and security would be monitored inside ontology.

2.4.3. Traditional vs. digital economics

I have observed quite a lot of factors dilating the rate of IoT development already. Such as technical and technological standardization, security of communications and transactions. There are some opinions about unsolved problems of the devices themselves on the part of the constant power supply, stable performance and ease of use. Some skeptics are inclined to believe that people are psychologically and socially, in principle, are not ready for a comprehensive digital environment. But now I would like to think about other factor affecting the growth of Internet of things segments – owners and management companies misunderstand ways of doing business in the new global information economy, which is more and more guided by a multi-level instant digital consumer interaction, objects, and algorithms. Perhaps this factor is the main "brake" for Internet of Things?

To find out what is hard to understand for business in new economics, let's define the differences between traditional and modern digital economics (IDC, 2016):

- a) The global information network is ubiquitous – any information could be accessed from anywhere at any time.
- b) Devices are mobile and smart – lots of “things” learned how to implement a fairly complex functionality and share structured data.
- c) Users are demanding – users now are quite diverse in professional and psychological level, they can present complex requirements and expect a personalized approach to their needs.

- d) Information became the main and most expensive resource – the majority of high-quality information has become more expensive than any other material resource. Monopoly on information is an impossible thing to own and defend, but developing new project or business is impracticable without significant information support.
- e) Risks raised – it is crucial to defend against increasingly complex risks undertaken different approaches to ensure business stability by transferring valuable financial resources from main operating competencies.
- f) Management principles are outdated – managers of the companies use the tools, developed for previous, or “pre-digital”, economics. Those old methods limit the ability to make right decisions in time.
- g) Modern marketing is complicated – it is necessary to effectively carry out business strategy without succumbing to an external marketing ploy. Understand the essence of the proposed products is more and more difficult task, and the consequences of wrong decisions are harder to calculate.
- h) Dependency on competitors and market raised (that’s why I am analyzing the situation before product development) – all businesses are highly affected by all changes.

Specialists in different spheres became independent – different professionals may change spheres of work. Also, it is complicated to audit technicians, because of their limited amount and huge professional competence.

According to particularities of digital economics found, I can estimate the incomprehension of entrepreneurs and managers and suggest possible solutions for problems. First of all, there is no clear view on which physical “things” and logical objects should be connected to the Internet to gain something. This is an important question of allocating deficient resources – of course, it is possible to proceed with a big amount of objects and employees in information exchange, but what are the benefits of it in operations management? Secondly, all current management technics are targeted on people, but how to administrate “things” is not defined. From the one hand, this sounds wonderful and convenient to appoint tasks to robots or algorithms, but, from the other hand, after a while, the manager realizes that the same robots and algorithms are working only in the established boundaries and functions are prone to mistakes. Things are straightforward enough in their actions and decisions and are not able to adapt business processes, in response to the rapidly changing situation around (that’s why I discussed multi-agent approach in Chapter 1 as a solution for a big range of troubles).

Another urgent issue is finding a customer in constant market dynamics, the variability of moods and strong informational dependence. New products are developed rapidly, consequently, people are not able to catch all trends, so the new product should be as detailed as possible to get some attention. To continue, information itself is problematic, because it confuses management, while complicated mathematical and statistical methods make actual decisions. Management trusts those mathematical models that are designed by undeniably talented professionals, but often not enough to understand the subject, economics, and marketing of given business.

There are more issues to be discussed (How to create a good team for IoT project? How to protect the business from risks? How to communicate with partners and competitors?), but it will not lead to any solutions. To my opinion, there are several steps to adopt management and business to a digital economics.

Marketing should be personified. At a time when markets demand high-quality and cheap products and the manufacturer can flexibly implement any design and art solution, it became really difficult and needed to adapt and deal with each particular customer. In an economy of consumption, where the set of goods, works and services are so closely linked, the business cannot be satisfied only with information about the simple "flat" market segments; it is relevant to know as much as possible about the complex market segments, define consumers within a multi-level classification. Not only relationships with customers should be under control, but also customers' relationships with each other.

New management instruments should be created. The manager should be able to make decisions on the go. Comprehensive model with adaptive expanding configuration is needed, where all information management tools are located. Such infrastructure could not be universal, because of different business areas.

The customer should get the real product, but not a prototype. Of course, IoT offers innovational products with huge functionality, but the user wants to see a "thing", not an idea, as he is not an investor. Moreover, professionals should teach other specialists, and whole project and human resource management systems have to fit digital economics. It means that old management methods are changed to new methodologies, like SCRUM, for instance. Finally, developed network of the partners, services, and communications is significant. Product with rich integration is more attractive for final users.

All in all, businesses need to fundamentally rethink the business model, including the methods of competitive advantage formation. If automation left some chances to save at least part of the traditional business processes, Internet of things is tough in this regard - we have to consider the problem in a comprehensive and wide manner, changing everything. An artificial narrowing of perspectives and scopes of IoT leads to the obvious inefficient investments. In total, to work into digital economics following functions should be implemented:

- a) Data analytics
- b) Knowledge and best practices management
- c) High-level competency support
- d) Designing of basis and special business models
- e) Researching and using complex marketing and financial schemes
- f) Development of standards and regulations
- g) Elevation of customer communications efficiency
- h) Permanent development of technological, manufacturing and management processes
- i) Risk management

2.4.4. Security

From tiny sensors to huge machines, the Internet of Things is expanding at great speed. Intel stated that 10 years ago, there were only 2 billion smart objects associated with the wireless world, and IDC estimated the number of connected devices by 2020 would be already 200 billion (IDC, 2016). Almost any connected device, starting with smart TVs, a fitness tracker or a home security system and ending with printers, automotive systems or lights with control over the network, will sooner or later expose to hacking. Below are some illustrative examples of such break-ins:

- More than 8,000 people have been victims of hacker attacks when hackers from the group Anonymous invaded the infrastructure of the European Space Agency and the stolen names, email addresses and passwords of people were then published in the form of three dump data in justpaste.it service.
- Symantec is using a specially configured computer Raspberry Pi, to attract attention to vulnerabilities lying on the surface of the fitness trackers. Security experts have found that some of these devices allow attackers to easily monitor the location of the tracker.
- A hacker and expert on cyber security, Chris Roberts from the company One World Labs in Denver, USA, managed to crack the onboard entertainment system in the plane and, according to the FBI report, dated April 2015, to intercept the aircraft control.

Because of huge amounts of information generated by the connected devices, priorities should shift towards the protection of the data that is important. The first step in creating a security infrastructure is in the study of species occurring threats. In addition to phishing, DoS and DDoS attacks and physical intrusion into the era of gadgets widespread hacking applications. Today the market offers a special automated tool for hacking, many of them are free. The fact is that in contrast to centralized Web environments, mobile applications are placed into non-regulated mobile device ecosystem. Unprotected code of mobile applications (the same one that you download when installing an application, for example, from the store AppStore or Google Play) allows attackers with ease to modify these applications and use them to their advantage. Because of such attacks, nine out of ten organizations (90%) experienced a negative impact on its business, including delays in product or service development (31%), reducing the productivity of their employees (30%), reduction in consumer confidence (28%) and a certain pressure (24%) (Compton & Mickelberg, 2014). All these points have a negative impact both on the corporate reputation and on the general performance of the company as well as the confidence of their customers in this industry.

The authentication procedure is an important aspect of working with connected devices. For example, when we open a smart car with a mobile phone, we want to be sure that no one except us can do it. Equipment suppliers should also be authorized to access the remote device. For example, Tesla electric car manufacturer notifies drivers about the availability of firmware updates and when this update will be downloaded. Thus, the driver realizes that the update has been received directly from Tesla, and it is not attempted break-in. For a more secure authentication, biometric data is used more widely, which allow reliably confirm that we are the ones who we are expected to be.

Analysis of the situation shows the need for a comprehensive and science-based approach to ensure the safety of the Internet of things:

- Risk assessment - for the developer, it is important to understand all potential vulnerabilities. The assessment methodology should cover the issues of privacy, security, prevent fraud, cyber-attacks, and theft of intellectual property. Risk assessment is not an easy task because the cyber criminals are constantly searching for and gradually learn more and more new types of threats. And as a universal solution to neutralize these threats do not exist, at this point it is recommended to invite a security expert consultations.

- Security at the design stage - the key point is that the safety of the device must be considered in the design. This includes the safety of the end points and preventive measures, including the creation of protected to breaking hardware and software.
- Ensuring data security - strong authentication, encryption, and secure management of encryption keys should be used to protect the information stored on a device, and at the time of its transfer.
- Lifecycle management - security should not be seen as an isolated process that just runs it once and forgets about it. It is important that the device used in the Internet of Things ecosystem are protected throughout their lifecycle, no matter whether it is a standalone product, or of a certain system, for example, integrated into the car.

Read more about security problems of healthcare IoT in 3.4 “Analysis of positive contribution and risks” section.

2.5. Telemedicine, healthcare and medical IoT

The difference of the telemedicine and healthcare/medical Internet of Things is small, however, improper understanding of terms leads to confusions in the field. In this section I explain the stated terms as well as how I use them, and how all of them are connected to treatment and IoT.

Telemedicine is the use of medical information exchanged from one site to another via electronic communications to improve, maintain or assist patients' health status. Closely associated with telemedicine is the term "telehealth," which is often used to encompass a broader definition of remote health care that does not always involve clinical services. Videoconferencing, transmission of still images, e-health including patient portals, remote monitoring of vital signs, continuing medical education, and nursing call centers are all considered part of telemedicine and telehealth. (Higgs, 2014) In simple words, telemedicine is Internet of Things applied for medical purposes, so it is a resumptive term used to describe modern ways of medical care with the use of information technologies.

Both medical and healthcare Internet of Things are considered to be telemedicine, but they are different. Healthcare is a type of medical care which is targeted to monitoring the normal conditions, supporting chronic states and using preventive approaches to ensure the healthy lifestyle. Medicine in the case of IoT is an area which is responsible for emergency treatment, diseases' studies and medical sciences. For my thesis, I consider medicine is something happening in the hospital to recover the health after some accident or illness, consequently

medical Internet of Things is about stationary solutions, medical databases and professional connected equipment. Healthcare Internet of Things is a set of different technologies and devices used to support personal health. That's why the terms healthcare IoT and personal healthcare IoT could be used interchangeably. Healthcare IoT provides personal services by using personal devices and systems targeted for a single person.

Continuous glucose monitor, pacemaker, cloud service with health records and children tracking device could be considered to be personal healthcare Internet of Things systems. Later in my paper, I will use all the terms, and sometimes medical IoT could be used to describe the whole stack of smart medical services, as healthcare is a part of medicine, while telemedicine is a new approach to medicine. Even if terms are different, all of them are tightly connected and it is not possible to study only one field, as all of them are about human health treatment and none of the fields could be considered as something separate. Internet of Things contributes to the improvement of the health system by increasing the transparency of processes and optimization of operating activities, which in turn helps to improve the quality of patient care. I will discuss more benefits of eHealthcare in the section 3. "Personal healthcare IoT study" and further.

2.5.1. Architecture of healthcare IoT

Continua health alliance has released the end-to-end architecture for connected health applications. This is the achievement of the more than 220-organization alliance, is said to be a noteworthy milestone in its goal to create an environment of interoperable connected personal health systems. The Continua end-to-end (E2E) reference architecture provides a high-level architectural overview of the ecosystem, includes three network interfaces and four reference device classes, and indicates constraints in topology, see Figure 8. Using the new end-to-end connected solution, devices can transfer data from consumer health devices to medical offices, hospitals, patient information systems, etc.

The Continua Design Guidelines (CDG) define a framework of underlying standards and criteria required to ensure the interoperability of components used for applications monitoring personal health and wellbeing. It also contains design guidelines that further clarify the underlying standards or specifications by reducing options or by adding a missing feature to improve interoperability. (Continua Alliance, 2016)

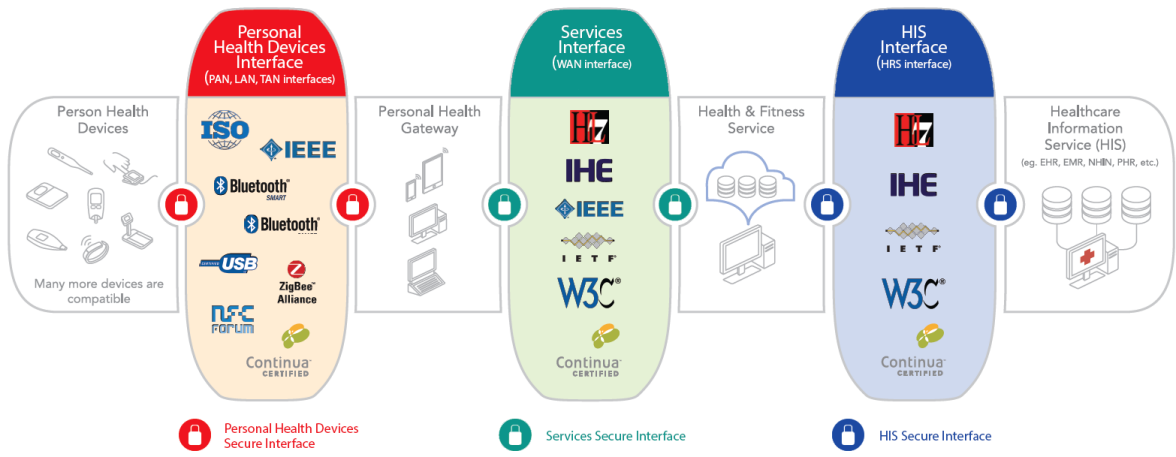


FIGURE 8. Healthcare IoT architecture proposed by Continua

3. PERSONAL HEALTHCARE IOT STUDY

In this chapter I will analyze the situation with healthcare Internet of Things. First of all, I am going to discuss the need of smart healthcare and why IoT can improve this relevant sector. After it, I am going to make a study of Finnish consumers, which will help me to understand the needs and readiness of people to smart wearables or even implanted solutions. Finally, I will speak about security concerns, positive contributions and proper approaches for building proper smart device and eHealth business. All results would be highlighted in the whitepaper prepared for IT and business specialists desiring to enter the smart healthcare market.

3.1. Motivation for healthcare IoT and study

Effective medical technologies are always the most relevant because maintaining health and the quality of life for years remains an urgent task. Internet of things in many ways alters notions of access to health services, increases the quality and reduces the cost. The habit of using smart things help the patient and the physician to cooperate efficiently in the diagnosis and treatment processes.

Modern technologies allow handling such enormous amounts of data that traditional methods have been physically impossible to master. If a person regularly monitors his health, the medical card swells to 2TB of data (Fox, 2010). Usually, this information is dispersed and stored in different locations on paper. Digital history (vaccinations, diseases, appointments, examinations, etc.) allows to forget and to lose nothing. Taking into consideration the important factors reduces the risk of incorrect diagnoses and prescriptions. Also, it is possible to remotely conduct consultations with leading experts, which increases the overall quality of medical care.

Health organizations, in accordance with their orientation, will be able to develop their own medical applications. Already the applications remind patients to take medicine on time, watching the human physical activity. The current control methods with external sensors and mobile phones would seem a hopelessly outdated technology and no one would be surprised by embedded in the lens and attached to the human skin sensors, or even when necessary implanted directly into the body.

Nowadays, global healthcare system wastes \$2 trillion per year (Korsten & Christian, 2010), which shows complete inefficiency, as changes are minor. Healthcare systems are the least efficient, comparing to other systems, and it has the biggest improvement potential, as Figure 9 shows. This prostration is mainly caused by the inability to properly collect data and transfer

it for subsequent analysis to support diagnosis and treatment method selection. The medical literature is doubling each seven years, and it becomes impossible for doctors to understand the condition of the patient and to prescribe a needed treatment. Moreover, the amount of patient data is dramatically expanding because of genomic data, making diagnostics even more complicated. Today 20% of medical errors are caused by diagnostic errors, which are not only incorrect diagnosis but delayed ones (IBM, 2015). Connected healthcare devices have a huge potential to accelerate the speeds of patient appeals and doctors decision-making, providing time for proper and efficient treatment, by collecting and analyzing patient data and medical resources.

