# A smarter home, the smarter choice?

By

Marie Berland Nesheim & Kine Sandanger Rosnes

Faculty of Social Sciences
UiS Business School
Spring of 2016

Universitetet
i Stavanger

**FACULTY OF SOCIAL SCIENCES,**
**UIS BUSINESS SCHOOL**

# MASTER’S THESIS

| | |
|---|---|
| STUDY PROGRAM:<br>Masters in Economics and Business Administration | THESIS IS WRITTEN IN THE FOLLOWING SPECIALIZATION/SUBJECT:<br>Strategic Management<br>IS THE ASSIGNMENT CONFIDENTIAL?<br>No |

TITLE:

A smarter home, the smarter choice?

| | | |
|---|---|---|
| AUTHOR(S) | | SUPERVISOR: |
| Student number: | Name: | Jan Frick |
| 227807<br>……..……..… | Marie Berland Nesheim<br>……………………………………. | |
| 229922<br>…………….. | Kine Sandanger Rosnes<br>……………………………………. | |

ACKNOWLEDGE RECEIPT OF 2 BOUND COPIES OF THESIS
Stavanger, ……/…… 2016 Signature administration:……………………………

# Abstract

In a world of expanding connected products, home automation has shown itself as one of the biggest trends to follow. Home automation is the automation of the home via highly advanced systems that control multiple functions of the home - more often called *smart homes.* The purpose of this thesis is to examine the developments of smart homes and how it affects us as consumers. We also try to identify users, benefits and issues of smart homes.

The research is done with a theoretical approach, via literature reviews and indirect observations.

The findings showed multiple areas of development. The smart home industry is growing and taking its share of the smart market. Multiple companies have entered the market, delivering complete smart homes or devices to make your home smarter. Companies are contributing to an easier tomorrow. Smart homes are for everyone, but we see it as highly beneficial for health purposes in a world where the elderly population is growing rapidly. This is an area of focus for the future.

Three main issues were identified; privacy, security and standards. These areas has to be addressed in near future for the smart home to be fully adopted. The privacy and security of data has to be secured in the best ways possible. The more our technological world grows, the more private data is collected and needed to control. Standards are greatly lacking within smart homes and the technology behind, and has to be in place to ensure proper protocols, methods and interoperability.

*Key words: Internet of Things, RFID, smart home, sensors, M2M, standardizations, WSN, middleware, security, energy, health care, home automation*

# Preface

This master's thesis is written as the final part of the MSc in Economics and Business Administration with a specialization in Strategic Management at UiS Business School, University of Stavanger.

The process of writing this thesis over the last five months has been challenging, but is has also been an exciting and interesting process. We have explored a subject we knew little to nothing about, and it has been a rollercoaster of knowledge ever since the first article.

We would like to thank our supervisor Jan Frick for the help and guidance into the exciting theme of smart homes. This is a theme we feel is highly relevant in the technological world we live in today.

We would also like to thank all of our fellow students, professors and friends for making our two years at UiS exciting and unforgettable.

*Stavanger, June 13th 2016*

Marie Berland Nesheim & Kine Sandanger Rosnes

# Table of content

# 1. Introduction

## 1.1 Motivation and background for the choice of topic

87% of people have never heard of the term “Internet of Things” (IoT) (Marr, 2015b). The term refers to devices that communicates, collects, and transmit data via the internet. In the year 2008 there were more things connected to the internet than there were people. Marr (2015b) believes that less than 0,1% of all the objects that can be connected to the Internet is currently connected, showing enormous potential and opportunities for both businesses and society. It’s predicted that there will be 6,4 billion connected things in use in 2016 (van der Meulen, 2015), an increase of 30 % from 2015. By 2020, 50 billion internet devices is believed to exist (Machado and Shah, 2016). According to some estimates, IoT could add $10-$15 trillion to the global GDP the next 20 years (Kellner, 2013). Estimations done by the McKinsey Global Institute say the IoT will have a total financial impact of up to $11 trillion by the year 2025 (Kavis, 2014).

The Consumer Electronics Show (CES) is the largest global technology tradeshow, held each year in Las Vegas by the Consumer Technology Association (CES, 2016). CES showcases new technology and products, as well as improved existing ones. Products comes from a wide range of consumer technology markets; accessories, audio, electronic gaming, fitness, health and biotech, internet services, robotics, sensors, smart homes, wearables, wireless devices & services, etc. Amongst the biggest trends at the 2016 tradeshow were drones, virtual reality, wearables and connected homes (Minor, 2016). A connected home - a smart home - dominated CES in 2015 (Curtis, 2015), and made a strong impact this year too. A smart home is a home with systems for automation – mainly of lighting, temperature, security and multimedia (Craven, 2015). Our smart products keep getting smarter and finding new areas to enter. Home appliances can be controlled by the touch of a button or even by voice activation (Mamiit, 2016). The development of RFID, sensors, and overall the Internet of Things are enabling a large and newer market to grow. The development and possibilities of smarter homes are interesting to follow. It happens rapidly, and can have a great impact on multiple sectors and our own private life.

## 1.2 Presentation of research problem

The aim of the thesis is to examine *the developments of smart homes and how it affects us as consumers*. We start by looking at the Internet of Things as a backbone for the development of smart homes, before we go into the background of smart homes themselves. The following questions will be analyzed to answer the thesis' research problem:

- What are major developments in the industry of smart homes?
- What will happen in the smart home industry forward?
- Who can use smart homes, and who will be using smart homes?
- What are the benefits and issues in the smart home industry?

The areas dominating the smart homes are security, energy and home automation. We have chosen to narrow down the areas of research to these because of their domination. In addition, we will look at devices that can be used in the house, i.e. robots, smart kitchens, etc. - making an fully automated home. We focus on the happenings in the western world. This is because we can collect more data in form of reports and articles from North America and Europe, and it is more relevant to us and the readers of the thesis.

## 1.3 Thesis structure

The thesis is divided into five main parts; theoretical background, method, analysis, discussion and conclusion. In the first part will go through the background of Internet of Things and enabling technologies for the internet development and risks. Where we will introduce smart home, and go through the status of development until now. In the second part, research design and methods used for writing the thesis will be presented. The third part analyses the development of smart homes today, costs and attitudes. Following the analysis is a discussion of users of smart homes, the need of a smart home through looking at benefits and disadvantages, and the future of smart homes. The thesis is ended with a conclusion of the findings.

# 2. Theoretical background

This chapter will go through relevant previous literature in the area of study. Firstly, we present the Internet of Things, enabling technologies, and internet risks. We will then present the main focus of the paper which is smart homes. This includes brief history, how it works, and our four selected areas.

## 2.1 Internet of Things

According to Wang (2010) the Internet of Things is defined as "Things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environment, and user context". This means that things are connected together and communicate with each other without any human interaction. The internet of things can be tracked all the way back to January 1926 (Novak, 2015) when Nikola Tesla said to Collier Magazine:

> "*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 real and rhythmic whole. We shall be able to communicate with one another instantly, irrespective of distance. Not only this, but through television and telephony we shall see and hear one another as perfectly as though we were face to face, despite intervening distances of thousands of miles; and the instruments through which we shall be able to do his will be amazingly simple compared with our present telephone. A man will be able to carry one in his vest pocket.*"

This was only six years after the television was introduced, and Tesla was already then predicting a world with worldwide mobile communication, videophones and broadcast TV. All of his predictions is now a reality, and even more wireless we believe will it be.