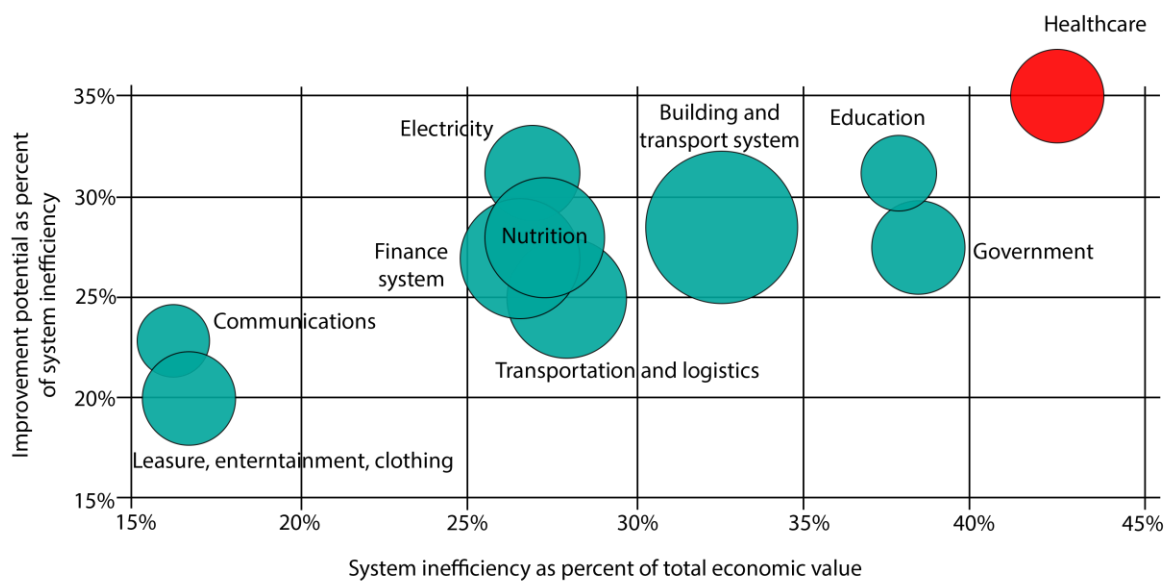


FIGURE 9. Inefficiency and improvement potential of different systems

Healthcare presents IT and medical companies a new business operating area, which is a rare situation in the 21st century. Even more special, this white space allows companies to make money while simultaneously doing a significant job for society. All in all, healthcare IoT can revolutionize in medical treatment, providing new ways for improved diagnosis and treatment, making people healthier in efficient and cost-effective manner, but the question is what companies should do to bring innovative solutions to the healthcare community and change the medicine completely. So, the aim of this study is to answer these questions and provide guidelines for proper design and development in telemedicine, making the bridge between medical, IT and business specialists.

3.2. Wearables and the user study

The focus of my study is personal healthcare Internet of Things, consequently, I would investigate wearables and research its existing audience and possible users conducting a quantitative study of a target group of 100 people of different ages, experiences and social groups. See Appendix 1 for the questionnaire. Wearables are the only type of smart devices that can deliver true personal experience and services. Of course, stationary home appliances are also the case but most of these products are borrowed from healthcare providers as they are more advanced and specific. To this group, I do not include hubs or some in-middle solutions, because of their supporting nature, but they are still smart healthcare IoT solutions. Therefore, by wearables in the thesis I mean:

1. Usual wearables which are used for patients' or users' continuous monitoring.
2. Smart solutions for monitoring and automation, for example, insulin pumps or other injectors.
3. Some of the implanted devices that could also be considered as wearables, in my opinion, as they are permanently in the body. Of course, it is a bit different situation, but pacemakers are included in the scope, as they are one of the most popular embedded actuators and it is more accurate to count them in the study.

First, I would understand what wearable is and how devices evolved. After it I will analyze possible consumers and patients, providing key findings which could be used to properly design the device to meet the needs and financial possibilities of the target group.

Wearable technology includes different items which could be worn on, in and around the body and have embedded electronics (logic and sensors) (PwC, 2014). Wearables are emerging slowly, however, they help to build a new health economy. It is the type of economy which transforms on the industry's economy, where people are no longer just patients, but healthcare customers. The traditional money flows in healthcare are changing, we have new stakeholders in the market, retail, telecom and tech sectors, etc. (Ledger & McCaffrey, 2014)

Today, our digital life is centered around smartphones and mobile technologies, but the technical community is always trying to enhance the scope of possible applications. Wearables are devices that promise to entertain, support users and provide great input/output, sensing capabilities. As I focus on healthcare wearables, they will produce huge amounts of raw data which could be used for analytics. Analyzing collected information could be performed by the use of smartphone calculating power and custom applications. This potential of the smartphone and wearables combination venture investments in eHealth and wearables technologies. In 2014

the smart health startups raised USD 2.3 billion and more than USD 200 million were only for wearables (Rock Health, 2014).

After small initial research, wearable technology occurs to be quite well-known and people are highly interested in it. 74% percent of respondents in Finland, 18-45 years old, know about smart health tracking, 18% have heard about it, but have no idea about applications of it. 8% of all respondents have never heard about wearable technologies. The situation with older people is only slightly different, which is quite surprising. In my opinion, pacemakers played a big role here because Finland is one of the leading countries in implanting pacemakers (PM) and implantable cardioverter defibrillator (ICD). In 2009 there were 796 PM implantations per one million of inhabitants in Finland, in 2013, 1020 operations were performed and the year 2016 number is outstanding - 1470 successful implantations (European Heart Rhythm Association, 2014). Moreover, the audience was asked how likely each of the following is to come about as a result of wearables use:

- 47% believe that life expectancy will grow by 10 years because of permanent monitoring available
- 34% believe that wearables will help to reduce national obesity levels, as they can help to count calories and monitor exercises in tight communication with specific mobile applications
- 21% believe that wearable technology and gamification would improve average person's athletic ability
- 71% think that wearables would increase the efficiency of diagnostic and treatment
- 58% believe that wearables designed for automation (actuators like insulin pumps) would increase the life convenience of people with chronic diseases

Due to the fact that wearables are only at the first stage of development and adoption, it is quite promising statistics, which shows that Finnish people are living at the technology edge, and they are quite ready for healthcare and medical revolution. Nowadays, only 1 in 10 users have a wearable and use it every day. If we also count insulin pumps and pacemakers 2 out of 10 respondents use some smart solution for healthcare use. These numbers show that even if wearables are a trend, not everyone wants to use them. Probably, the reason for it is the small variety of different solutions on the market. All products are quite similar and trivial. In Finland, 18% of the population (all ages) currently own a smart healthcare wearable product. 10% out of that 18 % use their smart solution daily, however, 1% of the owners have some device but

never use it for some personal reasons. Other people wear it few times a week and few times a month 5% and 2% respectively.

As the numbers above show, Finnish people have not fully accepted wearable technologies. The interest is still very strong. Among people with no wearables (82% of the population), more than half is not against using a wearable and most of them said that they are “very” or “somewhat” likely to buy a new device in a year. Mostly, they are interested in health monitoring (74%), automation solutions (9%) and fitness bands (63%). There is less interest to smartwatches and glasses. Only 3% of respondents are interested in clothing. Among all interviewed of any age, social position and income, the tendency is quite clear:

- Smart health monitoring device owners tend to be younger males (16 to 45 years old).
- Smart automation systems’ owners tend to be both males and females (18 to 68 years old). Older people are a bit worried about automated injections and try to avoid such kind of appliances.
- Fitness band buyers are a quite interesting group, as females of any age are more interested in tracking the exercises.

All survey participants weighing the purchase probability said that they are mostly hesitating about prices, privacy and security issues, technical faults and possible interest loss to usage. The last worry is quite critical and the situation is so that, according to some studies, a lot of users stop using newly purchased smart devices within few months (Ledger & McCaffrey, 2014). The main reasons for it are a big amount of required attention for syncing, charging and other steps to keep it running. Others say that their life convenience was not changed with a smart solution. Building a great appliance requires device makers to meet the consumers where they are and keeping the user engaged in first weeks of use is a relevant part of any healthcare Internet of Things strategy. Companies must consider innovative methods for rewards, incentives and actionable insights as a part of the whole sphere of user experience. Also, the big challenge is to select an appropriate target audience and hook the people who can benefit most. Nowadays, wearables and other smart solutions are targeted to people who already know the things and understand the benefits. This group is tiny. Read more about it in “Exploring new audience”.

Smart healthcare IoT solutions must meet the requirements of all ages. Some really targeted devices must be specific. For example, insulin pumps must be universal and user experience should be applicable for the child, adult, and elder, while ADHD monitors have to be

specifically developed for children, as well as elderly people's monitoring systems (Jane, 2011). Analyzing motivators for purchasing some smart healthcare device, I understood that companies must develop algorithms that can turn data into some clear insights for users or healthcare providers and all of the prepared insights must be involved into daily deeds. According to the survey, smart healthcare apps should contain following characteristics:

- Interoperable and connectable to different solutions with open standards (21% of respondents)
- Intelligent to provide useful insights (99% of respondents)
- Integrated to user's life and healthcare (67% of respondents)
- Social to be shared (7% of respondents)
- Engaging (48% of respondents)

To meet the enormous number of consumer's caprices healthcare organization and device makers must cooperate tightly to sharpen business models, build credibility and ensure data match system needs. Read more about it in "Exploring new audience".

The biggest question of every business is money, consequently, I analyzed the payability of possible and existing smart healthcare Internet of Things users and, of course, the majority of consumers do not want to pay much for their device. Modern engineering and materials allow making a device of any price. People are different and everyone needs different services. Price is the biggest concern for 91% of all the respondents. The money issue is even more relevant than security and privacy. In Finland all employees are insured by the government, employer, and organizations like Kela, so 59% are willing to receive smart healthcare appliances from these organizations. If we consider a situation when user still needs to purchase the device himself, 42% of population are ready to pay less than EUR 50, 27% can buy device for EUR 50-120, 23% are willing to pay EUR 120-200 and 8% of Finnish consumers are able to pay more than EUR 200 for smart healthcare appliance. Companies working with health and wellbeing can expect to buy if incentives are offered. Another step to attract consumers for smart products is a human touch. It could be used to help to choose a device and applications and navigate through a variety of health apps and appliances.

To continue, common and simple strategies are not working well with personal healthcare solutions, as consumers do not want to share health data, even if they trust doctors. Only 1 person in 5 wants to share his personal medical data with friends and family. 1 person in 20 will allow public access to their data through social networking. As I speak about parameters like

weight, sleep schedule or diet, 7%, 25% and 12% respectively would allow sharing. The quite captivating factor is interest in other's health. Almost no one (2%) is interested in their friend's health conditions, more people are concerned about family and children, 62% and 77%, correspondingly. All numbers above are applicable only for biological information, however, 23% of users are willing to share their exercise activities, so sport smart healthcare device industry could benefit from social media. It is an important path to customer engagement. For some people, the success of friends or a family member is perfect motivation. But getting consumers to share more personal data will require innovative and targeted approaches.

The situation with chronically ill people is completely different, as they are willing to share completely personal medical data for the community with the same disease (The Telegraph, 2011). People with cancer, diabetes, Parkinson's disease, hepatitis and HIV/AIDS want to be in the community to support others and get motivation. Virtual communities and disease-specific message boards are flooded with patients seeking to connect with more experienced people. PatientLikeMe is a great example of such portal. It consists of 250 000 members and there are millions of reports about 2 000 conditions.

The last topic for analysis is privacy. 68% of smart healthcare users say that they can trust their personal doctor. Moreover, healthcare providers (hospitals) and pharmacies are ranked highly. 46% of respondents can trust these organizations. Companies should ensure that privacy policies are completely clear. It should be a standard that healthcare providers and doctors may receive personal data by default, as audience trusts them. The generally required trend is transparency, but there is a variety of challenges here. See Appendix 2 for infographics and summarized audience study. Check 4. "Study outcomes and results" section for results, conclusions and recommendations.

3.3. Exploring new audience

Nowadays, the situation is so that all healthcare device makers are producing devices for two limited groups of people (PwC, 2014):

- Fitness people and highly healthy people
- People with hard chronic diseases

It is clearly seen that these two groups are edge points of the whole mass of possible users. Between these extremes, there is a huge disintegrated group of common people who are looking

for some wearables or other devices for extensive health monitoring. They are looking for information to avoid possible risks and to make some steps in time. Figure 10 depicts the target audience for health Internet of Things.

According to The Telegraph study (The Telegraph, 2011), at the end of 2009 the overall size of consumer-oriented medical IT market was \$290 billion. Imagine the size of the market when companies start to produce solutions targeted for everyone, instead of focusing on two limited groups. Possible consumers are quite healthy people with some troubles and bad habits, they are living without any devices today and even do not know about telemedicine. However, they could and want to use information gathering and monitoring solutions. They are looking for products that can provide hidden medical information to obtain ultimate health control without much attention and costs. We are now entering the era when technology is developed to the needed level and companies from different industries are willing to collaborate to produce better systems and needs of customers. Our environments become more digitalized and interconnected, consequently, health control solutions can become more advanced and intuitive, as well as cost effective. All factors (need and possibilities) make IT companies think about targeting usual people with new medical devices, however, managers and developers have no understanding of what are people looking for.

So, the next logical question is why to enter the segment now. As consumers begin to pay higher amounts for their health, I believe that people are more and more motivated to purchase an Internet of Things solution for self-monitoring to avoid huge medical and insurance costs. Moreover, the modern rhythm of living creates time frames for everyone, so there is not enough time for visiting doctors, while medical wearables would notify users and control the health status. Finally, the main reason for focusing on suggested segment is because it is feasible, what was not the same slightly in the past. The Internet and affordable sensors could dramatically improve the treatment and health management. (Christina, 2014)

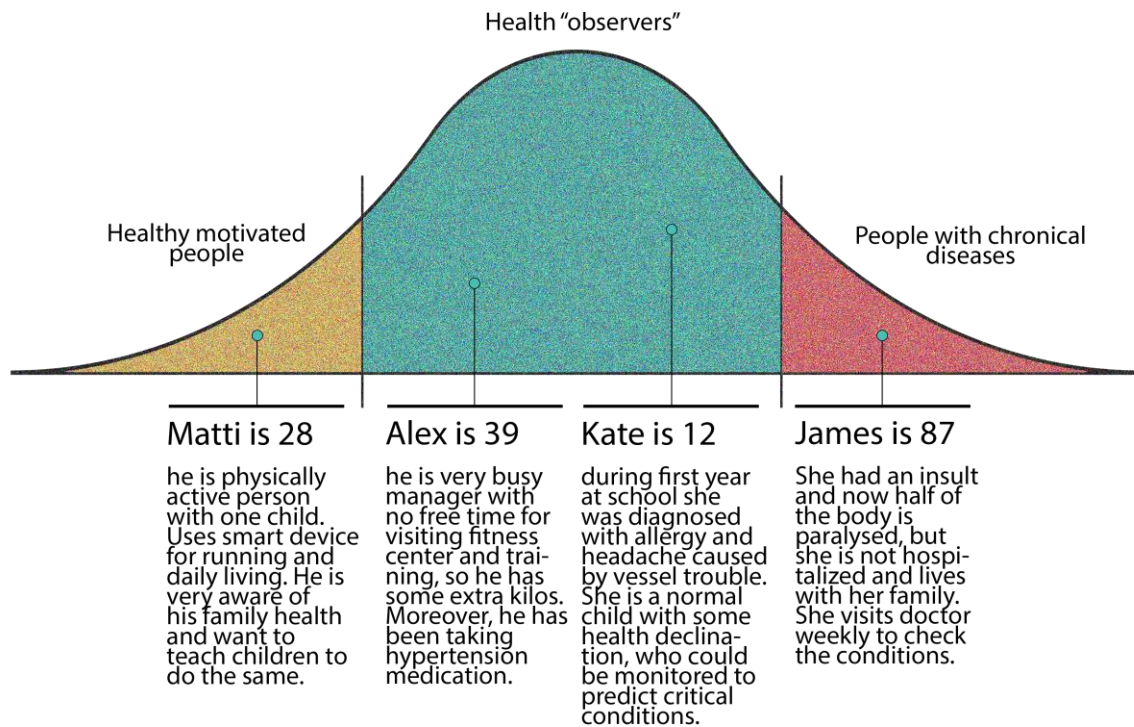


FIGURE 10. Example target audience for healthcare Internet of Things businesses

Let's understand the characteristics of consumers who want some medical information ("health observers" from now). That segment could not be presented as one structured group with same trouble and requirements; it's a heterogeneous set of consumers:

- Want to monitor health to take actions before actual illness started
- Want to break bad habits and addictions
- Are partly disabled and want to live independently
- Old people living alone
- Want to control the prescribed regime or pills reception for dose control
- Struggle with cardiac arrhythmia, high blood pressure, allergy, asthma and bronchitis, diabetes. In other words, struggle with conditions that require nearly permanent, seasonal or full-time attention and treatment with individualized approach
- Need temporary medical monitoring in case of rehabilitation or stresses
- Small children and mother home health monitoring after parturition

All of the possible cases shown above are just examples, and real scope is nearly borderless. See Figure 11 for some more cases and statistics.

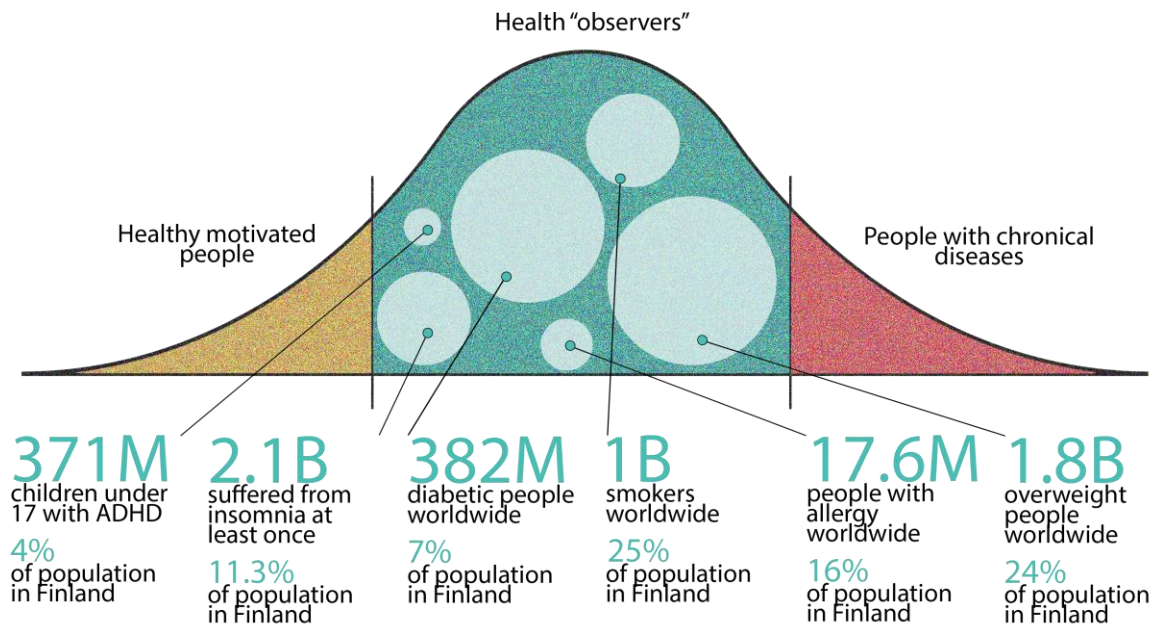


FIGURE 11. Examples of target groups with statistics in audience of "health observers"

To reach the "health observers" auditorium businesses have to develop solutions meeting important requirements and fulfilling the needs of all consumers (adults, children, old people, disabled people):

- Cost-effective and simple - as current users with ultimate motivation (life or death or heavy fitness interest) to use healthcare IoT rank those two criteria as the main ones, the situation will not change with "observers", as they will not pay money for the incomprehensible and expensive device. The adoption of new technology will depend on making the monitoring device and system easy for users. Everything should be intuitive, good-looking, featured and designed for specific "health checker" with a focus on his area of anxiety.
- Allows real-time monitoring - people are looking for devices that help with complex situations or just control the health. Telemedicine solutions should replace classic approach for analysis and diagnostics allowing health checks without multiple ineffective doctors visits. Also, permanent control would help to detect hidden troubles, which appear randomly, so they can not be detected in the hospital. Another motivation for such systems is fear of doctors, which prevents proper diagnostics because of stress (very popular among children).

- Internet-connected devices - collected monitoring data is nothing for the consumer, so it should be transferred to healthcare providers, who can discover it. Connection and ability to share medical observations with doctors give the main worth for IoT devices. This point produces an issue of the value of the single device and the same device in big interconnected infrastructure. That side of question would be discussed in Chapter X.

To sum up the requirements see Figure 12, where three main aspects of attention for product development are highlighted.

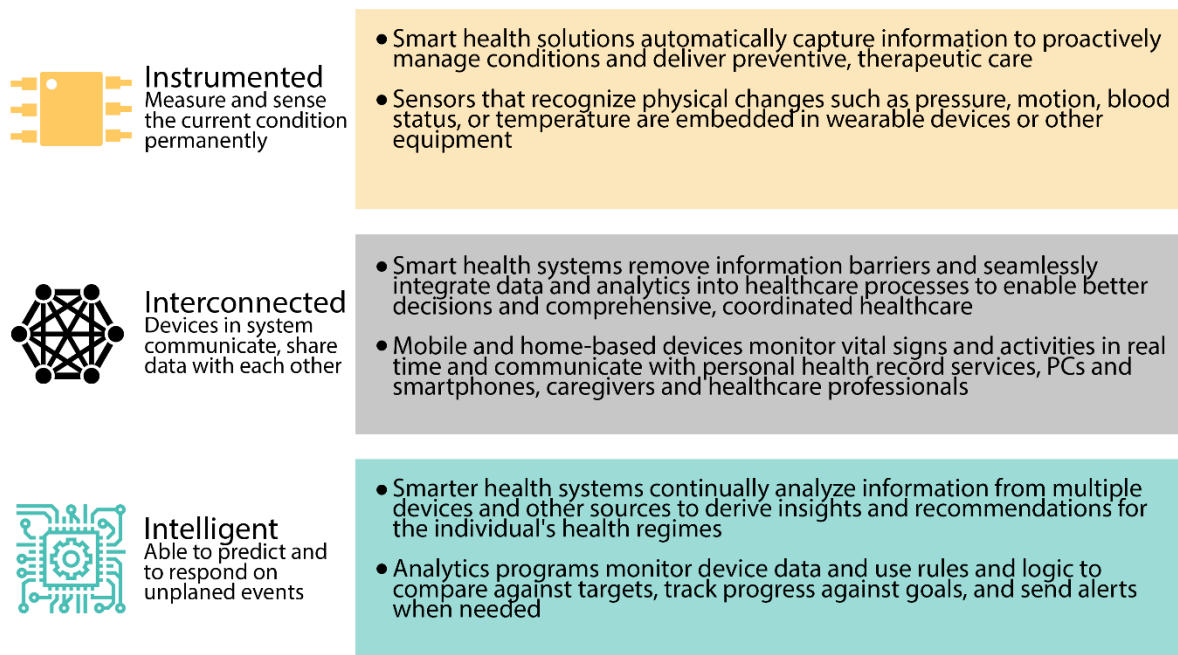


FIGURE 12. Characteristics of good smart healthcare solution

The majority of health devices today lack the use of connectivity or only locally connected, however, there are some innovative products on the market already showing the tendency of Internet of Things in healthcare (IPSO alliance, n.d.). Chinese company Xiaomi offers cheap and useful activity, sleeping and mood tracker. The market is filled by same wearables, but all of them are working not perfectly. Fitbit went further, and the company provides online storage for collected data and several analytics tools. Finnish Polar and Suunto are working with same projects, however, they are a little sport-oriented, which is still healthcare Internet of Things. As I speak about medical consumer products, Medtronic and Kaleido are leaders in diabetic treatment (Kaleido, 2016). Their insulin management solutions analyze data from pumps and continuous glucose monitoring sensor and send all information to the personal doctor. Real-

time control of sugar level and auto-injections helps people with diabetes to reduce the risk of glucose or insulin starvation.

From previous examples, it is clearly seen that there are two types of companies researching and developing smart solutions for healthcare: medical device makers and electronics makers. Both competitors have some strengths and weaknesses in the new market. Consumer electronics businesses are better in branding and managing the loyalty of consumers. Moreover, they have bigger consumer bases and existing digital products, which could be adopted for telemedicine. From the other hand, such organizations have no understanding of healthcare and human treatment. Also, their experience with products of strict regulations is little, what makes entering the market more difficult. Of course, regulation procedures are very different, depending on the country, but mainly, auditing of new healthcare and medical devices is very tough. Medical companies have more collaboration with care providers and understanding on healthcare, as well as a suitable technological stack to be used. They understand the principles of medical sensors and possibilities for invasive and non-invasive monitoring. The fact is that they can make an efficient medicinal product, but it will lose consumer-related games, as medical device makers do not understand the needs of healthy people, which should be reflected in features of the specific gadget. Finally, they are completely not familiar with consumer-oriented design, interfaces, and product placement. Probably the success is hidden in collaboration and partnerships.

3.3.1. Principles for delivering personal telemedicine

Entering the proposed market requires not only an innovative, usable gadget but success will only be achievable with the strong ecosystem. By ecosystem I mean a comprehensive infrastructure of different solutions with excellent user experience and support, see Figure 13. Following elements could be a part of the product for healthcare produced with Internet of Things principles in mind:

- Intelligent and connected device itself
- Online purchasing and support
- Warranty services
- Compatible accessories
- Social network
- The web or mobile application for self-data analytics
- Environments for medical professionals
- Hospital education

- Healthcare service providing

Delivering such kind of solution requires partners and collaborators, as a single company is not able to operate such widely from scratch. It means that adoption will depend on standards used (open standards are advised), interoperability and compatibility. This outlines the fact that companies from medical and healthcare, electronics, life sciences must communicate to introduce proper healthcare Internet of Things, while separate devices are just automotive solutions without smartness.

Rapid evolution and adoption of mobile devices provide a great opportunity to make healthcare gadgets cheaper and more integrated to lives of users from the very beginning. The smartphone is a perfect gateway for health data. It can process, analyze and structure it, without any extra hardware unit. According to “Mobile Health 2010” by Susannah Fox, even in 2010 17% of smartphone owners used applications for health monitoring or for looking up medical information. 9% of interviewed people used applications for activity tracking (Fox, 2010). Moreover, 10% (or 1.09 billion) of all downloaded apps from Google Play (Market in 2010) and iTunes store were closely related to medicine and lifestyle. Nowadays, the situation is even more developed. Twice more people are using apps for health monitoring and tracking. 87% of users tried at least one application. (Mark, 2011) Statistics show the tendency of rising interest to telemedicine, consequently wearable (mainly wearables can sense the body properly, see Chapter X) devices would be demanded, as they support the need for the efficient approach. Nonetheless, gaming electronics and fitness equipment are becoming useful for healthcare monitoring, as they introduce new methods of remote tracking.

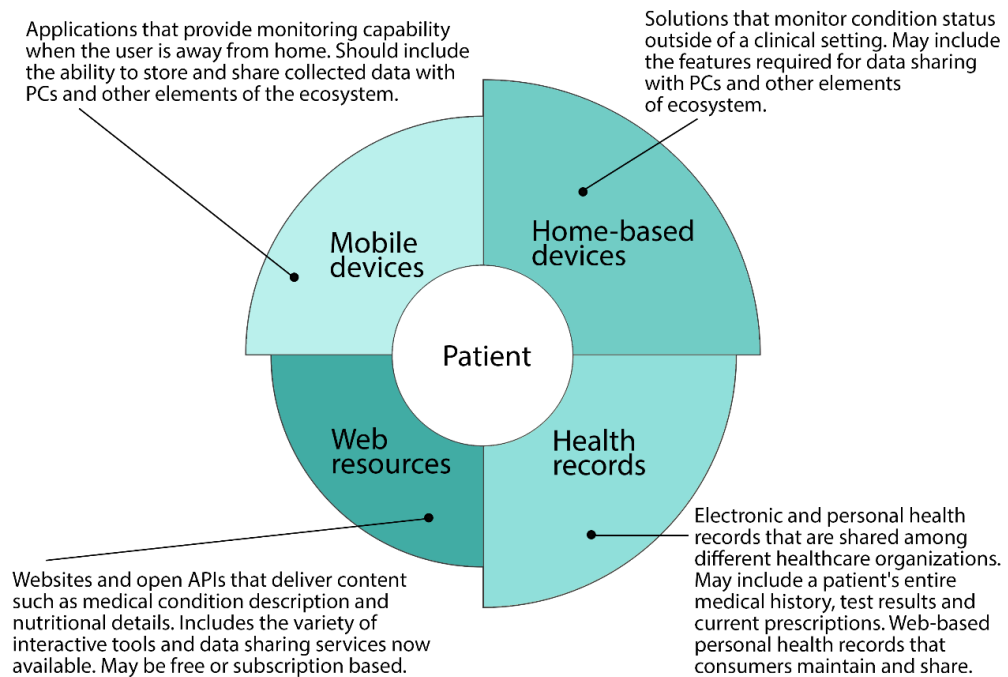


FIGURE 13. Elements of smart healthcare solution

For companies willing to expand to the smart healthcare market, I suggest to follow four main principles:

- Make an easy solution.
- Design the device with the end system result in mind.
- Choose business positions and partners deliberately.
- Set the rules and work on standardization.

Making a simple device with intuitive controls or application is very important, as the adoption of the new product will depend on simple approachability of monitoring for everyone involved. As stated before, device and user interface have to be intuitive and not too featured at least at the beginning, while consumers take up the technology. As for examples, elders need static interfaces and full automation in settings and device set up. People with diabetes seek for permanent notifications and rich decision-making capability. Kids with ADHD need a very basic user interface, which will not distract them from learning the process or playing. On the other hand, busy executives would prefer rich featured device and powerful mobile app. All in all, each solution should be personalized for target group with specific monitoring goals or disease. Systems should help users to control the health passively setting the rules for actions and feedbacking. Regarding data presentation, measurements should occur for the user in a structured format with clear visualization. Finally, the user must be the head of the device, consequently, the possibilities for configurations have to be wide (even for children with ADHD

initial parent or doctor set up should contain a rich list of preferences). It is nice to mention here, that breakthroughs in technologies will provide new methods for simple user-device interaction. For instance, augmented reality will allow to see notifications or call for urgent actions immediately without any attention to the device or smartphone themselves. Bioacoustic and other non-invasive sensors would allow measuring difficult and hidden conditions of the body painless and on the go.

Consumers need a comprehensive system to meet the objectives of health monitoring maximally absolute. It requires integration with healthcare providers, social organizations, insurance companies and so on, consequently, the appliance must be designed with the end system result in focus. Integration into diagnostic and cure processes are important, consequently, data should be stored in easy to examine and transmit format. Data analytics is another important feature because users will get some understandable outcome, not just raw measurements. It means that the real value of smart healthcare is in data, which should be mined, consolidated and explained. Social networking integration is another must have for healthcare Internet of Things because it will help people to find other struggling with the same condition. It will allow receiving advice and gain motivation, providing not only physical but a mental cure, which is not less important.

Next, business positions and partners should be chosen thoughtfully. Companies need to select an optimal sphere and business position in healthcare ecosystem by evaluating their operating strengths and weaknesses. Partners are crucial because the single company is not able to provide full smart healthcare system at this stage of development, see Figure 14. In the medical market, healthcare providers are the ultimate partners, because consumers follow their recommendations. Moreover, they are one of the most important parts who use the devices and applications, so they could easily reject the solution and it will ruin the business. Finally, device makers should collaborate with hospitals and pharmacists, as well as with insurance companies.

Finally, set the rules and work on standardization for the whole sector. The industry is looking for interconnectivity of all devices. Therefore device makers collaboration is needed, which will help to set the requirements of technologies and regulations for the connected health device ecosystem faster. The best example here is Continua Health Alliance (Continua Alliance, 2016), which consists of around 250 companies from IT, governance, and medical fields, working on developing norms and regulation, as well as certification processes.

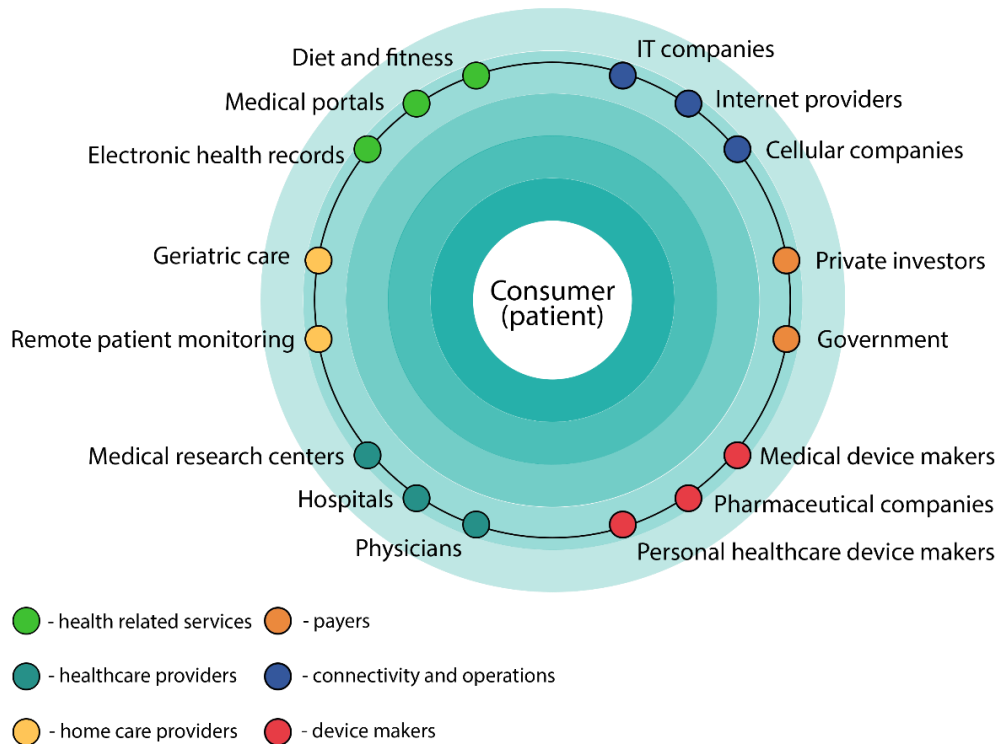


FIGURE 14. Ecosystem of participants needed for delivering telemedicine services

3.4. Analysis of positive contribution and risks

In this chapter, I would like to speak about possible risks of healthcare Internet of Things and their correlation with benefits for society. Previously, a lot of different advantages of telemedicine were presented, but in this chapter I would like to analyze the risk landscape behind good promises of digital healthcare, understand the sources of risk in modern networked medical devices and, finally, prepare recommendations for maximizing value to patients while minimizing security risks coming from software, hardware, firmware and communication technologies across personal medical devices. The aim of this chapter is to find the balance between clear benefits and ability to protect the technology and communication foundations of modern devices.