### 2.1.1 The history of the Internet

Before we can understand the Internet of Things we need to look at the beginning of the Internet. The technological foundation for the internet was made in the DARPA-project in the late 1960s (Rossen and Liseter, 2015). The goal was to develop an efficient data transport network for access to major computing facilities in universities that DARPA has sponsored. An important principle was that there should be a strong network in failure situations. There should not be a central control point for the network, but several autonomous centers that could communicate although some lines or units fell out. The solution for the communication was built on a concept called packet switching, which shared outgoing messages into a number of smaller packages that everyone got the same address. The packages would even find their way through the net, often different paths before they were reunited at their destination. This kind of a system would be able to adapt to situations where parts of the network was inoperable for short or long periods.

The first nodes were connected in December 1969 and the net was named ARPANET (Rossen and Liseter, 2015). After only one year the number of nodes grew to 13, and increased to approximately 50 nodes in 1975. Only two of these were outside the US, one in London and the other in Kjeller. DARPA left it up to the participating institutions to develop software for host computers, and that's how the internet already from the beginning got a "voluntary character".

In the first half of 1970, the development of the first local distribution networks started (Rossen and Liseter, 2015), and it became clear that there was a need for a technology that connected LANs together. In order to connect different networks together you'd need to build gateways that could receive and transmit information to global addresses and handle different package sizes. In addition, one would need a more flexible and robust transport protocol than the one used in ARPANET. This sparked the development of Transmission Control Protocol/Internet Protocol ( TCP/IP), which is the basis for today's internet.

The first TCP/IP attempts took place in 1975 (Rossen and Liseter, 2015), and over the next few years' protocol was continuously improved and improved with support for a wide range of services. Berkeley University, which had a contract with DARPA on the further development of AT & T's UNIX system, built TCP/IP in the operating system itself, which eventually was set free at the disposal of all universities in the US and Europe. TCP/IP was eventually such a key factor that DARPA decided to introduce it as a standard protocol in ARPANET. This work was completed in early 1983. The result was "a network of networks" called INTERNET, also monitored, maintained and managed by BBN. Many wanted to connect to the internet, but DARPA set a condition. The network would only be used for non-commercial purposes, primarily research. The term "research" was, however, used in a very general sense, and eventually be able to both public institutions, universities, colleges, research and development departments connect. This happened gladly by a local area network was connected to existing routers, or via its own routers and leased lines to the nearest routes in INTERNET. That's how INTERNET steadily expanded, and eventually got a fairly complex infrastructure without clear boundaries and central management. The various components were paid and driven by countless organization in more or less voluntarily.

In 1986, the National Science Foundation (NSF) in the United States took on the responsibility of running a high-speed backbone network that would tie together the five newly established supercomputer centers in the United States (Rossen and Liseter, 2015). These networks were paired with appropriate routers and had ramifications for Europe. Eventually, the remaining portion of

ARPANET was unnecessary. In the end of the 1980s ARPANET was phased out, which also made the INTERNET disappeared. Instead came a rapidly growing conglomerate of networks and routers called the Internet, defined as a network of interoperable, TCP/IP-based networks. This internet had no overarching structure and had many owners and operating organizations.

Sir Tim Berners-Lee, a British computer scientist, proposed the world wide web in 1989 (Berners-Lee and Fischetti, 2000), and already in 1991 the first web page was created. But even before the first web page was connected to the internet, a device was connected to it in 1990 (Newton, 2012); a toaster that could be turn on and off over the internet.

### 2.1.2 History of the Internet of Things

There has been visions of smart, communicating objects even before the global computer network was launched forty-five years ago (Press, 2014). As the Internet has grown to link all signs of intelligence around the world, a number of other terms related to the idea and practice of connecting everything to everything made their appearance; including Radio Frequency Identification (RFID), context-aware computing, machine-to-machine (M2M), and the Web of Things.

In 1949 the development of the bar code started with Norman Joseph Woodland (Press, 2014). He received the first patent for a linear bar code in the year 1952. More than twenty years later George Laurer, was one of those primarily responsible for refining the idea for use by supermarkets. In 1973 Mario Cardullo received the first patent for a passive, read-write RFID tag (Press, 2014). And in 1974 a Universal Product Code (UPC) label was used to check out purchases at a store for the first time.

In the 1990s Xerox EuroPARC’s Mik Lamming and Mike Flynn demonstrated the Forget-Me-Not (Press, 2014), a wearable device that communicates via wireless transmitters and records interactions with people and devices, storing the information in a database. In the year 1995, Siemens set up a department to develop and launch a GSM data module called #M1” for machine-to-machine (M2M) industrial applications, enabling machines to communicate over wireless networks. The first M1 module was used for point of sale (POS) terminals, in vehicle telematics, remote monitoring and tracking and tracing applications. The Auto-ID Center was established at MIT in the late 90s. Sanjay Sarma, David Brock and Kevin Ashton turned RFID into a networking technology by linking objects to the Internet through the RFID tag (Machado and Shah, 2016).

In October 2004, Neil Gershen, Raffi Krikorian and Danny Cohen (2004) wrote in the Scientific American: “Giving everyday objects the ability to connect to a data network would have a range of benefits: making it easier for homeowners to configure their lights and switches, reducing the cost and complexity of building construction, assisting with home health care. Many alternative standards currently compete to do just that - a situation reminiscent of the early days of the Internet, when computers and networks came in multiple incompatible types.”

## 2.2 Development of the Internet of Things

Connected things send and receive data through the network relating to a variety of physical characteristics such as pulse rates, revolutions per minute, velocity, moisture levels or temperature (Rubens, 2014). The network is also relating to more complex data such as maintenance requirements, sound, and static or moving images. The beginning of IoT applications are the things themselves. These edge devices usually have a low-power processor, no screen, some sort of implanted operating system and a way of communicating using one or more communication protocols. The things can connect directly to the Internet, to an Internet gateway device or to neighboring things. Under you’ll find different technologies enabling connecting things to the internet, to get things to react or communicate.

### 2.2.1 Radio Frequency Identification (RFID)

Radio-frequency identification (RFID) is used for object-to-object communication (Ferguson, 2002), and is a technology using radio frequency to identify and track objects. RFID technology systems consists of a tag and a reader. This kind of communication has become practical for allowing a “silent commerce” that requires no human interaction. The tag is placed on or in a product, and the reader reads the information situated in the tag. Companies are rapidly adopting the technology to reduce costs, help customers and enhance security. As RFID becomes more sophisticated and widespread, it begins to reshape companies, supply chains, even industries.

To understand the ability of object-to-object communication, it’s useful to compare the technology to its most immediate precursor; bar coding (Ferguson, 2002). Warehouses, manufacturing, plants, and retail stores have for a long time used bar code labels to track and manage inventory and work in progress. Replacing bar codes with smart tags provides a raft of advantages, i.e. items doesn’t have to be read one at a time. Because RFID tags and readers communicate wirelessly, cartons, whole carts, or pallets of products can be read in an instant. The items also doesn’t have to be near a reader. A smart tag can be read at a distance without pointing the reader directly at the tag. The technology doesn’t require perfect conditions because smart tags can withstand harsh treatment and temperature extremes. They can even be used under extremely adverse conditions, such as in an arctic oil field. The RFID tag can also hold a lot more information than the barcodes relatively simple information (Webb, 2008). A smart tag can carry extensive, specific information - giving each item a unique identity and history.

There are three main types of RFID tags today; passive, active and battery-assisted passive.

*Passive tags*

Passive RFID tags are tags without an internal power source. They rely on the radio frequency-signal from the reader to be identified. Passive tags can be read up to six meters away, but are scanned manually in most commercial uses (RFID Journal, 2016). Since the passive tag requires less components, it’s cheaper to produce. This makes it affordable for many industries, and passive tags are therefore the most used.