The rewards of bringing Internet of Things to healthcare is not so perfect, and it is producing some areas of concern. To understand the risks, I would firstly briefly analyze the promise of digital medical technologies again, to show the roots of security troubles. There are four main types of telemedicine devices, shown in Figure 15. I would focus on personal ones only, as they are the focus of thesis study and because of the high difference of stationary medical appliances in applications, security, and regulations:

- Consumer products for health monitoring
- Internally embedded medical devices
- Wearable, external devices

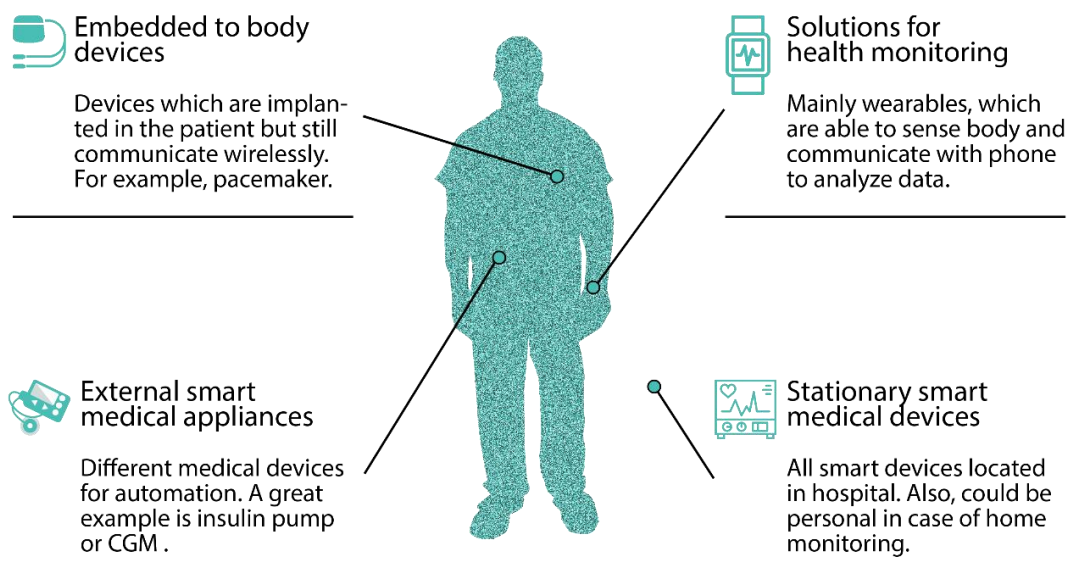


FIGURE 15. Categories of smart medical devices

One of the main ideas of healthcare Internet of Things is to individualize medicine by allowing people to select needed devices and systems to meet their goals for health, what makes the first risk - now each owner of the medical device could be attacked personally. Another advantage of digital healthcare is permanent monitoring and big amounts of statistical data. Health-monitoring products provide real-time feedback about nutrition, fitness, pulse, blood pressure, and other vital signs. All of the collected data must be secured. Finally, Internet of Things brings automation as a part of digitalisation, powered by artificial intelligence, consequently system can make mistakes, followed by wrong injections or wrong pills recommendations, what can affect the patient's condition or even kill him.

3.4.1. Smart healthcare security concerns

Society's desire and technological ability to use networking technologies always exceed their ability to control the security of that technologies. Networked medical devices are not an exclusion. They provide huge benefits for the modern healthcare system, so developers and adopters close their eyes and try not to notice serious security gaps in new products. The situation will remain the same or get worse if security officials and device makers do not take

the required steps now. It could happen that a huge boom of medical zero-day exploits and security holes without defense will arrive on the market. So, there are four main and close areas of healthcare Internet of Things concern (Harries, 2014):

- Accidental failures
- Protecting patient's privacy
- Intentional disrupt
- Widespread disrupt

Accidental failures are the most evident problem, which decreases the general trust of users, because if any great failure happens, society will refuse networked medical devices, delaying the evolution of healthcare and medicine for years. People can trust doctors, but it is always hard to trust the machine if there were some mechanical or software error, led to some irreversible consequence. Networked medical devices are vulnerable to more than just criminal intent. Like any other mechanical, digital device or technology they can break down completely or proper behavior can be changed. It is not a result of improper engineering or bad parts; it is a result of manufacturing defects, software mistakes or other circumstance affected by millions of conditions. The complexity of devices and operational technology which controls physical processes, such as pumps, creates exponential opportunities for flaws in design, implementation, or operation, any of which can lead to dramatic accidental failure. The probability of failure must be tiny (it could not be real 0 in practice and even in theory) when it comes to medical devices compared to other networked technologies.

Protecting patient privacy is the next issue to be worried about. According to PricewaterhouseCoopers (PwC) Global State of Information Security survey 2015, the number of security rifts reported by healthcare providers dramatically increased by 60% from 2013 to 2014, what is almost twice bigger risk growth, comparing to other industries and systems, consequently another crucial point and second concern is protecting the personal and private patient data, as it is considered to be the most valuable information for hackers and further intimidation, for example (PwC, 2014). Vulnerabilities in the networked medical devices produce huge troubles for owners of these appliances, since they monitor, access and store patients' most personal information – biological and medical data. To fulfill Internet of Things paradigm all of the devices must have wireless communication module to be able to transfer data at any time and from everywhere, so the capability of wireless networking is one of the main strengths of smart healthcare for achieving high efficiency. From the other hand, as with any wireless solutions, user want to be sure there is no transmission of unencrypted personal

data, or that there are no backdoors to the device from the network. Additionally, some smart devices are capable not only of health monitoring but also on billing (making online financial operations), used as a separate feature or as an extension for medical purposes (e.g. as a part of healthcare provider policy or for ease of operations). Vulnerabilities in such solutions put patients at risk of losing both medical and banking information; both types are most private ones. Since medical IoT is still in its inception, no one knows the ways information could be used by criminals (e.g. biological logs could be changed to prevent some person from getting some job, gamblers can steal data of professional athletes for perfect bids, criminals can change parameters and kill people with pacemakers or insulin pumps), however there is a strong understanding that it must be secured to avoid data interception or loss.

Intentional disrupt is another concern. Racketeers, terrorists and other criminals seek to exploit as many vulnerabilities in whole IT infrastructure as possible to commit crimes and cause chaotic situations. When it touches banks or transport systems, the consequences are manageable by the government, however, when a device is on a human or even under his skin, the consequences of the cyber crime committed using that device might be particularly personal and threatening. A pacemaker is a good example. It is possible for criminals to connect to it and to kill the person. Same could happen with insulin pumps or any medicine-delivering systems. Today there are already few cases reported by The US Department of Homeland Security. Widespread disruption is quite a doubtful risk, but as medical devices are connected to the global network, some targeted malware could spread across the Internet and act against only selected medical devices, so everyone with the vulnerable device is affected. This is quite a doubtful scenario; however, it still should be considered.

Even though telemedicine represents many risks almost half of respondents polled by PwC had integrated medical devices into their enterprise information systems, however, they had not ensured the security and safety of these smart devices in needed manner. 37% said that they contacted manufacturers or looked through manuals to understand security capabilities of medical devices and possible risks for users, only 59% of previous 37% performed some risk assessment of the solution. 56% of this 59% implemented some extra security controls, what is a tiny amount of all respondents, what confirms that people want to use new appliances much more than to assure that they are secure. (Lee, 2014)

To sum up everything, I would like to demonstrate an example situation, which shows the lack of security in insulin pumps, which are the most used monitoring/automation smart health

solutions after usual monitoring wearables. Two analysts, Jay Radcliffe and Barnaby Jack, have analyzed insulin pumps. In 2011, Radcliffe discovered that knowing of insulin pump's serial number would allow connecting to it from 100-150 feet. As these devices have almost no security today, an attacker could turn off the pump or cause an insulin overdose with cheap and ordinary electronic equipment. Following, Jack found a way to compromise an insulin pump even without the serial number from 300 feet. This would let a hacker scan for any nearby devices instead of having to target a specific device identified beforehand. (Finkle, 2014)

3.4.2. Risk sources, recommendations for regulations and security

Sources of security risks in smart healthcare devices are quite general, as a set of technologies is the same for every modern technological solution. However, medical devices are regulated strongly, consequently, it produces a new range of risks because of improper regulating approach.

The software and firmware used in medical devices is a diverse and completely inconsistent mix of different standards, their versions and methods of connecting everything together. The reason for this is the market hustle and bustle and improper control, geared by new operating area, where pioneering may build a good reputation for company, manufacturer's preferences and patient's needs. All in all, no one even tried to the standard operating environment, architectures, communications methods, and other backends. Nowadays, Continua Alliance is trying to work on widely accepted standards and recommendations for building smart medical devices, but even them cover mainly personal solutions, not hospital-wide ones. Mainly, the size of the device is critical for technology and standard selection, what makes more difficulties, as small devices are special ones, tended to perform an exact monitoring or automation. Moreover, as for embedded to body solutions battery life is a big point, so, for instance, pacemakers operate with custom processing units and custom operating systems, what puts security nearly away, as device makers can not work on one product for a long time, investing huge money. To my opinion, it is quite surprising, because people would prefer highly secured device, which is even more expensive, instead of the cheap working solution with poor security capabilities. Probably it happens because of lack of technical understanding, or maybe it is just a paradox of modern market with typical business needs of saving resources, time, reducing costs and simplifying processes.

As smart healthcare devices must be connected to the inner world, the communication technologies used are a bit more standard than the other components of devices, because of

existing communication protocols and technologies with regulations. For example, some home-based stationary devices may be connected by WiFi, while pacemakers or insulin pumps or any other wearables are more likely to use a shorter-range technology such as Bluetooth Smart. Using an existing known standard of communication still is not an ultimate solution, because of the nature of personal healthcare devices, their behavior and operating power. Whereas a local hospital network with stationary devices has some defined boundaries and permanent, stable needs, network professionals may monitor and update the security in a quite easy way, starting from simple ACLs and traffic blocking to some advanced measures and continual hardware and firmware updates. For smart medical devices, like wearables, the situation is different - there is the challenge of fixing vulnerabilities after they are discovered. If for example, a device has been surgically implanted, patching the software or firmware is not always possible, while changing hardware requires a risky operation. Moreover, updating normal networked devices requires no regulations, when some manufacturers avoid changes, even security updates, as re-approval of audit agency is required. Patching medical devices remains costly and hindering, as device makers must prove that the patched device still meets all medical claims. So, less patching is performed for medical devices, compared to other IT systems.

To conclude the source of risks analysis, access control management is a big dilemma for device makers, as most personal data is accessed by the device, consequently, healthcare appliance needs to be highly secured and protected from criminal access and meddling, but still open enough for medical personnel. This question is very hot especially for automation systems and devices for monitoring chronic conditions. Different manufacturers have different approaches to find the perfect balance in the security and accessibility for allowed personnel. Some companies just restrict all types of access, except for owner's one. In this case, all credentials are stored somewhere, and patients prefer to keep them close in case of an emergency situation so that doctors can easily access the device. The main drawback here is that criminals are also able to get hold of access. Other manufacturers increase the emphasis on security by avoiding such hard-coded credentials, but they risk to keep out allowed medical personnel during an extreme situation.

As with any security challenges of new technologies, open collaboration and communication are key factors needed to manage and reduce risks. This includes collaboration and communication among regulators, as well as between regulators, industry, and medical and

healthcare specialists, providers, consumers. Here are the recommendations to continue innovation in telemedicine with minimization of security risks:

1. The first requirement for medical device manufacturers is to build a good smart solution is the **“secure-by-design” approach** to research and development. It means that security must be number one issue while designing and building the product. It should not be added afterward, as it was in the past, what caused different challenges. For instance, security experts have had to deal with the reckless shortcuts developers had taken to try to assemble security in after product development. Adding security features to the product after initial engineering is a losing deal because it is completely ineffective to try to secure systems, which are already in use.

According to Stuart McClure, worldwide technology officer: *“Cybersecurity has to be baked into the equipment, systems, and networks at the very start of the design process.”* To put security right in the design process a lot of investments are needed, both financial and resources. However, medical device makers will benefit in the future from prioritizing security in its approach to product design today. (Harries, 2014)

To maximize the advantages of smart networked medical appliances, a careful balance between the control of security and the flexibility essential for practitioners and patients is required. Sometimes, flexibility and adoption in the field of medicine breed security vulnerabilities, as device and healthcare providers, who are adopters, change configurations or security features or combine technologies. A secure-by-design approach might include the ease of approaches such as automated logging and monitoring of device modifications in the field, to identify vulnerabilities and better manage them.

The partnership of national governments and device makers (and other members of medical industry) might make this secure-by-design approach easier by providing initial funding for an open-source, common-language software library and APIs for medical devices. Today the majority of device manufacturers write their own code, which is customized to some exact company or project. As developers are not security specialists this code optimization is more likely to be inefficient in other projects and also ready products may communicate not so good with other appliances, what undermine Internet of Things paradigm. Such small software operations also tend to make it difficult to find

and patch existing bugs and vulnerabilities.

The correlation described in the previous paragraph could be a great opportunity for aligning innovation from companies, privacy and security rules from government and specialists in the area. It would reduce the costs for device makers, and consequently accelerate the innovation, all while allowing for better security. As one company or organization finds a security threat or bug, the fixes would be available to the entire community and industry.

It is important to mention that even the best secure-by-design products will still have some bugs and vulnerabilities. Therefore, the solution for it is in cooperation of the medical device industry with computer security researchers. It will create public awareness around IT security in telemedicine and affect public safety and trust in networked medical devices. Also, a good step is using the results of enthusiasts' tests. Too often companies do not rely on such hackers, although, most of them are driven by curiosity and public-mindedness. On the other hand, some companies have already applied such methods and "bug-bounty" programs offer financial rewards to enthusiasts who provide low-cost security testing for the software and firmware of medical devices. If this program would be co-funded by the government with industry-wide scope, it would dramatically improve security with minimal costs.

A new approach for risk management is needed, and it begins in cooperation between the manufacturers and developers of the device and its software. All device makers should work together and in tight contact with regulators, as stated above, to develop a comprehensive risk management model to apply during innovation, design, manufacturing, delivery and support processes. A new model should present Internet of Things medical appliances as a platform, but not a single device. That approach would create industry coalitions to consider the security of technologies. The main goal of the described model is to make devices as a platform, which could be supplemented with other technologies and services. The logical question is why is it not effective to apply existing highly-developed risk models which were created for PC and other systems security? The answer is the big difference of healthcare industry from others, the distinction in credential management, access control and updating. However, the existing models for cybersecurity risk management can be a launching point.

2. **Improving public-public and public-private collaboration** is another issue. Healthcare and telemedicine are overcrowded with different regulations which do not suit the real needs of digital age medicine evolution. Adding more regulations will only worsen the situation, and more coordination is important. The truth is that regulators are not so fast with technological innovation. To deal with rapid changes, regulators require feedback from everyone involved through transparent, collaborative forums which ensure the regulators' independent function.

The process of improving security demands a place to talk about these issues, providing clearness on the regulatory point of view, reaching agreement on how to enable innovation and manufacturing a safe product of the public interest. Manufacturers should also continue improving communications among themselves. For example, the Industrial Internet Consortium (IIC), formed by Intel, IBM, Cisco, AT&T, and Microsoft, is an example of how industry collaboration can help unlock business value while also improving security.

The EU might consider such models for adopting new regulations. Current EU procedures for smart medical device approval are quite short and outdated. The European Parliament is considering new regulations that would promote safety as well as innovation. However, some manufacturers worry that such rules would create unnecessary layers of bureaucracy and delay patient access to innovative products, which is the number one issue to be avoided. Figure 16 shows infographics about regulatory spectrum for smart medical solutions and following there is an overview of regulatory bodies of different countries:

- a. European Union – a slate of proposed regulations are currently being considered by the European Parliament, and the EU put out newly revisited guidance on software as a medical device in late 2014. Look for something definitive in the short term, which will likely push off more aggressive investment into the European eHealth space. (Valsamidou, 2014)
- b. United States – the FDA's latest regulatory guidance is non-binding and eHealth in the US is quite a big business, nowadays, wearables and monitoring devices of all sort are in focus, what represents a small part of the potential market. (U.S. Food and Drug Administration, 2016)
- c. Russia – government currently pursues its own product testing on all medical devices, and does not recognize foreign CE markings, FDA 510(k) clearance or

other national approvals. Russian medical device registration process continues to be mired in an opaque bureaucracy, and major overhauls to the regulatory framework of networked medical devices are only in plans now. (Valsamidou, 2014)

- d. United Kingdom – recently the Medicines and Healthcare Products Regulatory Agency made clear that software with explicit medical purpose and devices that meet the requirements of Medical Device Directive will be regulated as devices and will have to undergo a conformity assessment. (Valsamidou, 2014)
- e. Japan – connected medical devices will now be treated under the same regulatory regime as other medical devices. Japan is one of the leading countries for normal and smart medical devices, consequently, norms in Japan are in the huge interest of international regulatory bodies. (Valsamidou, 2014)
- f. China – despite a major overhaul of Chinese medical device regulation in 2014, the government did not address networked medical devices. Nowadays, China remains a relatively small player in the eHealth space, but growth could be explosive over the medium-term. However, government policies that favor domestic device manufacturers over foreign competitors could limit investor appetite. (Valsamidou, 2014)
- g. Brazil – in 2014 the National Health Surveillance Agency failed to move forward with new regulatory requirements for smart healthcare devices and software. Analysts predict that demand for networked medical devices will only grow Brazil’s position as the largest market in Latin America. (U.S. Food and Drug Administration, 2016)
- h. Australia – since 2011 there were no noticeable changes to the Australian Regulatory Guidelines for medical devices, leaving a hole in the rules regarding smart medical devices. Australia is trying to follow USA or EU norms now. (U.S. Food and Drug Administration, 2016)

Personal medical devices stream data to cloud resources and join the owner, while traveling, so different jurisdictions, and privacy regulations apply in different countries. This means that international regulators have to consider the transnational nature of data. Standards must be coordinated worldwide so that they vary only slightly from country to country. It would cut the costs and scale security.

3. The **current regulatory methods and the whole paradigm should be changed** to encourage innovation in the field, while still meeting security needs and public needs.

The majority of regulations give the officials only a brief look at the new medical device before it goes directly to consumers. The good method here is to compare new solutions with existing ones and to determine the risks and benefits of treating the identical problems. There is a need to classify the proposed product and review its risks and advantages for society. Such processes already exist. For example, FDA's 510(k) process, European Dutch agencies and international alliance Continua, which was previously presented (Gang, 2011). All regulations must be modern and meet current technologies, as some device makers use old technologies because they are sure that they will get officials' approval. It stifles the innovation dramatically, which next decreases the security and collects vulnerabilities. One possible solution here is a streamlined approval process, suggested by McAfee.

Software security for non-medical devices is a well-known field, so security experts already know the vulnerabilities of general commercial software, which allows a solid background for medical devices, where the same or similar vulnerabilities exist. The regulatory process should encourage security by design as well as the ability to patch systems after they are deployed. Consequently, the regulation process must be strict and flexible for device makers at the same time.

4. It is required that a proposed model offers a **voice to the public**, especially patients and other users involved in the process. In most countries, governments and private companies do not count the public's interest in medical questions. It affects the quality of service dramatically by non-researched approaches to usability, effectiveness, and security.

Regulators have already recognized the value of public input, especially from patients. This approach should be industry-wide and offer specific guidance on how feedback from patients, or the broader public, should be collected and presented into the regulatory process.

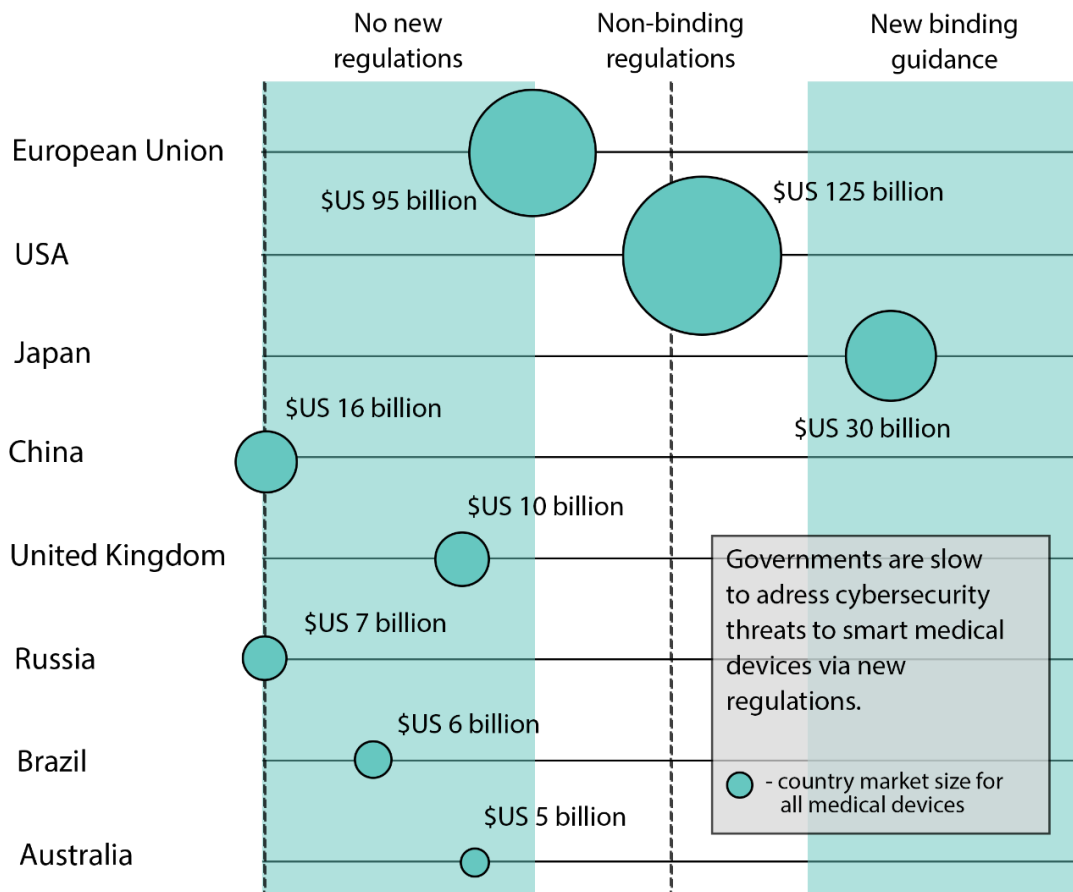


FIGURE 16. Regulatory spectrum for networked medical devices

To sum up, it is clear that connected medical devices introduce security flaws along advantages described many times already. All of the possible security issues could be managed with some critical steps, where security must be in focus from the first design sketches. All innovations in medicine are risky, health and medical specialists should drive the balance between patients experience and security. Now it is crucial to understand the core of medical devices failures and share it with everyone involved in the industry. As open standards should be used for devices to provide connectivity, “open” security methods should be used to improve general situation.

4. STUDY OUTCOMES AND RESULTS

This section is about the results of the study, lessons learned, the analysis and the whitepaper, which is an attachment itself, see Appendix 5. Attached whitepaper is the main place for results and guidelines. I will also briefly summarize the work below.

The study showed that healthcare sector is seeking for Internet of Things, as none of other social areas. It gives a huge variety of applications for modern technologies. Personal healthcare was named number one focus for businesses after research. Analyzing markets, audience and personal smart healthcare I came up with following key statements:

- Only narrow groups of users are covered now. Devices should be produced for everyone, for people who can use them daily.
- Everyone is looking for a secure and efficient solution. The system should be simple to use and automatized.
- Users are not able to pay a lot of money, however, tight collaboration in the industry could cut the costs dramatically.
- Security and privacy are number one concerns. The security-by-design approach is recommended for device makers.
- Regulations are different, depending on the country. Companies should collaborate with government to make the regulatory process more efficient.
- Developers must use open standards in order to meet the idea of interconnectivity.
- It is not possible to work alone on healthcare IoT market, as it is about ecosystems. Communication is the key.

Today, eHealth sector is developing quite rapidly and it is a good chance for businesses because there is no big concurrency on market still. Developing a proper product may attract many consumers and afterward it could be developed and connected to other systems, making first inclinations to real Internet of Things. Working with standards will open even more doors for companies, as their currently proprietary standards could be used in the whole industry, making the owner a true market leader. All in all, IoT is about innovations and it is worth investing, especially in the personal healthcare sector. Read section 5. “Designing a smart healthcare device” to see how guidelines and the whole study could be applied to the real project.

5. DESIGNING A SMART HEALTHCARE DEVICE

In this part, I will show the design of a real smart healthcare device based on my study's results. I will focus on chronically ill people with type 1 diabetes and develop an insulin pump, which works with the CGM (continuous glucose monitor) system and mobile application, used to predict doses for injections, patient-doctor communication, bracelet control and condition tracking. The core idea of this part is to show how to design and develop a smart healthcare IoT device, meeting the real needs of market and consumers in the target audience. Moreover, I started the work on this project with a team in May 2016, consequently, it could be seen as the main motivator for the whole thesis.

5.1. Introduction and motivation

The initial idea was born some time ago when the understanding of medical automation, healthcare IoT and general engineering skills were poor. However, the need for such an appliance was already clear for us and our desire was increasing dramatically. First of all, I want to show why insulin pump is a good and really demanding product. If you revisit the section 3.3. "Exploring new audience", it will be clear that people with diabetes are not covered by existing businesses, as they are also in the information seekers group. Additionally, they require something more than just data tracking and statistics. It is automation capability. Moreover, according to audience study, it is seen that people are ready for smart appliances and they can trust technologies, but the questions of privacy, price, security and technical reliability are relevant. All in all, the task was to develop innovational, a reliable device with high-security focus, permanent consumer support and high interconnection capability for future healthcare IoT. That means that our main challenges were to use open standards, apply security-by-design approach and to develop an initial ecosystem.

The next thing to explain is why we have chosen an insulin pump. There is no personal background motivation for it. Analyzing the medical market, I found out that any types of insulin injectors are popular, as 387 million people worldwide are living with this disease. 56 million of people in the European region, 61 million in Americas (37 million for the North America region) and 138 million in Western Pacific are injecting insulin several times per day. If we count that an average person with diabetes injects insulin 4 times per day, the number of all daily injections will be over 1B only in the highlighted regions. In practice, the number of diabetics is much bigger and 46% out of the whole amount is undiagnosed, making the total amount almost twice bigger. Statistics is very surprising and specialists predict 205M of people expected increase until 2035. (American Diabetes Advocates (ADA), 2014) Such big audience

intends a huge variety of existing and developed devices, however, this is not true. All present devices could be divided into two big groups:

- Devices developed by leading medical companies
- Smart solutions created by enthusiasts and startups

Solutions from the first group lack intelligence and mostly were modern 5-7 years ago. They can measure sugar levels and inject a proper dose of insulin based on human calculations and some static algorithms. All of them are cumbersome and difficult to keep running. The second group is more interesting as there is some intelligence in systems, however, most of them require a special proprietary control device, which is not effective as everyone owns a smartphone (100% of respondents of my audience study) with powerful calculation and communication capabilities. As an example of such devices, I can present two solutions by Kaleido (Kaleido, 2016) and Medtronic (Medtronic, 2016) for second and first groups, respectively. Also, see Figure 17 for put on body devices.



FIGURE 17. Kaleido (left) and Medtronic (right) devices on body

After competitors' research and market study, the list of problems to solve and challenges is clear:

- Avoid using extra devices and use a smartphone.
- Make a comfortable device.
- Create one device that fits all components.
- Think about the future ecosystem and focus on developing a connectable device.
- Make a modern and good-looking device.
- Use open standards.
- Make an application useful and able to provide data insights.
- Develop an intuitive application and intuitive device controls.
- Focus on security.
- Focus on targeted audience.

Of course, this list is not full, but these aspects are crucial.

After initial research and development, the idea of the bracelet was born. It fulfills the medical prescriptions (shoulder is a good place for insulin injection) and requirements of proper smart healthcare wearable. In following chapters I will discuss features, technical details, and model of the bracelet itself.

5.2. Diabetes

In the introduction, I said bracelet is targeted for people with type 1 diabetes. In this chapter, I would like to explain the disease, differences between types and origin of the problem. Understanding of these questions helped me to develop a device, as understanding diabetes allowed me to understand how, what, why and when to inject.

Diabetes (diabetes mellitus) is an endocrine disease, which is characterized by a chronic blood sugar (glucose) levels increase due to absolute or relative insulin deficiency. Insulin is a pancreatic hormone. The disease leads to disruption of all types of metabolism, vascular, nervous system and other organs damages. There are several types of diabetes:

- Type 1. Insulin-dependent diabetes.
- Type 2. Insulin-non-dependent diabetes.
- Secondary diabetes. Also named symptomatic.
- Gestational diabetes.
- Diabetes caused by malnutrition.

Type 1 and type 2 diabetes are most popular ones. The main reason for type 1 diabetes is an autoimmune process caused by the failure of the immune system. Body starts to produce antibodies against pancreatic cells to destroy them. The main factors that provoke the emergence of type 1 diabetes is a viral infection or the genetic susceptibility to the disease. Type 2 diabetes could be a result of lifestyle, obesity and so on. Whatever the cause of diabetes is, the consequence is following: the body can not use all glucose (sugar) from food and stores the rest in the liver and muscles. Unused glucose is circulated in excess in the blood. It affects all organs and tissues. Since the glucose uptake in cells is insufficient, organism begins to use fats as an energy source. As a result, increased quantities of toxic to the body and especially the brain substances (ketone bodies) are generated, affecting the whole metabolism process. Typically, type 1 diabetes (insulin-dependent) develops rapidly, sometimes suddenly. Insulin-non-dependent diabetes develops gradually and is characterized by moderate symptoms. (Fadeev, 2009)

Treatment of diabetes is held for life. Daily use of insulin is necessary only for patients with diabetes of the type 1 diabetes and in the case of the progression of diabetes of the second type. When type 2 diabetes becomes also insulin-dependent, it could be considered to be type 1. That's why Insula is targeted to type 1 diabetics. As stated before, insulin is a hormone of human pancreas, which reduces and regulates the level of blood glucose. There are different types of insulin to be injected:

- high-speed (simple) insulin
- short-acting insulin
- intermediate-acting duration insulin
- insulin of prolonged or long activity
- combined (mixed)

All insulin pumps are responsible for delivering basal insulin and injecting insulin in case of an emergency situation or increased glucose levels. Basal insulin's primary job is to keep blood glucose levels in check during periods of fasting, including sleeping. While fasting, the liver continuously secretes glucose into the bloodstream, and basal insulin is needed to keep these glucose levels under control. Basal insulin could be intermediate-acting or long-acting. Many people with diabetes like basal insulin because it puts them in control of monitoring their glucose levels and allows them to have a more flexible lifestyle. However, sugar levels must be checked constantly, as they are changing dramatically because of different conditions, diet and mood. That is why CGM is the second relevant part (after pump itself) of a good smart insulin pump.

Now, when it's clear what insulin is, following factors could be added to Insula requirements:

- The cartridge must contain few daily doses of insulin
- The cartridge should be filled by patient based on selected by doctor type of insulin

The next logical question is the needle. Insulin is inserted under the skin, consequently, the needle should be 4-6mm at 90 degrees level. Other medical peculiarities and mechanisms would be described later.

5.3. Bracelet design and technologies

According to market and disease studies, I was able to develop a smart bracelet for automation, see Figure 18. In this chapter and sub-chapters, I will explain the technical aspects and solutions applied, as well as the materials used, modules, etc. Moreover, I will show the model made in Solidworks in detail.



FIGURE 18. Insula bracelet Solidworks model

Nowadays, the bracelet is targeted for all adults. It is designed to carry 300 IU of insulin. IU is an International Unit of measurement for the amount of a substance in pharmacology. It would be enough for 10-15 days for average diabetics. However, the bracelet could not be worn for the whole period, as it is restricted due to the injection needle and CGM sensor (which is also a needle). Needles could be inside the body for several days. If the bracelet is removed from the shoulder, the needles should be changed to new ones.

5.3.1. Model and features

The bracelet is a flexible unibody object. It is made of soft-touch plastic. The stripes which touch the body are changeable and are made of bactericidal silicone. Between them, there is a rechargeable insulin cartridge, which is connected to the needle and operating module, where the pump is located. The same box holds the CGM module. Depending on the sizes of the

custom-made logic module, the BLE module and used CGM appliance, battery, and wireless charger could be put to the same metal box or a new one (there is some extra space left in case of redesign and new features). The button is used to control the bracelet mechanically in case of smartphone discharge. It is possible to deliver a minimal dose of insulin by putting the bracelet in the special mode. By inserting several doses, normal levels could be achieved. Specific button presses combinations are used to control Insula in the mechanical mode. The button is surrounded by LED tape used for intuitive feedback. See Figure 19 and Figure 20 for model views. See Appendix 3 for Insula bracelet infographic.