Passive tags can be placed on people to deny or permit entry to restricted areas or the use of equipment (Ferguson, 2002). For example, FedEx uses tagged identity wristbands as an alternative to easily lost keys. This gives the drivers access to their vehicles, ensuring only authorized use and speeding delivery time. In some cases, the limitations are for the restricted person’s own good. For example in a nursing home the tags can keep demented people for getting to the roof.

*Active tags*

Active RFID tags have an added component in form of a battery. The battery allows the tag to constantly be on the lookout for a signal from its reader, and can be operated at a much greater length (RFID Journal, 2016). Active tags with a single battery can normally be read from about 30 meters or more away. With an additional battery, it can be read at over 100 meters. In addition, the performance of the tag is not affected by water or metal. Because of the added features the active tag is great for situations where the tags cannot “wait in line” to be scanned, but is also more expensive.

Another great advantage of active tags is that they can detect the presence of a tagged object automatically (Ferguson, 2002), even when humans might prefer that the items not be noticed. That’s probably why the technology was so attractive to a liquor distributor in the UK whose inventory consisted of single-malt whiskeys. The expensive spirits had a tendency of leaving the building unauthorized, so the distributor built a new warehouse security system with RFID readers to track tagged cartons, avoiding the whiskey from being stolen or accidentally misrouted.

*Battery-Assisted Passive tags (BAP)*

Battery-Assisted Passive tags (or semi-passive) are tags with a small battery that transmits an ID signal periodically (Atzori et. al., 2010). This allows for greater read distances and quicker response time than ordinary RFID tags (coreRFID, 2016). BAP tags only use the power of the reader to identify that the reading is in progress. They use their own implanted battery to power up, run the chip, to transmit and receive data, and keep the memory. The tag's battery usually last about 5 years (Smiley, 2016). When the battery dies, the tags behave as passive tags so that nothing is lost. the battery cannot be recharged and needs to be replaced.  The difference from active tags is that BAP tags do not transmit. They use the battery to improve the signal strength when they respond to a reader, and usually have a slightly longer lifespan than active tags (Rubens, 2014). BAP tags in ISO card format, for example, are often used as personal identifiers in access control systems, loyalty systems, personnel management or membership cards. This is most likely because they have a read distance of up to 5 meters and can be used while inside a pocket, in a purse or hanging from a lanyard.

*RFID systems*

Active- and passive systems are the most commonly used RFID systems. An active system generates a constant signal between the reader and the tag. The passive system receives a radio wave, then modulates the wave to the data content in the radio frequency tag, and returns the modulated signal (Harmon, 2010). A typical RFID system has few readers and many tags. One reader can handle several tags.

The RFID systems are broken down in three types of frequency bands; low, high and ultra-high. A system that operates at lower frequencies has a shorter read range and slower data read. A system that operates at higher frequencies transfers data faster and longer. The higher the frequency, the more the sensitivity to radio wave interferences. Active and passive systems can operate on either frequency bands.

*The breakthrough of RFID technology*

RFID is not a new technology, and has been used commercially since the 1970s (Webb, 2008). Some of the first significant work related to the RFID was done already in 1948 by Stockman

(Chawla, 2007), but wasn't used commercially before the 1970s (Webb, 2008). RFID has been taken more into use the last decade. In 2005, three main factors were slowing down the breakthrough; international standards, security of the data, and price (Duin, 2008). The extensive technology breakthrough has enabled the RFID price to be lowered the last years, but the work on standardizations and the issue of data security are still slowing down the full potential. Several standardization-organizations have been working to create international standards for the use of RFID (Atzori, Iera & Morabito, 2010). ISO, EIC, EPCglobal and ETSI are amongst the organizations that have developed standards that are used today.

### 2.2.2 Sensors

According to the Business Dictionary (2016), a sensor is a "Device that detects changes in the ambient conditions or in the state of another device or a system, and conveys or records this information in a certain manner." There are many types of sensors - amongst them pressure sensors, humidity sensors, passive infrared sensors, and displacement sensors.

Using sensors to transmit information is used more as the internet access and user face has expanded. A sensor network is made up of sensing nodes that communicate in a wireless multi-hop fashion (Atzori et. al., 2010). These networks are called wireless sensing networks, and was incepted in the late 90s (Ammari, 2013). The number of sensing nodes are usually high, and they are self-contained with their own energy source (Olafsen, 2007). The sensor network is able to deliver data exceeding what an RFID tag can deliver. Sensors can give locations, availability, movement, temperature, state of physical health, etc. Wireless sensor networks (WSN) have a gathering point, named *sink*, that stores the data collected by the sensing nodes (Ammari, 2013). This way, the sensing nodes can collect more data. One of the main issues with WSN are the limited number of IP addresses in the current internet (Atzori et al., 2010). There are not enough IP addresses for the high numbers of sensing nodes needed for a complete Internet of Things situation as it is today. The IEEE 802.15.4 standard is what most WSN are based on.

Developments are being made in microelectromechanical systems (MEMS), which consist of tiny sensors and actuators that are capable of sensing what's going on and act on it (Ferguson, 2002). Location-sensing technology is also making strides. Over short distances, wireless technologies such as Bluetooth lets smart objects know when other smart objects come into range, so that they can communicate. Over longer distances, the United States Global Positioning System (GPS), opened up to commercial access in May 2000, making it possible to pinpoint and track object almost anywhere.

### 2.2.3 Hybrid: RFID sensing networks

RFID systems and sensors combined allows new applications of the Internet of Things. Using sensing technology in passive RFID tags expands the use of passive RFID systems, and can allow a passive system to sense, compute and communicate. The combination is called RFID sensing networks (Atzori et al., 2010). The sensing tag still harvests its own power from the reader, and therefore does not have the same range as wireless sensing networks. As of today, there are few standards for these networks.

In Barcelona, Spain, 18 000 trash bins are being equipped with smart chips and sensors that will tell the collection company how full each bin is and when it was last emptied (Ferguson 2002). With that information, the company can route its trucks to stop only for bins that needs to be emptied or serviced. These applications were just the beginning. Sensing technology is advancing rapidly as new findings in materials and chemical sciences give rise to an array of new sensors, actuators, and transmitters with far greater capabilities to detect and transmit environmental information.

### 2.2.4 Machine to Machine (M2M)

The increasingly popular machine-to-machine technology plans to take advantage of the high developments (Lawton, 2004). M2M would influence connectivity to enable machines to communicate directly with one another. An example of M2M use can be when the window blinds register incoming sun, transferring data to the air conditioner and thermostat so it can regulate to its set temperature.

M2M is based on the idea that a machine is more valuable when it is networked, and the network has a higher value when more machines are connected (Lawton, 2004). With M2M, machines not only collects data about other devices, but also takes action based on the information in certain cases. Sensors that gather the information that some M2M systems transmit are becoming more widely used and thus are driving demand for the technology (Lawton, 2004). The lower cost of sensors and initiatives for integrating them into larger systems are also increasing the approach’s popularity. The biggest trend is that vendors are expanding M2M in to wireless technology, using radio chips or modules they can attach to almost any device or machine. M2M is gearing up for exponential growth.

M2M works with standardized technologies such as TCP/IP, IEEE 802.11 wireless LANs, cellular communications technologies, and wired networks as Ethernet (Lawton, 2004). Using standards allows for easier device interoperation in M2M systems and facilitates using mass-produced, standards-compliant equipment - making implementation less expensive, simpler, and quicker. M2M nodes can operate autonomously, push information to multiple systems and other nodes, and even make some decisions on their own.

M2M applications are used for monitoring environments or activities and for controlling devices or systems (Lawton, 2004). M2M could for example be used to monitor and control building temperatures, lighting levels, and security. You could use M2M to monitor soil moisture in your garden by setting irrigation schedules to use water efficiently. In addition, M2M monitoring applications can be used for tracking equipment and merchandise that have sensors, such as RFID tags. M2M-based control applications need systems to make decisions based on input from multiple sensors. For example, a network of distributed temperature sensors could control a heating system.