FIGURE 19. Insula bracelet view from top



FIGURE 20. Insula bracelet strap

5.3.2. Mechanisms

The bracelet consists of different mechanical and electronic parts and in this chapter I want to explain the following things:

- Insulin delivery mechanism
- CGM module mechanism
- Clasp mechanism
- Needle injection mechanism
- Button

Charging and bracelet-smartphone communication principles will be discussed in the Section 5.3.3. “Control and communication”.

The first mechanism to be explained is the insulin delivery mechanism. The flexible tube is connected to pump. On the other side, there is a one-way valve. The pump forces the needed amount of pressure to the tube, which makes the piston to move, pushing the insulin to the body through the needle. One-way valve allows air to substitute the liquid insulin in the tube, normalizing the pressure. After all the insulin is used, the tube could be changed to new one, or just new insulin could be injected inside, by removing the tube and pushing the piston to start position with insulin from the other side. Air will go out through the same one-way valve, making sure that insulin stays inside and no air would be injected into the body.

The clasp mechanism is very simple. The strap has “tooth”. It is put to the clasp hole, where a special plate flips and allows “tooth” only to go inside, which allows the user to tight the bracelet as much as needed. To let loose the clasp, bracelet should be pushed quite hard near clasp hole, which will release the plate. Such mechanism has some benefits. There is no need to manufacture bracelets of different sizes. It is durable and water resistant. It is a nice point to mention that the whole bracelet is waterproofed and it could be washed easily.

The button was described a bit so far. It is a round element, made of stainless steel with logo etching. As Insula is worn on the shoulder, the button must be secured from occasional pushes. It is done so that it should be pressed hard and long enough to transfer the bracelet to mechanical control mode. Moreover, it could be locked from the application. In the case of phone discharge, it is unlocked automatically with LED notification and vibration (this module is not designed yet).

The CGM module is one of the most difficult ones to implement. The sensor is inserted under the skin, where it remains for several days, detecting glucose in the surrounding fluid. The sensor uses the same enzymes to measure glucose levels as a test strip: glucose oxidase. These enzymes convert glucose to hydrogen peroxide. The peroxide reacts with a platinum plate inside the sensor, generating an electrical signal. A smartphone converts the electrical signal data into a glucose reading based on existing algorithms. These basic features are shared by all CGM sensors. The chemical layers on top of the glucose oxidase keep the sensors functional under the very poor working conditions that exist inside the body. (Erika Gebel Berg, 2014) There are several manufacturers of CGM modules and it is more cost-effective to use them, instead of designing and manufacturing proprietary ones. The module of needed size could be purchased and placed on the existing components infrastructure.

The needle injection mechanism is the last thing to be explained in this chapter. Now the automated mechanism is showed on the model. The automatic needle insertion is done by a ball screw. Such type of solution requires the bracelet to be around 1.2 cm thick to allocate the needed elements. Also, the CGM needle uses same mechanics. The main drawbacks of such solution are precision and price. It must be tested practically, not only theoretically. It requires full bracelet manufacturing, which is still too early. Another solution is manual needle insertion. In this case, needles are shipped on a special magnet platform, which connects them to bracelet side mechanisms. All in all, the question of needle insertion is still opened and it is a big engineering challenge, which requires professional work and could not be done by me and other team members.

5.3.3. Control and communication

To be a smart device Insula must be connected to the mobile application, which requires some communication protocol. Also, the bracelet must be charged somehow. Open standards must be used for both processes, as in the future Insula must become a smart device in big healthcare IoT infrastructure. According to Continua guidelines for healthcare device making (Continua Alliance, 2016), Qi and BLE should be used.

Qi is the only globally accepted wireless charging standard. It was created by Wireless Power Consortium, which consists of more than 100 different companies. The Qi standard is designed for the transmission of energy to various devices using magnetic induction. Technically it is very similar to the solution that is used to charge electric toothbrushes.

In simple words, the base station includes an induction coil which produces an electromagnetic field when AC flows. The charging device has a coil, able to catch the field, converting the resulting energy into direct current used to charge the battery. If we look at the process in more detail, the transmitter (charger) consists of a current transformer (ac-dc power converter), the transmitting coil, voltage and current sensors and controller. The receiver contains a receiving coil, a rectifier, a voltage regulator and a controller. The energy is transferred from the transmitter to the receiver via a related magnetic field generated in the flow of alternating current for the transmitter coil. If the receiver coil is in close proximity, a significant portion of the transmitter power lines passes through the receiver coil, creating an alternating current in the receiver, which then already was converted into a DC voltage.

The Qi standard supports data transfer protocol between the charger and charging the device at a rate of 2 kbit/s. With regard to the security of wireless chargers, I can say that non-ionizing frequency is used not to cause adverse physiological effects. The Qi standard includes the detection of foreign objects in the field of action of the charger, providing added security feature. Charging is only possible with Qi-compatible devices. Also, chargers and charging devices have built-in safety mechanisms based on the thermal control. All highlighted features of Qi wireless charging technology make the protocol completely suitable for smart healthcare solution.

BLE is the recommended protocol for wearable-smartphone communication. To address the limitations of wearables, the Bluetooth Special Interest Group (SIG) has introduced Bluetooth Low Energy (BLE) specifically designed to achieve the lowest possible power for short-range communication. Just like Bluetooth classic, BLE continues to operate in 2.4GHz ISM band with a bandwidth of 1Mbps, however, it consumes much less power. The protocol is optimized to burst transmit small blocks of data at regular intervals, thus enabling the host processor to maximize the amount of time it can operate in a low power mode when information is not being transmitted. Moreover, Easy BLE Smart Ready host is available in modern smartphones, making adoption easier.

At this point, I would like to finish the technical overview of the project, as the scope of my study is focused not on hardware or software, but on finding guidelines and approaches for entering the healthcare IoT market, while the bracelet design could be considered as a separate topic for a thesis paper.

5.4. Application design

The mobile application is used to control the insulin bracelet. It gets data from CGM permanently and analyses the information to predict doses and critical picks, based on current blood indexes and nutrition. Moreover, it provides statistics and insights. Also, it is capable of contacting the personal doctor and community. All in all, the application is the management unit of the whole appliance. See Appendix 4 for application mockups.

The app design was one of the biggest issues to solve. According to my studies, any smart healthcare application should be easy and intuitive. I decided to remove all controls which are unnecessary for glucose level tracking. Using IBM Watson Alchemy and Google Nutrition API allows users to specify what they are eating in plain text (Michelle, 2011). It makes application smarter and even simpler.

5.5. Business aspects

The business constituent is very import for Insula project now. Finding appropriate partners in eHealth sector and manufacturing is crucial. At this point, it is quite hard to state the exact amount of investments needed and the exact price of the bracelet with the whole system. However, I have some aim estimations. As the appliance targeted for anyone with diabetes, it should be affordable. Choosing such strategy for price building would also attract more consumers, as clear benefits of smart device and good price remove all existing product from market leading positions. For now, the price of bracelet manufacturing and materials is around 20-30 euros, but the custom chip is needed, development of which could increase the prices. The whole Insula ecosystem must be 80-120 euros for consumers. This price would allow receiving profit while supporting consumer range and growing.

Business planning, brand and strategic managements, localization issues and crowdfunding approaches are important parts of every startup lifecycle, however, those topics are out of the scope and the purpose of this chapter is to highlight biggest and foundational aspects. I think that mission of Insula could describe the business approach quite good. So, our mission is to provide secure and personal health service for everyone with diabetes, making the life of the patient easier with innovation and technologies, working out of the box.

5.6. Conclusions and future work

To conclude the introduction to my project, I would like to say that it is just the beginning and more specific steps are coming. Plans are big, but the bracelet and app prototypes must be real, what is planned to be done in few months. Here is the list of nearest future work and issues to be revisited for Insula appearing on the market:

- Finishing the design of all mechanisms
- Consider following bracelet improvements:
 - Adding extra tube with another type of insulin
 - Adding a small tube with glucose in case of insulin overdose
 - Adding vibrating module
- Custom chip creation
- First prototype
- iOS application development
- Android application design and development
- BLE configuration
- Finding appropriate factories for manufacturing
- Finding partners for creating the ecosystem (tight collaboration with hospitals and healthcare providers)
- Finding pilot consumers
- Crowdfunding or direct investments
- Certification and testing

6. CONCLUSION

Healthcare and medicine are very important social sectors and the need for technological support there is increasing permanently as tools and treatment techniques are becoming more advanced. Modern telecommunications and machine learning open new paths for diagnostic process and treatment procedures. Internet of Things offers the concept of the interconnected world, where medical services are supported by every aspect of being, from nutrition to transportation. All in all, the benefits of smart services in personal healthcare observed through the study are overcoming all drawbacks. However, security and privacy, user experience and adoption are huge points to be studied and improved.

This study that now concludes has focused on personal healthcare Internet of Things, which provides the user with digital medical and wellbeing services or application. It is the biggest part of the whole medical sector, as a number of healthy people is bigger and it is important to catch their attention and focus it on health before serious troubles when medicine starts.

Hopefully, my study outcomes are useful for all sorts of businesses, but it is nice to understand that there is no gold standard for making businesses, even in the healthcare field, where many regulations are applied. The purpose of my work is to provide insights of the smart healthcare sector and to provide key findings for IT people who are not able to use technologies for developing a proper product, and for business specialists who can not correlate the possibilities of modern technologies to the needs of consumers. My report should close the gap between two tightly connected groups of people, providing understanding on the whole field and requirements for new products.

This is, of course, only a very preliminary proposal that has helped me to develop my knowledge in different ways:

- It has allowed me to enter a field of research that was completely unknown to me before, which is telemedicine, with its technological and medical foundations.
- It has allowed me to have a first look on how research is carried out in this area.
- It has familiarized me with some aspects of medicine.
- It has shown me the path for the use of business studies for technological projects.

To conclude, I would like to say that of course there are a lot of ways in which my study could be extended:

- Medical IoT could be explored and its correlation to healthcare could be researched.

- Different and more complex studies could be performed for focused areas, like security or adoption of smart healthcare devices.
- Alternative example products could be developed.

BIBLIOGRAPHY

(PwC), F. W., 2014. *Making Care Mobile: Introducing the apps pharmacy*, s.l.: s.n.

American Diabetes Advocates (ADA), 2014. *Global Diabetes Population*. [Online]

Available at: <http://www.americandiabetesadvocates.org/>

[Accessed November 2016].

Christina, F., 2014. *Exclusive: Two Apple medical trials shed light on how HealthKit will work*, s.l.: Reuters.

Cisco, 2016. *Internet of Things*. [Online]

Available at: <http://www.cisco.com/c/en/us/solutions/internet-of-things/overview.html>

[Accessed September 2016].

Compton, M. & Mickelberg, K., 2014. *Connecting Cybersecurity with the Internet of Things*, s.l.: PwC.

Continua Alliance, 2016. *H.810 Interoperability design guidelines for personal connected health systems*, s.l.: s.n.

Erika Gebel Berg, P., 2014. Anatomy of a CGM Sensor. *Diabetes forecast*.

European Heart Rhythm Association, 2014. *Statistics on the use of cardiac electronic devices and electrophysiological procedures in the European Society of Cardiology countries*, s.l.: s.n.

Evans, P. C. & Annunziata, M., 2012. *Industrial Internet, Pushing the Boundary of Mind and Machines*, s.l.: s.n.

Fadeev, P., 2009. *Diabetes*. Moscow: Oniks.

Finkle, J., 2014. *U.S. Government Probes Medical Devices for Possible Cyber Flaws*, s.l.: Reuters.

Fox, S., 2010. *Mobile Health 2010*, s.l.: s.n.

Gang, G., 2011. *Internet of Things Security Analysis, International Conference on Internet Technology and Applications*. s.l., s.n.

Google Trends, 2016. *IoT search term*. [Online]

Available at:

<https://www.google.com/trends/explore?date=all&q=%22internet%20of%20things%22&hl=en-US>

[Accessed September 2016].

Harries, P., 2014. *The Prognosis for Healthcare Payers and Providers: Rising Cybersecurity Risks and Costs*, s.l.: PwC.

Higgs, R., 2014. What is telemedicine?. *ICUcare LLC*.

IBM, 2015. *Watson for a Smarter Planet: Healthcare*. [Online]

Available at: <http://www-03.ibm.com/innovation/us/watson/>

[Accessed November 2016].

IDC, 2014. *U.S. Wearable Computing Device 2014–2018: Forecast and Analysis*, s.l.: s.n.

IDC, 2016. *Worldwide Internet of Things Forecast Update: 2015 – 2019*, s.l.: s.n.

Iera, A., Morabito, G. & Atzori, L., 2010. *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*. s.l.:Springer.

Internet of Things Russian research center, 2013. *What is holding up the IoT*. [Online]

Available at: <http://internetofthings.ru/issledovaniya/26-v-chjom-sila-interneta-veshchej>

[Accessed September 2016].

Internet Telecommunications Union (ITU), n.d. [Online]

Available at: <http://www.itu.int/en/Pages/default.aspx>

[Accessed September 2016].

IPSO alliance, n.d. *Enabling IoT devices' interoperability*. [Online]

Available at: <http://www.ipso-alliance.org/>

[Accessed September 2016].

Jane, H., 2011. *White coat syndrome' sees blood pressure mis-diagnosed*, s.l.: BBC News.

Kaleido, 2016. *Kaleido insulin pump*. [Online]

Available at: <http://www.hellokaleido.com/>

[Accessed September 2016].

- Kiritsis, D., 2011. Closed-loop PLM for intelligent products in the era of IoT. In: *Emerging Industry Needs for Frameworks and Technologies for Echanging and Sharing Product Lifecycle on Computer-aided Design*. s.l.:s.n., pp. 479-501.
- Korsten, P. & Christian, S., 2010. *The world's 4 trillion dollar challenge*, s.l.: IBM Institute for Business Value.
- Kranz, M., 2016. *Building the Internet of Things: Implement New Business Models, Disrupt Competitors, Transform Your Industry*. s.l.:s.n.
- Lampi, M., 2016. Digital Archiving and eServices.
- Ledger, D. & McCaffrey, D., 2014. *Inside Wearables Whitepaper*, s.l.: s.n.
- Lee, S. M., 2014. *Genentech CEO wonders if wearables craze is 'a bit trivial*, s.l.: San Francisco Chronicle.
- Mark, L., 2011. *Health apps contribute 10% to 10 billion app downloads*, s.l.: Healthy living.
- Medtronic, 2016. *The MiniMed Paradigm Revel System*. [Online]
Available at: <http://professional.medtronicdiabetes.com/paradigm-revel-real-time>
[Accessed November 2016].
- Michelle, C., 2011. *Next for Jeopardy! Winner: Dr. Watson, I Presume?*, s.l.: Time.
- Mzahm, A. M., 2012. *Towards a Design Model for Things in Agents of Things*, s.l.: s.n.
- Niewolny, D., 2014. *How IoT is revolutionizing healthcare*, s.l.: Freescale.
- Postscapes, 2015. *Internet of Things history*. [Online]
Available at: <http://www.postscapes.com/internet-of-things-history/>
[Accessed October 2016].
- PwC, 2014. *Health wearables: early days*, s.l.: s.n.
- PwC, 2014. *PwC Global State of Information Security Survey 2015*, s.l.: s.n.
- Rock Health, 2014. *2014 Midyear Digital Health Funding Update: Obliterating Records*, s.l.: s.n.

Sklyar, V., 2016. *Top ten technologies for IoT*. [Online]

Available at: <https://habrahabr.ru/post/308892/>

[Accessed September 2016].

The Telegraph, 2011. *S&N and the global medical device industry by numbers*, s.l.: s.n.

U.S. Food and Drug Administration, 2016. *Overview of Device Regulation*, s.l.: s.n.

Valsamidou, A., 2014. *Update on the European Proposal for a Medical Devices Regulation*, s.l.: s.n.

Vermesan, O., Friess, P., Guillemin, P. & Gusmeroli, S., 2011. Internet of things strategic research roadmap. In: *Internet of Things: Global Technological and Societal Trends*. s.l.:s.n., pp. 9-52.

Wei, W. & Toenjes, R., 2012. *A Comprehensive Ontology for Knowledge Representation in the Internet of Things*, s.l.: IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

Whitman, M., 2015. *10 Big Tech Trends in Healthcare*, s.l.: HP Matter.