### 2.2.5 Standardizations

The issue of standards has been a major reason for why the development and use of RFID, wireless sensor networks and M2M has been slowed down. Internationally recognized standards for the development and use of the technology needed to create the fully connected Internet of Things for a commercial use have to be set. According to the European Telecommunications Standards Institute (ETSI, 2016b), the use of standards gives three major advantages; interoperable and cost-effective solutions, opportunities in new areas, and the market can reach its full potential.

*RFID*

By 2008, many standards had been set for RFID technology. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) set standards for frequencies, data-encoding methods, and the use of RFID technology and performance testing (Webb, 2008). In 2010 the focus of RFID standardization was on RFID frequency and reader-tag communication protocols, labels and data on tags. EPCglobal, ETSI and ISO were the main organizations involved (Atzori et al., 2010). The work on further standards for RFID is still ongoing.

For RFID to be fully successful in the market, a wide range of standards are needed. Amongst these are technical-, data-, conformance-, application- and network standards (Harmon, 2010). Conformance standards are standards for enabling interoperability between products from different manufacturers.

*Wireless sensor networks (WSN)*

Wireless sensor networks have mainly been based on the IEEE 802.15.4 standards. The Institute of Electrical and Electronics Engineers (IEEE) have developed several major standards, and is one of the leading standards-making organization (Wikipedia, 2016c) The IEEE 802.15.4 standard defines the physical and MAC layers for low-power, low-bit rate communications in wireless personal area networks (WPAN) (Atzori et al., 2010). The Open Geospatial Consortium (OGC) are working on standards that will allow interoperability of monitoring and controlling wireless sensor networks through a web browser (Wikipedia, 2016f). The University of California Berkeley started the project OpenWSN to build an open-based standard of protocols that can be implemented with the existing IEEE standard (OpenWSN, 2016; Watteyne et al., 2012).

*RFID Sensing Networks*

As of today, there are few standards for commercial RFID sensing networks. Standardizations are under continuous development because of the rapid changes and progress in the used technologies.

*Machine-to-machine*

Machine to machine (M2M) communication standards have been driven forward by two main organizations; the 3$^{rd}$-generation partnership project (3GPP) and the European Telecommunications Standard Institute (ETSI). They have defined one proposal each for architectures for M2M. 3GPP focuses mainly on communication, and has developed the 3GPP machine-type communications – also called MTC. ETSI on the other hand focuses on applications of M2M, and developed the ETSI M2M architecture. Together they are trying to define a combined model – the ETSI/3GPP architectural model (Misic & Misic, 2014).

In addition to 3GPP and ETSI, several open machine to machine initiatives have been started. Eclipse Machine to Machine Industry Working Group are working on open communication protocols, frameworks and tools. ITU-T Focus Group M2M are working on a common M2M service layer. In addition, we have initiatives as Weightless, XMPP, and OASIS MQTT (Wikipedia, 2016d).

### 2.2.6 Middleware

Atzori et. al. (2010) describes Middleware as a software layer between the technology and the application levels. The software helps manage the complexity and heterogeneity in the systems by providing a common programming across the systems (Bakken, 2001). Middleware can make coding more portable, more productive and give fewer errors. It masks heterogeneity and gives transparency (Bakken, 2001). Having a good middleware has been a requirement for functioning global Internet of Things projects (Amaral et al., 2016). There are many different middleware software existing today. ROS, iRoom, Aura, JCAF, Voyager, Smart-Its, UbiComp, ACOSO and Context Toolkit make up some of them (Fortino & Trunfio, 2014).

The architecture of the middleware varies from software to software. Most middleware architectures used for the Internet of Things follows the Service-oriented Architecture (SOA) (Atzori et al., 2010). OASIS (2012) defines Service-oriented Architecture as “a paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains.” As seen figure 1, SOA has five horizontal layers dealing with the enabling the capabilities that are required by the applications running on the middleware (OpenGroup, 2016); Consumer Interface Layer, Business Process Layer, Services Layer, Service Components Layer, and Operational Systems Layer. The Integration Layer, Quality of Service Layer, Informational Layer and the Governance Layer makes up the four supporting layers to the horizontal layers. Each horizontal layer is supported by every supporting layer (Wikipedia, 2016f).

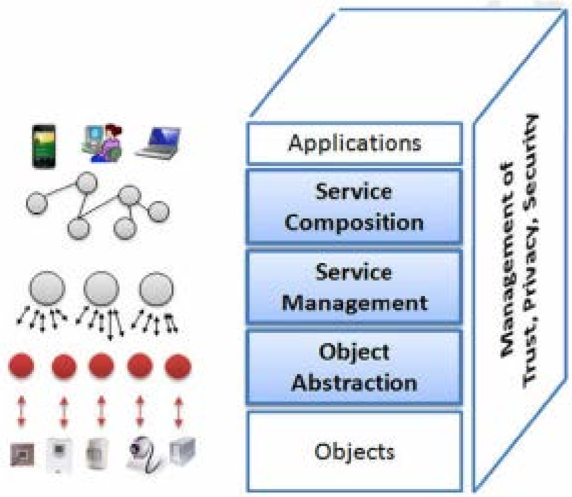

*Figure 1: SOA-based architecture for the IoT Middleware (Atzori et. al., 2010)*

## 2.3 Internet risks

Although IoT can result in financial-, safety-, health-, and quality-of-life benefits, IoT can also introduce new risks (ISACA, 2015). Any new technology, process or business method can increase risk, but IoT, because of its pervasiveness, has the potential to increase risk significantly. Risk scenarios differ between enterprises that manufacture and sell communication-capable embedded systems and enterprises that are users of IoT devices.

### 2.3.1 Business risk

One of the most significant business risks is the potential health- and safety impact if the operation of a device is sabotaged (ISACA, 2015). Research shows that wireless, potentially lethal attacks are possible against implantable biomedical devices, such as a defibrillator or a pacemaker. Similar life-threatening attacks have demonstrated against automobile systems, including the ability to disable the braking systems of an automobile when it is in motion (Greenberg, 2013).

Privacy is a significant business risk consideration. In the 2014 ISACA risk/Reward Barometer (ISACA, 2014) about people's attitude toward decreasing level of personal privacy, 69% said they were very concerned, 25% were somewhat concerned, 4% not concerned, and the last 2% didn't believe that personal privacy was decreasing. There are many examples where privacy impacts existence. One example that shows unwanted privacy impact is home monitoring systems. These systems are designed to protect the home and its inhabitants, but can be vulnerable to wireless attacks that violate privacy and security. Video baby monitors are often placed in a child's bedroom so that parents can check on the child remotely, from almost anywhere. These monitors can broadcast to TVs, handheld receivers, to PCs and Smartphones (ISACA, 2015). Many incidents of intruders hacking into Internet-enabled video baby monitors have been reported. Most monitors have security features, but parents are responsible for enabling these features and setting a password.

Not only human agents bring about these health and safety impacts; A malware can infect a system with a critical safety role, such as a navigation system in an airplane, an automobile braking system or a smoke sensor (ISACA, 2015).

In addition to health and safety risks, regulatory risk is possible. Regulatory concerns can occur when embedded computing complements (ISACA, 2015):

- process potentially sensitive data (e.g., PoS systems that process payment information)

- intersects with regulatory-governed business processes (e.g., financial reporting for public companies or patient care in a clinical environment)
- impacts on the critical infrastructure (e.g., power and industrial control systems)

Regulatory mandates often apply to communication-enabled devices. If regulatory mandates apply, the complexity of the regulated environment can be compounded because of devices of this type (ISACA, 2015). For example, a point of sale (POS) system in a retail location may be built to conform to pay card industry (PCI) requirements, but a smoke detector on the same network may not conform. A magnetic resonance imaging (MRI) machine may be built to comply with the Health Insurance Portability and Accountability Act (HIPAA) technical requirements, but the thermostat in an operating theater may not comply.

Unexpected costs can occur if an existing, non-computing-cable is replaced with a computing-cable device because it could require additional connectivity (possibly requiring personnel resources or capital expenditure), or it may require additional support to realize the full value (ISACA, 2015). Consumers should therefore evaluate whether the connection of a device to the network adds sufficient business value to justify potential increases in risk.

### 2.3.2 Operational risk

In addition to business risk, the operational aspects of using an embedded system must be considered. For example, machine-to-machine communication must be appropriately secured to ensure that only personnel and authorized devices have access to make configuration changes and gather telemetry data. In most cases, this security requires operational planning and needs to tie into current security and monitoring controls to ensure that the level of access is appropriate.

Likewise, from an operational perspective, challenges can be introduced when devices are deployed without the knowledge of the personnel that holds a stake in configuring, monitoring, maintaining and securing the device (ISACA, 2015). Shadow IT is the deployment of technology components without centralized oversight and appropriate governance and can have a significant damaging impact on IoT usage. Without someone “at the switch” to ensure that risk scenarios are addressed, devices behave as expected and devices are appropriately secured - the enterprise may unknowingly take on risk that is outside of the enterprise comfort level.

### 2.3.3 Technical risk

At a technical level, embedded computing has the potential for more complex set of challenges than traditional IT (ISACA, 2015). Embedded (IoT) devices can like traditional computing devices be attacked, suffer outages and be compromised by malware, because they are addressable and connected to network. Because the underlying operation of IoT devices may be less transparent (due to less clear organizational administration responsibility) and a large quantity of IoT devices is possible in the long run, keeping them secured is likely to be more complex than for traditional computing devices.

In terms of technical risk, attacks against the IoT devices should be considered (ISACA, 2015). Many well-publicized attacks against embedded systems illustrate how these types of attacks can detrimentally impact IoT computing. For example, Spanish security researchers Javier Vazques-Vidal and Alberto Garcia Illera developed the Can Hacking Tool (CHT) from off-the-shelf electronic components (Greenberg, 2014). This tool proves how easy it is to hack a car and wirelessly interact with it in ways that can make operation potentially unsafe. Attacks against IoT devices can be challenging for manufacturers to respond to (ISACA, 2015). In some situations, the pathway to remediate the issues requires a hardware upgrade rather than modifications to the firmware alone. This dynamic can expose enterprises that employ IoT devices to attacks, with minimal ability to implement countermeasures. Even in situations where a firmware updates remediates for the issue - a new attack or vulnerabilities discovered in an IoT hardware device requires operation personnel to maintain awareness of those developments and implement mechanisms to respond.

Devices that process personal, private or potentially sensitive information of customers (e.g. equipment in a healthcare context) have the potential to impact user privacy (ISACA, 2015). Like other challenges, privacy impacts should be evacuated prior to deployment. As wearables and other connected devices increasingly make their way into the workplace, IT professionals still see more risk than benefits (ISACA, 2015). Still, with sound preparation, education and governance, enterprises can be well positioned to embrace the benefits of the Internet of Things.

## 2.4 Smart home

The definition of a smart home has been greatly expanded the last years. The basis of a smart home is that it has advanced automation systems (Smart Home Energy, 2016). It started small, and now includes multiple functions. Craven (2015) defines a smart home as “a house that has highly advanced automatic systems for lighting, temperature control, multimedia, security, and other functions”. This means that the home will appear “intelligent” because its computer system can monitor so many aspects of daily living (Alonso et. al., 2011).

The smart home technology has become increasingly sophisticated. Coded signals are sent through the home’s wiring to outlets and switches that are programmed to operate appliances and electronic devices in every aspect of the house. The development of solutions for smart homes is about to adopt the technology in such a way that it solves people’s needs at home, and can be used by everyone in an easy way (Lyse, 2016).

The developments of smart sensor systems have led to a new era of universal networks (Suryadevara and Mukhopadhyay, 2015). The increase in users of the internet and advancements in global computing widely enables internet connected everyday things. Internet of Things is about things talking together, M2M communications, as well as person-to-computer communications by extending to things usages. In the present technological scenario, the two terms IoT and Smart things repeatedly occur together. The Internet of Things contributes to the growth of smartness in interconnected things. In general, smart things and the Internet of Things follow each other in their individual application scenarios. The main objective of IoT is to have the ability to uniquely recognize, signify and access things at anytime and anywhere in an internetwork and this can allow controlling of any “things” in an ideal situation.

Home automation is a smart home system with scattered wireless smart sensing units and effective data processing system that can be realized with the help of an IoT framework (Suryadevara and Mukhopadhyay, 2015). Additionally, the system can be used for monitoring the behavior of an inhabitant and evaluate the longitudinal elderly healthcare assessment. Therefore, the IoT framework can fuse the smart sensor data of household appliance usages and execute multiple tasks of IoT for the smart home monitoring system.

Smart home solutions are making homes more special and provides comfort, safety and security in our everyday life. It will also provide lower energy consumption, and thus savings in energy costs in the long run. With a smart home you have full control of all electrical installations. The system is dynamic and alive, and can in a simple way be adapted to all phases of life. Smart homes are equally good in everything from cottages and apartments to luxurious villas and commercial buildings.

### 2.4.1 History of smart homes

One can say that the basis of smart homes was already set in the early 1900s when household machines were introduced. But it wasn't until the mid-1900s that the thought of a more automated home was sown. The first home computer, the ECHO IV, was introduced in 1966. It was built to compute shopping lists, to control the power of appliances, and to control the temperature of the home (Rothfeld, 2015). This was the true start of smart homes. In the 1970s, the very first home automation system was created. The X10 used power lines to communicate between appliances (Wikipedia, 2016g). Following this new development, an interest group called Smart House was created in the US in 1984. Their mission was to advocate for inclusion of technology in the home design. By the 1990s, the entertainment industry took over the term smart home. Movies and tv series about homes with systems and appliances with somewhat of a mind of their own was made. The term smart home became widely known.

*Earlier projects*

Smart homes have been seen as a hopeful and cost-effective way of improving home care of elderly and disabled. A number of earlier projects have therefore been mostly related to health and improving the quality of life. Chan et al. (2008) goes through a large number of earlier projects in their research;

- *ACHE* is an adaptive house that uses neural networks in controlling the energy. Temperature, heating and lighting does not have to be pre-programmed by the residents because the home used reinforcement learning. The house monitors the environment and analyzes the patterns to adjust according to the resident.
- *GatorTech Smart House* has individual smart devices fitted with sensors. These are connected to an operational platform, and tries to elevate comfort and safety.
- *Elite Care* is an assisted living facility with inhabitants suffering from dementia and Alzheimer's. The facility detects changes in physical or cognitive condition based on

continuous monitoring. By detecting the changes, they can find solutions for them to stay as self-sufficient as long as possible.

- *Ubiquitous Home* was developed in Japan. The home is equipped with sensors that monitored human activities. It also has microphones and cameras to capture activities that sensors does not pick up on. The data collected in this project is gathered to understand the human behavior and find solutions for automation in future smart homes.

Similar smart homes equipped with sensors have been developed in Europe. *CarerNet, The Millennium Home, SmartBo* and the *HIS project* are some of them. All main systems of these homes were controlled automatically.