APPENDICES

Appendix 1

Questionnaire used to explore target audience for smart healthcare devices in Finland

- How old are you? (select the answer)
 - a. Under 18
 - b. 18-45
 - c. Over 45
- Are you permanently living in Finland? (select the answer)
 - a. Yes
 - b. No
- If you are not Finnish, specify your home country. (fill in the field)
- What is your occupation? (fill in the field)
- Are you working? (select the answer only if not clear from the previous question)
 - a. Yes, full-time
 - b. Yes, part-time
 - c. No
- Do you have some chronic illness? (select the answer)
 - a. Yes
 - b. No
- If you answered "yes" to the previous question, specify the illness, if you want to. (fill in the field)
- Do you have a professional IT background? (select the answer)
 - a. Yes
 - b. No
- Do you have a professional medical background? (select the answer)
 - a. Yes
 - b. No
- Do you have a smartphone? (select the answer)
 - a. Yes
 - b. No
- Are you familiar with Internet of Things (IoT)? (select the answer)
 - a. Yes
 - b. No

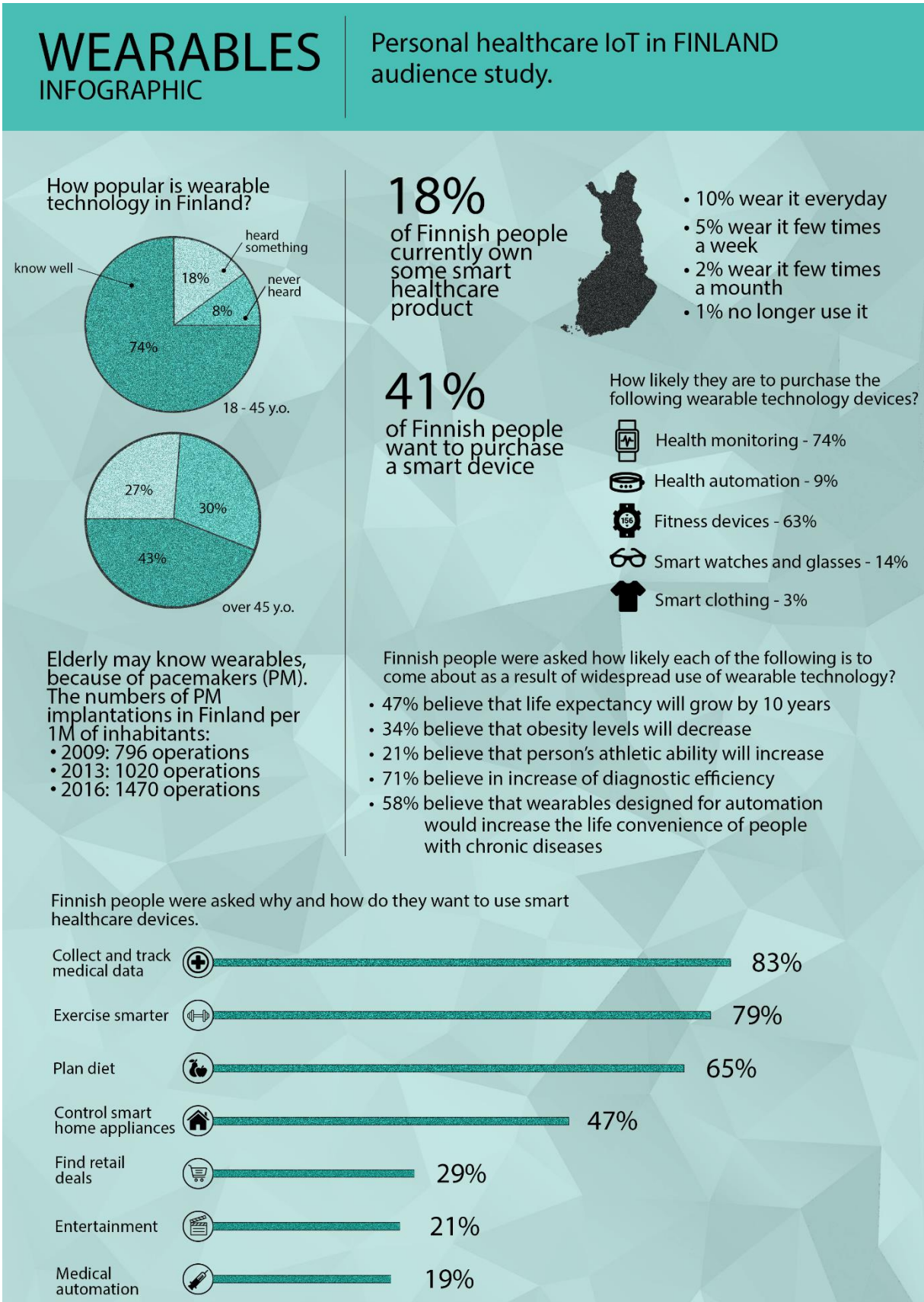
- If you answered "yes" to the previous question, rate your experience from 1 to 5. (fill in the field)
- Are you familiar with IoT application for medicine and healthcare? (select the answer)
 - a. Yes, I know the topic very well
 - b. Somewhat familiar
 - c. I have heard
 - d. No idea. Never heard about it
- Do you know what wearable technology is? (select the answer)
 - a. I know well
 - b. I heard something
 - c. Never heard
- Do you consider pacemaker to be a wearable? (select the answer)
 - a. Yes
 - b. No
 - c. I don't know
- Do you consider insulin pump to be a wearable? (select the answer)
 - a. Yes
 - b. No
 - c. I don't know
- Do you consider insulin pump to be healthcare IoT? (select the answer)
 - a. Yes
 - b. No
 - c. I don't know
- Do you have some smart healthcare product? (select the answer)
 - a. Yes
 - b. No
 - c. I am not sure, specify the name of device or brand
- If you answered "yes" to the previous question, how often do you use your device?/If you answered "no" to the previous question, how likely you are up to buy a new smart device? (select the answer)
 - a. I wear it every day/I want to buy an exact product
 - b. I wear it few times a week/I know for what I want to use it, but I have not chosen the exact product or model yet
 - c. I wear it few times a month/I want some product probably

- d. I never use it, but I used it for some time after purchase/I have never thought about it
- e. I have never used it after purchase/I do not want to
- How likely you will purchase one of the following items. Rate by priority from 1 to 5. (drag the elements or put numbers in case of hardcopy)
 - a. Insulin pump with CGM
 - b. Fitness tracker
 - c. Smart watches or glasses
 - d. Smart T-shirt that senses your sweat
 - e. Wristband which tracks your blood pressure and pulse
- What do you think is most likely to be a result of healthcare IoT widespread? Rate by priority from 1 to 5. (drag the elements or put numbers in case of hardcopy)
 - a. Life expectancy will grow by 10 years
 - b. Obesity levels will decrease
 - c. Person's athletic ability will increase
 - d. Diagnostic and treatment would be more efficient
 - e. The life convenience of chronically ill people would increase
- If you will have an opportunity to choose any smart healthcare device, how do you want to use it? Rate the probability. Rate by priority from 1 to 5. (drag the elements or put numbers in case of hardcopy)
 - a. Collect and track medical data
 - b. Plan personal diet
 - c. Exercise smarter
 - d. Control smart-home appliances
 - e. Entertainment purposes
 - f. Find retail deals
 - g. Medical automation purpose (rank as highest only if you have some chronic disease, for example, diabetes)
- How much money can you spend on healthcare wearable? (select the answer)
 - a. I want it for free from government organization
 - b. I want it for free from employer
 - c. I want it for free from insurance company
 - d. Less than 50€
 - e. 50€ to 120€
 - f. 120€ to 200€

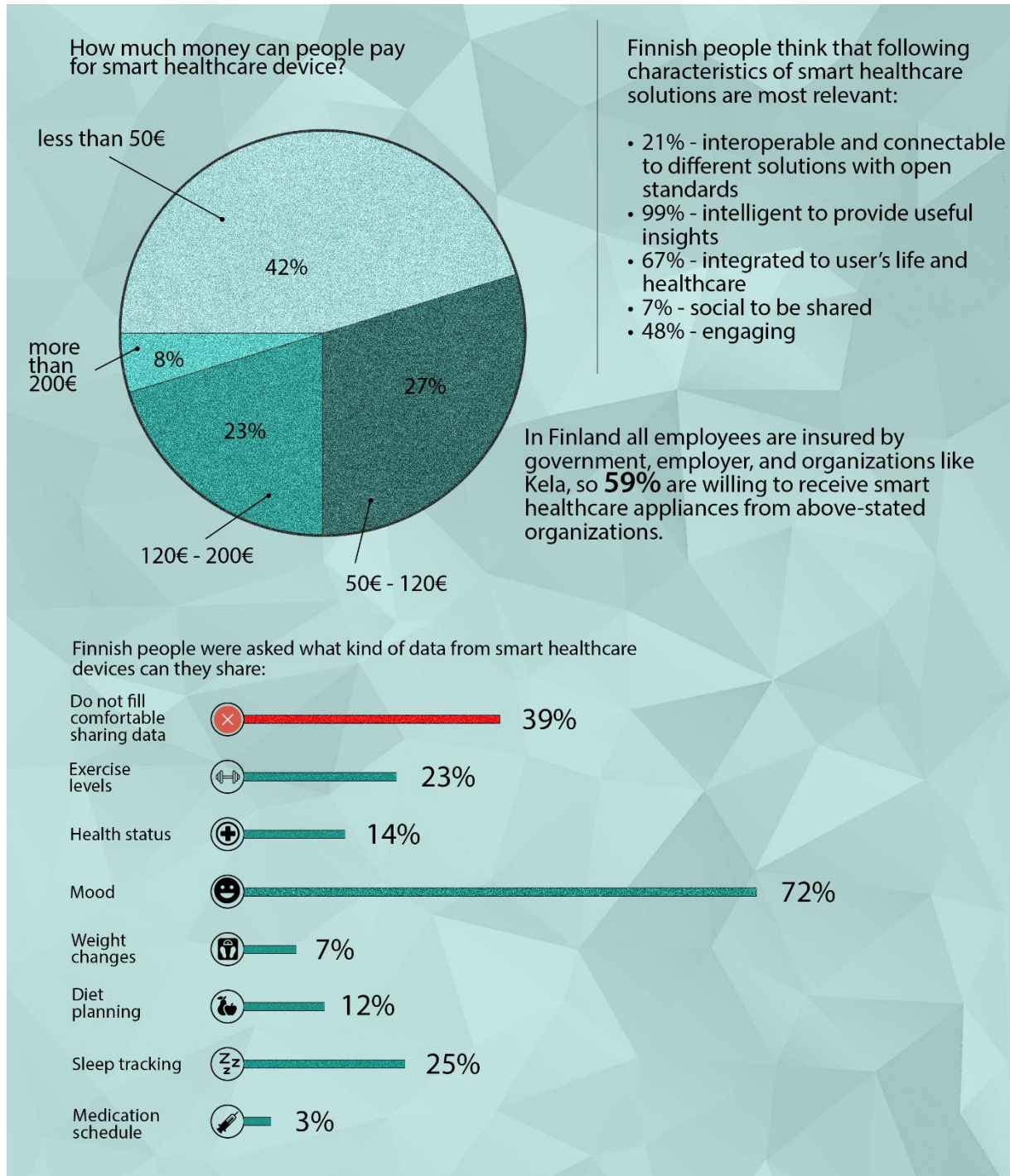
- g. More than 200€
- If your answer to the previous question starts from "I want it for free", please, still evaluate how much money can you spend on healthcare wearable. (select the answer)
 - a. Less than 50€
 - b. 50€ to 120€
 - c. 121€ to 200€
 - d. More than 200€
- Evaluate the relevance of characteristics of smart healthcare appliance. Rate by priority from 1 to 5. (drag the elements or put numbers in case of hardcopy)
 - a. Interoperable and connectable to other solutions
 - b. Intelligent to provide useful data insights
 - c. Integrated to daily life and healthcare
 - d. Social to be shared
 - e. Engaging
- Are you open to sharing some personal healthcare data? (select the answer)
 - a. Yes
 - b. No
- If you answered "yes" to the previous question, what kind of data do you want to share? Rate by probability from 1 to 5. (drag the elements or put numbers in case of hardcopy)
 - a. Exercise levels
 - b. Personal health status
 - c. Mood
 - d. Weight tracking
 - e. Diet
 - f. Sleep statistics
 - g. Medication schedule
- Express your own thoughts about healthcare IoT and wearables. (fill in the field)

Appendix 2(1)

Audience study infographic



Appendix 2(2)



Appendix 3

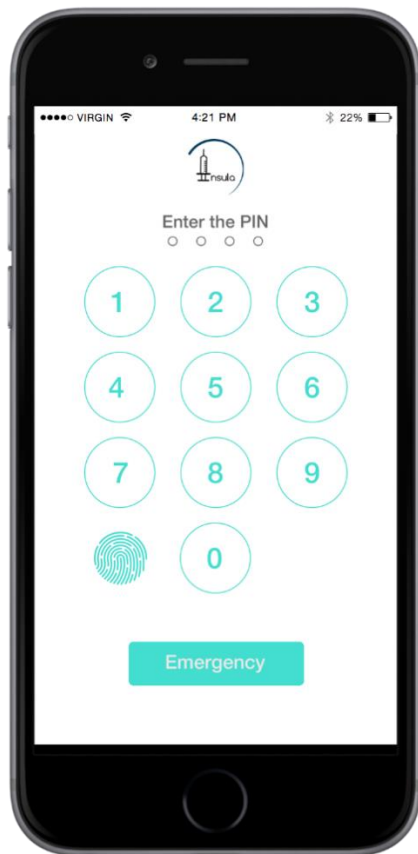
Bracelet infographic



Appendix 4(1)

Application mockups

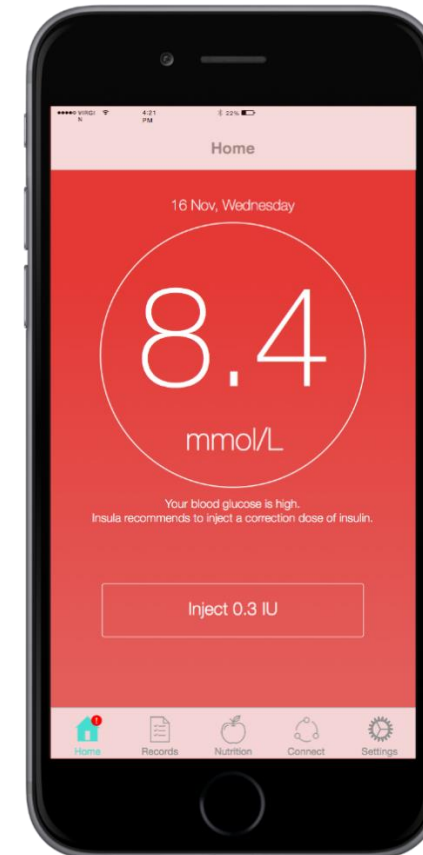
Personal and secure for
you



Track your current status

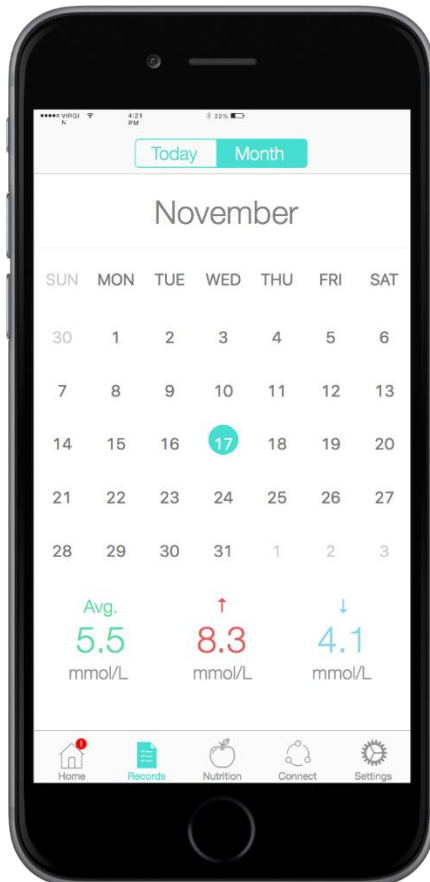


Be warned



Appendix 4(2)

Daily recorded statistics of **everything you** might **need**



Calculate **required dose** based on next meal

Personal approach for every patient & community **support**

The smartphone screen displays the Nutrition input form. It includes the following information:

- Specify your food:** 6:00 PM
- Chicken:** 200g. (with minus and plus buttons)
- Tomatoes:** 50g. (with minus, plus, and a green plus button)
- Suggested dose:** 0.2 IU at 5:00 PM
- Accept** button at the bottom.

The bottom navigation bar includes icons for Home, Records, Nutrition, Connect, and Settings.

The smartphone screen displays a patient profile for Matti Lehtonen. It includes the following information:

- Community** and **Doctor** tabs at the top.
- Matti Lehtonen**, Mikkelin Keskussairaala
- Phone:** +358453123456
- E-mail:** lehtonen@hospital.fi
- Contact via application** button
- Emergency call** button

The bottom navigation bar includes icons for Home, Records, Nutrition, Connect, and Settings.