### 2.4.2 How does a smart home work?

The sudden explosion of smart homes the last decade comes from of the enabling internet technologies. Sensor development and the access to Wi-Fi has led to a rapid eruption of systems, appliances and gadgets. Advanced sensor networks, RFID technology and Wi-Fi is enabling things to communicate with each other. That is what makes a smart home – a home where the systems and appliances communicate with you and each other.

A smart home system is a complex, but easy to use, system. The smart home system consists of a platform run on a technology protocol (often called a hub), a network and an interface. The original platform protocol is the X10. This was a manual platform where you plugged in what you wanted to automate (Woodford, 2015). Later, computer-controlled and Wireless Internet systems were developed. Zigbee, Z-Wave, Thread, Insteon and Wi-Fi are only some of the standards within technology protocols used (Wikipedia, 2016b). These are standards that doesn’t run with each other (Shankland, 2016). The network connects the platform, interface and the appliances connected to the platform together. Powerline Carrier Systems sends coded signals that convey commands (Rouse, 2005). These commands control how and when the specific device will operate. What allows you as a user to control the home as you want, is the interface. The interface often comes in form of an app on a tablet or a mobile device. This is where you can easily turn on or off heating, lighting, and alarm systems. You control the house with a swipe or a click.

### 2.4.3 Areas of research

Until now, the main focus of smart homes has been on security, energy and health. This is what has been easiest to produce, commercialize and sell. 90% of consumers says that security is the top reason to invest in a smart home system is because of security (Icontrol, 2015). Smart homes were also originally thought of for health purposes – to help people in need at home. Because of the enormous attention on these areas, we have chosen to focus on them is this thesis. In addition to security, energy and health – we look at home automation in form of complete systems and smart devices.

### *Security*

In today's world there are security systems fitted for every lifestyle, budget and need. In addition to keeping your house safe and secure, security systems in today's age can keep you connected to your home whenever and wherever as long as you have a mobile device (Honeywell, 2016a). Security systems can be equipped with touch screens, surveillance cameras, motion sensors, 24-hour monitoring, environmental sensors, theft protection, emergency help, remote locking, and much more. -

A lot of security systems offer 24-hour monitoring via a central station with highly trained home security professionals standing by, ready to send help in case of emergency (Honeywell, 2016a). Different security systems have different type of sensors, Honeywell is one of many companies that offers sensors detecting movement both inside and outside, listening for the sound of breaking glass to guard against intruders, protecting valuables and more. These sensors enhance the effectiveness of your security system and provide the complete, whole-house protection. Some sensors can even detect the difference between an intruder and your pet. These gives you the chance to let animals up to 50 kg move freely around the home without triggering the alarm (Honeywell, 2016a). Environmental sensors help prevent disaster before it starts, and are ideal for bathrooms, kitchens, laundry rooms and basements. These detectors can notify owners when detecting floods, leaks and extreme temperatures - helping minimizing the risk of dangerous conditions and damages to the home and interior. Imagine a furnace or a stove that could sense the presence of nearby flammable materials and turn itself off before a potential fire started (Ferguson, 2002). You can integrate the management of outlets where you connect electrical appliances such as irons, coffee maker, washing machine etc. to reduce and prevent of fire. In Norway, Lyse has installed a fire alarm that immediately and automatically alerts the fire department when triggered (Lyse, 2016). There are also wireless theft protection sensors that can be affixed to any valuable in the home, and send out an alert when an attempt is made to move or disturb the object. These kind of sensors are great for valuables like electronics, artwork, computers, antiques, etc.

With digital video security, one can view live-streaming video in and around the house or receive clips and images of important events when they occur (Honeywell, 2016a). One can even view video and receive notifications of activity in dark and low-light indoor environments for added peace of mind. It is also possible to watch your pet at any time of the day or get a notification when your pet sitter or dog walker arrives, or if they didn’t show up.

Most alarm systems come with a remote panic pendant that provides a peace of mind by summoning emergency help with the press of a button (Honeywell, 2016a). A button lets the person in need of emergency assistance send signals to the central to call the police or a medical response team when the alarm is triggered. Compact and water-resistant, the alarm can be worn as a belt, pendant, wristband or keychain style for example.

Another device that can boost your security is remote locking. You can leave the home and make sure that doors and windows are closed (Carlo Gavazzi AS, 2016). It is possible to schedule the doors to lock and unlock automatically whenever you turn on or off your security system, and set scenes and schedules for added safety and convenience (Honeywell, 2016c). You can lock the door from any location as long as you have an internet connection (Honeywell, 2016a). With a touch of a button you can unlock the door from your office to let in someone who lost their key or is delivering a package. Or in the event that you forgot to lock the door when going on vacation, you can do it even though you’ve already left your house. The lock can be scheduled to lock the same time every night, or unlock the same time every morning.

*Energy*

A network of smart meters, smart devices and smart networks continuously communicate with each other to ensure peak leveling and load balancing of energy consumption, down to the device level (Cognizant, 2014). To reduce demands during high peak periods, smart networks communicate with devices when energy demand is high and track how much electricity is used and when it is used.

Smart objects makes it is easier to save money and energy, and make your home more efficient and comfortable place (Honeywell, 2016b). Some items that can be controlled are thermostats, lighting, ceiling fans, air-conditions and more. Whether you’re home or on the go, the smart devices are managed via your smartphone or a compatible wireless devices. Most devices can be set to automatically adjust every time the security system is armed or disarmed. Smart lighting gives you the option of turn on or off lighting remotely. If you go on vacation and forget to turn off your lights, you can turn them off by using a smartphone or a mobile device - saving money and energy. Installing automated shades makes them automatically lower to block out sun and heat during hot periods to cut your cooling costs. Or the shades can be automatically raised to let sun in to warm your home during cooler weather. One can also save electricity by letting natural light in to offset the need for electrical light.

Creating automated scenes and schedules with different smart devices can help maximize energy savings effortlessly while making the home greener (Honeywell, 2016b). An example of a schedule can be for the lights to turn off, the shades to be drawn and the thermostat adjusting itself to a more economical setting when you leave the house for the day. Or you can set a schedule to turn on the heat when you leave for your cabin so you enter a warm and comfortable cabin. A set of devices can turn on or off at different times of the day, or on one or more days of the week. It's also possible to set scenes and schedules for energy savings and receive alerts on a smartphone or mobile device when settings are changing, or if an object exceeds a specified range. Lyse offers an automatic electricity meter supplied by Lyse Elnett with all their Smartly-products (Lyse, 2016). The automatic meter transmits the measurements to Lyse every hour. This makes it much easier to have control over the current costs, what the costs were at a specific time period, or when a device was in use. With this function it is easy to refrain from using much electricity when the power is expensive to save electricity and money.

*Health*

The report from "An Aging World" showed that within the next decade, there will be more elderly people than children (National Institute on Aging, et al., 2011; Pilkington, 2009). The age span of humans has increased over the last decade and people over the age of 65 are estimated to rise to 19,3% by 2050 (Gavrilov and Heuveline, 2003). The life expectancy for the 21th century is projected to grow for individuals; from 46-89 years to 66-93 years (World Development Indicators, 2012). Our aging population expects that this better longevity will help them to live an independent and higher quality life in their own home (Suryadevara and Mukhopadhyay, 2015). However, those with a poor health condition require help in the form of medical assistance that can be delivered directly in times of need. One of the main concerns are the increased cost of providing healthcare services and the sustainability of the services (Khawaja, 2011). According to a news report, the cost of healthcare is increasing rapidly (Armstrong 2009). The needs of care are rising, but the low staff levels within health care does not have the capacity to meet the needs (RCN 2010). Over half of the respondents in a Norwegian health care report on institutions for elderly thinks that the patients needs for safety, companionship and activity is not met (Gautun & Hermansen, 2011). Hence, there is a necessity for an alternative, low-cost, and sustainable arrangement of healthcare for the near future. A solution is to transform the normal home to smart home through universal computing technology to support the care of the elderly living independently. Smart home health care comes in form of monitoring and technology solutions for understanding and helping the patient.

Big data in healthcare is being used to cure disease, predict epidemics, improve quality of life and avoid preventable deaths (Marr, 2015b). Big data is a term for large or complex data sets that traditional data processing applications are inadequate to process (Wikipedia, 2016a). With the world's population increasing and everybody living longer, models for treatment delivery are quickly changing, and many of the decisions behind those changes are being driven by data. The drive is to understand as much as possible about a patient as early in their life as possible – hopefully picking up on warning signs of serious illness early enough for treatment to be far more simple (and less expensive) than if it had not been spotted until later. Advances in sensor technology are making the creation of new data much easier (Cousin et al., 2015). But tracking activity and adding sensors to pill bottles and hospital beds are only the first step. To be beneficial, all those data need to be communicated, aggregated, and analyzed in ways that enable new and more effective action. The technologies that enables what is known as the IoT is opening new ways to create value from information (Orton-Jones, 2014). For example, a health care provider could detect potential issues in a prosthetic knee joint, using peripheral data sensors summarizing the bilateral force distribution and pressure patterns (Cousin, 2015). This would deliver great value to the patient (alerting him or her to see the doctor at the first hint of strain), the supplier (allowing for 24/7 monitoring and the opportunity to adjust treatment), and the payer (by avoiding additional costs due to remedial treatment or prolonged recovery).

Preventive and wellness care focuses on two types of health consumers: individuals at risk for specific chronic diseases and generally healthy individuals (Cousin, 2015). Medical technology in these areas is largely designed around portable and at-home devices. Most IoT-enabled devices have been wearables like activity monitors and other measurement devices like digital thermometers and digital scales, with an element of data-based services to track results. Wearable shipments almost tripled between the first quarter of 2014 and a year later (IDC, 2015). Apps can be used as everything from pedometers to measure how far you walk in a day, to calorie counters to help you plan your meals or diet. Millions of people are using mobile technology to help them try and live healthier lifestyles (Marr, 2015b). More recently, a steady stream of dedicated wearable devices has emerged, such as Samsung Gear Fit, Jawbone and Fitbit that all allows you to track your progress and upload your data to be complied alongside everyone else’s.

More than a third of Americans suffer from chronic conditions that can get hugely expensive (CDC, 2016). Once a patient falls prey to a chronic disease, the need for continuous health monitoring becomes more important. A number of IoT-enabled devices (stationary, wearables, implantable, or ingestible) are open to patients and providers to monitor heart conditions, diabetes, and other ailments. The devices monitor clinical data (e.g., heart rate or blood glucose), adherence data (e.g., taking medications as prescribed), and consumer health data (e.g., physical activity) (Infobionic, 2016).

Heart-rate and blood-glucose sensors are widely available, but are rarely set up to export their data to a system that aggregates and shares information with all parties involved (Cousin, 2015). While companies have sold remote monitoring products for years, utility to all parties has so far been limited. To realize real value, both providers and patients need these sensors to move beyond mere fall detection and be able to measure a wide array of biosigns so it can communicate those data to an integrated smart home system. Solving these communication issues can ease the shift to greater home care, driving better outcomes for patients and reduced cost for all (Cousin, 2015).

Identity chips have been inserted under the skin of cats, dogs and other pets to help identify runaways for years. A company from Florida have developed a passive RFID chip compatible with human tissue (Ferguson, 2002). It could be used to carry medical information on patients with artificial joints or pacemakers, or to help locating children and impaired adults who gets lost. There’s no logical limit to what information such a chip could carry. The government of Malaysia has already presented a multipurpose smart card that serves as an identity card, passport, source of e-cash, and driver’s licenses. In the future they might be implanted.

*Home automation*

Many manufacturers offer smart appliances – appliances that can be connected to smart electric meters or home energy management systems. This helps you shift over to use energy in off-peak hours, and less energy in peak-hours (U.S. Department of Energy, 2016). Air conditioners, dishwashers, refrigerators and other appliances are available as smart appliances. Companies like

Google and Samsung are investing in home devices. Having a connected kitchen could save the food and beverage industry as much as 15% annually (Marr, 2015b). Google bought smart thermostat maker nest Labs for $3.2B (Bergen, 2016), and Samsung purchased the connected home company Smart Things for $200M (Marr, 2015a). Companies are gearing up for you to communicate with your smart appliances in an effortless and casual manner.

Honeywell's Z-Wave® enabled thermostats can automatically alter the temperature every time you turn on or off your security system (Honeywell, 2016c). It allows you to design customized scenes and schedules for comfort and energy savings, or control your thermostats on-the-go via a mobile device. Precise temperature control provides better comfort and fewer temperature swings. It is also possible to create lockouts to keep temperature limited to a minimum or maximum setting, ideally in homes where children may attempt to adjust the thermostat. You can operate the shades in your home for ambiance, privacy and security by lowering and raising them at specified times. Automated shades make it easier to access skylights and other hard-to-reach windows (Honeywell, 2016c). They're also an ideal way to reduce glare and help shield artwork, furniture, carpeting and floors from the damaging effects of direct sunlight. Entertainment in your household can be a high quality, cinematic experience when you integrate your for example Honeywell systems with popular home systems from vendors like Control 4®, Crestron®, Lutron®, Savant®, RadioRA® 2 or Universal Remote Control (Honeywell, 2016c). Transform your living room into a home theater with the touch of a button.

Creating scenes and schedules can improve your lifestyle and help you save energy and money without a change in your daily routine (Honeywell, 2016c). A "nighttime" scene could involve having the doors lock and the lights shut off when you turn on and off the security system at nightfall. A schedule might be created to set the thermostat to a specific temperature and have the porch and hallway lights on an hour before arriving home from work, so you'll come home to a comfortable, well-lit home. With smart lighting you can turn selected outdoor and indoor lights on or off automatically every time you turn on or off your security system (Honeywell, 2016c). Tell your system to turn one set of lights on 30 minutes before you get home from work and turn them off an hour after you've gone to bed. You can program scenes and schedules for security, control the atmosphere in form of lights or temperature from any remote location.

# 3. Method

In the following chapter we will argue the choice of method, and address the issues of validity, reliability and error sources.

Method comes from the Greek word *methodos* – meaning *to follow a specific road towards a goal* (Store Norske Leksikon, 2016). Within the methodology of social science, the method you choose determines a great part of how you do your research. A method determines what you collect of data, and how you collect it. It also tells you how to analyze and interpret the data collected in the research (Johannessen et al., 2011). The use of method should help secure validity and reliability and minimizing errors to the research. It will help us highlight various issues and hopefully give new knowledge and recognition (Halvorsen, 1993).

## 3.1 Methodological approach

The choice of method is decided by the research question, and the resources in form of time, people and money (Johannessen et al., 2011). The methods used should highlight the research question as best as possible.

We have chosen to do a theoretical approach in this thesis. We have done a literature review and indirect observations to answer the research question, because these methods give us more detailed answers and we could catch developments as they were happening in the process of writing this thesis. We want to describe what is happening in the development and use of smart homes, and this is best done through existing literature and observation.

### 3.1.1 Literature review

The literature study gave an overview and insight into previous research within internet technologies and the use of them. To answer how internet technologies, have and are being used in a household, it was important to look at the existing information. There was much research related to the different technologies and smart homes. Since this is an area in high development, articles, papers and announcements of new products are constantly being written.