Personal healthcare Internet of Things

Guidelines for developing proper
smart healthcare solutions



INTRODUCTION

ABOUT THE PAPER

The Internet of Things (IoT) is much more than the result of modern and complex technologies smashed together. In the following pages, you'll **read about how Internet of Things is revolutionizing healthcare sector** bringing new approaches to treatment and diagnostic, as well as health control.

The purpose of the paper is to **show what eHealth sector is**, how IoT is applied for medical purposes and to **provide the combination of guidelines, trends and findings which could be used to design and develop a proper smart solution**. The report is focused on consumer-oriented or personal healthcare. The audience study was performed in Finland.

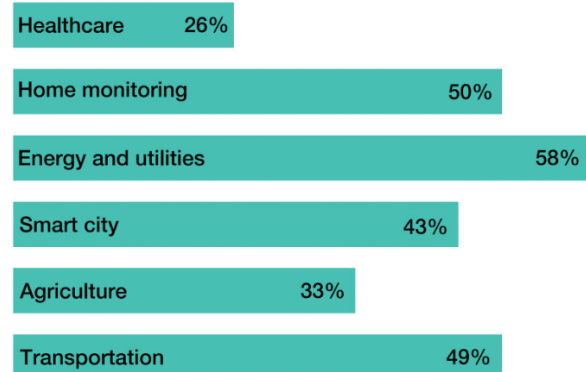
All in all, the study covers key digital medicine issues, such as perspectives, security and privacy, regulations and adoption, patient's user experience and market research.

The paper is **based on thesis [7] and provides key findings, summarizes the studies performed for academic purposes**, however the output and results are very useful and practical to speed IoT adoption and deliver measurable results across healthcare industry. The guidelines are **targeted to business specialists who are willing to operate in eHealth sector** but are not able to correlate the needs and technological capabilities, as well as **IT specialist who are not familiar with non-technical aspects of healthcare Internet of Things**. Also, large and small businesses can benefit from this paper, as they will understand how to derive the greatest benefit from smart healthcare products. Finally, everyone interested in the field could find the report worth reading.

INTERNET OF THINGS GEARS THE INNOVATION OF 21 CENTURY

Today, when all sectors are developed no more crucial changes are happening and something revolutionary is needed. It is Internet of Things, which connects everything together. It provides new ways of collecting and using data. Businesses are building IoT into future strategies and business models. Companies across all industries now have IoT in their plans. The worldwide Internet of Things market spend will grow from \$591.7 billion in 2014 to \$1.3 trillion in 2019 with a compound annual growth rate of 17%. The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019, hitting 30 billion in 2020. [1]

Graphic 1: IoT network connections - 2014 vs. 2015 % growth [2]



The Internet of Things is in our homes, cars and phones, and, increasingly, on your body. It's connecting people to their cities and apartments, linking patients to health care providers, bringing companies in closer touch with their consumers and capturing our imaginations. As IoT is about connections, graphic 1 shows the growth of network connections. It clear that healthcare sector is an outsider, consequently it should be considered as a new opportunity for new business, however medical sector is tough and well-regulated.

IOT IN HEALTHCARE: THE TIME IS NOW

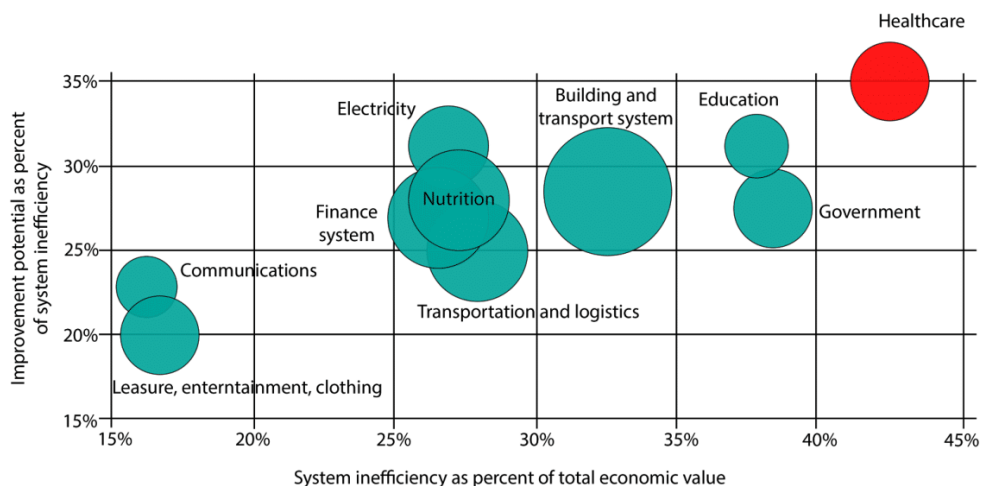
In the Internet of Things devices collect and transfer information directly to each other and the cloud, making it possible to gather, record and analyze data faster and more accurately. That suggests all sorts of interesting possibilities across a range of industries. But nowhere does the IoT offer greater promise than in the field of healthcare, where its principles are already being applied to improve access to care, increase the quality of care and most importantly reduce the cost of care. As the technology for collecting, analyzing and transmitting data in the IoT continues to mature, we'll see more and more new IoT-driven healthcare applications and systems emerge. [3]

Effective medical technologies are always the most relevant because maintaining health and the quality of life for years remains an urgent task. Internet of things in many ways alters notions of access to health services, increases the quality and reduces the cost. The habit of using smart things help the patient and the physician to cooperate efficiently in the diagnosis and treatment processes. Nowadays, global healthcare system wastes \$2 trillion per year, which shows complete inefficiency, as changes are minor. [6] Healthcare systems are the least efficient, comparing to other systems, and it has the biggest improvement potential. See Graphic 2.

This prostration is mainly caused by the inability to properly collect data and transfer it for subsequent analysis to support diagnosis and treatment method selection. The medical literature is doubling each seven years, and it becomes impossible for doctors to understand the condition of the patient and to prescribe a needed treatment. Moreover, the amount of patient data is dramatically expanding because of genomic data, making diagnostics even more complicated. Today 20% of medical errors are caused by diagnostic errors, which are not only incorrect diagnosis but delayed ones. [5] Connected healthcare devices have a huge potential to accelerate the speeds of patient appeals and doctors decision-making, providing time for proper and efficient treatment, by collecting and analyzing patient data and medical resources.

Healthcare presents IT and medical companies a new business operating area, which is a rare situation in the 21st century. Even more special, this white space allows companies to make money while simultaneously doing a significant job for society. All in all, healthcare IoT can revolutionize the medical treatment, providing new ways for improved diagnosis and treatment, making people healthier in efficient and cost-effective manner, but the question is what companies should do to bring innovative solutions to the healthcare community and change the medicine completely.

Graphic 2: Inefficiency and improvement potential of healthcare sector [4]



FACTORS ACCELERATING ADOPTION OF eHEALTH AND KEY FINDINGS

Networked medical devices have bridged the human-machine interface, delivering the most personal of benefits. They literally embed the Internet into people's lives, improving medical outcomes, offering better quality of life, and lowering healthcare costs. They also potentially introduce security flaws, market incomprehension and other challenges along with clear benefits. However, these troubles can be managed, and even it is possible to improve the quality of service, if they have been overcome properly.

KEY TROUBLES AND QUESTIONS OBSERVED AND COVERED

- **Who is the user of healthcare devices? How this audience should be targeted?**
- **Security and privacy are number one issues.**
- **What is the appropriate price for personal healthcare solution?**
- **What are the needs of people?**
- **Regulations are not clear.**
- **Community and ecosystems: why are they important?**
- **User experience in smart healthcare.**
- **Collaboration with partners.**

TARGET THE HEALTH OBSERVERS

There is a huge disintegrated group of common people who are looking for some wearables or other devices for extensive health monitoring. They are looking for information to avoid possible risks and to make some steps in time. Today there are no solutions for them, so this group must be targeted to put eHealth on new level. See graphic 4 for exact audiences.

People from this group is not highly healthy motivated and are not doing a lot of sports. They are healthy, in general, or have some popular

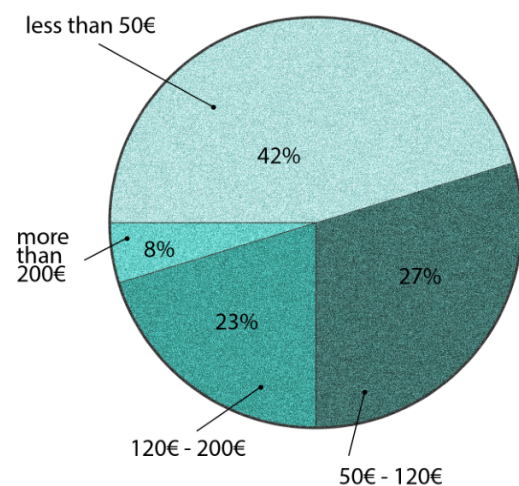
chronic illness and willing to support their current condition without wasting too much time on it. To reach the "health observers" auditorium businesses have to develop solutions meeting important requirements and fulfilling the needs of all consumers, from children to elders.

MAKE COST-EFFECTIVE PRODUCTS

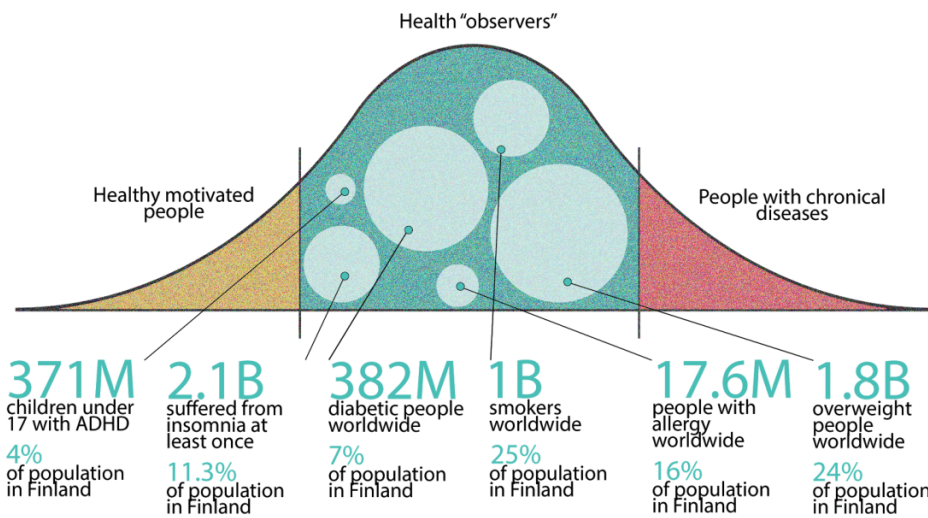
Current users with ultimate motivation (life or death or heavy fitness interest) to use healthcare IoT rank this criteria as the main one, the situation will not change with "observers", as they will not pay money for the incomprehensible and expensive device.

Price is the biggest concern for 91% of all respondents. The money issue is even more relevant than security and privacy. In Finland all employees are insured by government, employer, and organizations like Kela, so 59% are willing to receive smart healthcare appliances from above-stated organizations. See Graphic 3 for Finnish audience research.

Graphic 3: How much Finnish people are able to pay for smart healthcare solution.



Appendix 5(5)



Graphic 4: Examples of target groups with statistics in audience of "health observers"

ALLOW REAL-TIME MONITORING

People are looking for devices that help with complex situations or just control the health. Telemedicine solutions should replace classic approach for analysis and diagnostics allowing health checks without multiple ineffective doctors visits.

EVERYONE IS LOOKING FOR SIMPLICITY

Making a simple device with intuitive controls or application is very important, as adoption of the new product will depend on simple approachability of monitoring for everyone involved. Device and user interface have to be intuitive and not too featured at least at the beginning, while consumers take up the technology.

DESIGN THE DEVICE WITH THE END SYSTEM RESULT IN MIND

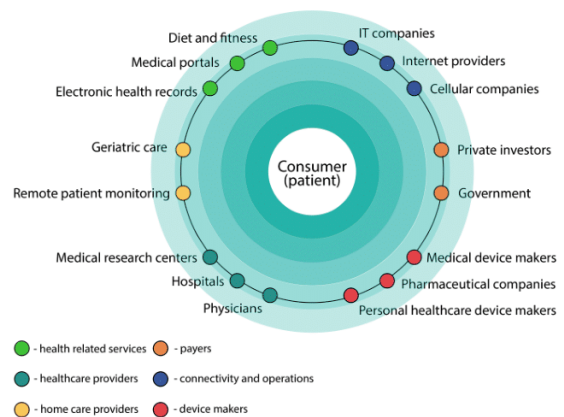
Consumers need a comprehensive system to meet the objectives of health monitoring maximally absolute. It requires integration with healthcare providers, social organizations, insurance companies and so on, consequently the appliance must be designed with the end system result in focus.

CHOOSE BUSINESS POSITIONS AND PARTNERS WELL

Companies need to select an optimal sphere and business position in healthcare ecosystem by

evaluating their operating strengths and weaknesses. Partners are crucial because the single company is not able to provide full smart healthcare system at this stage of development, see Graphic 5.

Graphic 5: Participants of IoT healthcare ecosystem



SHARING DATA AND GETTING FEEDBACK ARE CRITICAL

Users want health professionals to incorporate data from health devices into diagnosis and treatment decisions. Consumers recognize that monitoring data, when combined with a range of other inputs, enables health professionals to see a more complete picture.

Appendix 5(6)

5

WORK ON STANDARDIZATION

The industry is looking for interconnectivity of all devices. Therefore device makers collaboration is needed, which will help to set the requirements of technologies and regulations for the connected health device ecosystem faster.

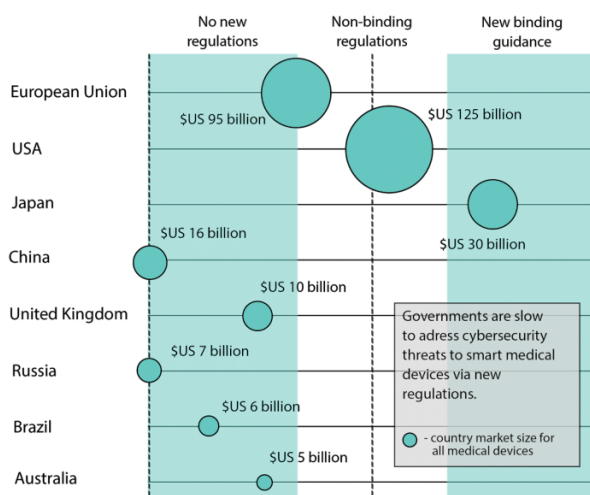
APPLY THE “SECURE-BY-DESIGN” APPROACH

Security must be number one issue while designing and building the product. It should not be added afterward, as it was in the past, what caused different challenges.

IMPROVE COLLABORATION

Improving public-public and public-private collaboration is another issue. Healthcare and telemedicine are overcrowded with different regulations which do not suit the real needs of digital age medicine evolution. Adding more regulations will only worsen the situation, and more coordination is important. The truth is that regulators are not so fast with technological innovation, see Graph 6.

Graphic 6: Regulatory spectrum for networked medical devices



REGULATORY METHODS SHOULD BE CHANGED

The current regulatory methods and the whole paradigm should be changed to encourage innovation in the field, while still meeting security needs and public needs.

USAGE SHIFTING TOWARD PREVENTION AND MANAGEMENT OF HEALTH

People are using devices to measure and manage a known health problem. However, interest in preventative usage is on the rise. Within two years, 30 percent more respondents expect to be using devices to encourage physical activity, and twice as many will depend on devices to inform others of someone's changing health condition.

USAGE SHIFTING TOWARD PREVENTION AND MANAGEMENT OF HEALTH

Not surprisingly, the top data requirement is privacy and security, as noted by 96% of respondents. However, more interestingly, a high percentage of respondents also want to be able to share and use the data in a variety of ways.

CONCLUSION

The medical profession should benefit from networked medical devices in ways that are still unclear sometimes. The practice of medicine is as old as human civilization, though it sometimes resists adopting of new technology. Someday tools were changed, nowadays IoT should be involved in treatment and diagnosis processes. Health practitioners and physicians, working with patients and their families, device makers, developers and business specialists are particularly well suited to drive the right balances among security, safety, effectiveness, and patient experience.

REFERENCES

- [1] IDC, "Worldwide Internet of Things Forecast"
Update: 2015 – 2019, February 2016
- [2] Verizon, "State of the Market:
Internet of Things 2016", April 2016
- [3] Freescale, "How the Internet of
Things Is Revolutionizing
Healthcare", David Niewolny, October 2013
- [4] IBM Institute for Business Value, "The future of
connected health devices", March 2011
- [5] Watson for a Smarter Planet: Healthcare
- [6] Korsten, Peter and Christian Seider, "The world's
4 trillion dollar challenge: Using a
system-of-systems approach to build a smarter
planet," IBM Institute for Business Value,
January 2010
- [7] Kirill Lazarev, "Internet of Things for personal
healthcare. Studies of application, motivation
and audience of eHealth sector. Smart wearable
design", December 2016