The search for data has been done in many different databases (ORIA, Web of Science, etc.) with search words related to Internet of Things, Smart Homes, Smart House, RFID, sensors, and other technologies. Because of the fast development and need for information on products and projects, the whole of internet has been included in our search for literature. Google search, producer’s websites, books, web articles and similar have been used as sources in the thesis. We have tried to mainly search for primary sources, but also use secondary sources as many products aren’t addressed detailed enough at the primary source. We have chosen to include literature in multiple languages. Most literature within this area is written in English since technology is a global phenomenon affecting all.

### 3.1.2 Indirect observation

Observation here means the registration of data through scientific instruments. Observation can also refer to the data that has been collected while the research has been going on (Wikipedia, 2016e). When doing indirect observation, you use the information given by secondary sources – relying on the observations from them. Since technology and products are moving at a fast pace, we have to observe and collect data while looking at existing research and writing the thesis. Indirect observation has been done to try and capture the changes and find something new. The secondary sources are in this case information from producers and web articles announcing new developments and products.

## 3.2 Validity

Validity says something about how well, or relevant, the data represents the researched phenomenon. Does the data collected help answer the research question or not? The goal is high validity (Johannessen et al., 2011). If the data measures something else than what we want to explore, they aren’t usable to give an answer to the research question.

Validity is classified in internal validity and external validity. Internal validity says something about how the researcher has to control variables that can affect the result. External validity says something about the generalization of the study – in what grade it can be generalized in other contexts (Thomas, Silverman, & Nelson, 2005).

The validity of the literature gathered is somewhat difficult to assess – both the internal and external. Most research used in this thesis is qualitative. It is research that tells us about phenomena’s in the text; what is happening, who is working on what, what is being developed? It is also research telling us the same about the past. We believe that the external validity is high because of how the information can be transferred into other contexts. This is a general study of the development and use of smart homes. We cannot exclude that no research has methodically faults, and therefore cannot say that all research is correct. The official research that has been published are believed to have higher validity than the data collected from web-pages. Still, as the data collected is relevant and helps to our purpose in this paper, we believe that the validity is somewhat high.

## 3.3 Reliability

Reliability in this context tells us how reliable the data is. Has the data collected been affected by the way the collecting of it was completed? (Johannessen et. al., 2011). The goal is to have high reliability, meaning that the research can be re-done and would show the same results (Halvorsen, 1993). As with validity, reliability can be divided into internal and external. The external reliability says something about the content of the data and to what degree the study can be verified. Internal reliability is the degree of agreement on the results amongst researchers doing reliability tests on the conducted research.

The reliability of this paper could be somewhat varied. If the same literature is used in a verifying of the thesis, the literature used as data should show the same findings. Published research will not be changed unless revised editions are published. This means that the reliability of the published literature will be high. Since technology and product development is constantly moving forward, the reliability could be varied. New and updated literature will be put out, but as told; if the same literature is used in verifying tests – the data should be the same.

## 3.4 Error sources

There are many things that can lead to errors and error sources leads to fallacies. In this study, we believe error sources could mainly come from expectations, validity, reliability and interpretation. The data used and how we have collected it, is driven from our expectations and search for specific areas we want to look at. Our interpretation and understanding of the data cannot be assessed without re-testing the literature later. Error sources can therefore happen in our interpretation and understanding. Most reports on attitudes and wants of the smart home, in addition to health reports, comes from the United States and Canada. We say that we focus on the western world, but cannot say that all data from North America holds for everyone else. Testing in a technology market can be difficult because the market always changes. To reduce the chance of wrong information we tried to not use any literature older than six months in the analysis.

# 4. Analysis

In this chapter we look at the current developments within smart homes. We look at the smart home systems and companies of today and the use of smart homes. Developments within the four main areas are presented; security, energy, health and home automation. Lastly, the costs of -, and attitudes towards smart homes are analyzed.

## 4.1 Smart home developments

### 4.1.1 Smart home producers and systems

The main smart home suppliers can be separated in two groups: 1) companies that deliver a complete smart home system and 2) companies that deliver a smart home hub with the possibility of adding products from themselves or partners. Smartly (Smartly, 2016d), Family@Home (GreenPeak, 2015) are two of the complete smart home systems, delivered by Lyse and GreenPeak. Most companies have focused on making a smart hub with additional devices. Some of them are Amazon with their Echo (Amazon, 2016b; Kastrenakes, 2015), Samsung's SmartThings (Gibbs, 2015a), Lowe's Iris (Higginbotham, 2015; Lowe's, 2016), and the newly launched Stavanger-based Futurehome (Futurehome, 2016).

Amongst the most popular technology protocols that smart home systems and smart devices are built on are Z-wave, Zigbee, KNX, x10, C-Bus, Bluetooth, Wi-Fi and Insteon (Wikipedia, 2016b). Z-wave is the largest of protocols, and are amongst the alliances that have been created to strengthen the position as a standard (Alliance, 2016). Interoperability between standards are still low, forcing companies to build more open networks. ETSI is one of the standardization organizations working on smart home standards (ETSI, 2016a).

### 4.1.2 Penetration of smart homes

Worldwide, smart home systems and appliances have entered 0,77% of households in 2016 (Digital Market Outlook, 2015a). The annual growth rate of the smart home market is at 28,78% until 2020, with an expectancy to reach a penetration of 2,97% - resulting in 44,1 million active households that are smart worldwide.

In the 2015 report about smart home from Icontrol Networks, shows that security is still dominating the smart home (Icontrol, 2015). 90% of consumers says that security is the top reason to invest in a smart home system. Others ranking high are energy efficiency and automation. Icontrol found that the devices that dominates the consumers list for most desired are self-adjusting thermostats (72%), doors that can be remotely locked (71%), a master remote control for all household activities (68%), automatic adjustable outdoor lighting (65%) and home monitoring camera's (65%). Smart homes have a positive outlook with 50% of the people in the reports saying that they plan to buy a minimum of one smart home product in 2016. Icontrol found that consumers want simple and easy-to-use products that solve everyday problems. And 60% of consumers wished that the devices worked better together (Icontrol, 2015). Intel finds similar numbers in their report (Intel, 2015). The participants expect the home to be as easy to install as cable tv, and 86% wants a single device that can manage all devices connected to the smart system.

## 4.2 Developments in the main areas

Major trends within the smart home market are voice controlled interfaces, the debut of real intelligence and learning, delivery of complete smart home systems and partnership between companies. There is less competition for the technology, pushing companies into alliances and partnerships “just in case”, to not miss anything (Taylor, 2016). Details and examples of developments and the trends will talked about in sections security, energy, health and home automation.

### 4.2.1 Security

Until now, security has been the largest sales segment within smart homes systems and appliances. The revenue in the security segment will be about 3 050,3 million USD in 2016, and is expected to have an annual growth rate of almost 30% until 2020 (Digital Market Outlook, 2015a). Most of the revenue from security in smart homes comes from the United States, followed by Japan, Germany, China and the United Kingdom. Smart home security is today used in 0,53% of households in the world, and is expected to grow to about 2% by 2020. This counts for 30,9 million households.

The development within security is less drastic, but shows some new features and gadgets. Continuing the key-less locking systems, the smart lock maker Latch is focusing in on luxury homes (Keating, 2016). The sleek keypad has Touch ID where the users enter a passcode to open the lock. In addition, an app can open the door for you, and you can share the app with your nearest.

Within the area of surveillance, Netatmo have recently presented a revolutionary security camera that detects and recognizes people, cars and animals (Syrkett, 2016). The camera can differ between the three, and sends out precise alerts when something happens outside of the home (Netatmo, 2016). In 2014, Nest bought and improved the wireless security camera Dropcam. It is now been renamed and revamped – introducing the Nest Cam. The Nest Cam has higher video definition, zoom, night vision, and the important two-way communication. A unique part of the camera is that it has sound and motion-detection, and can also be mounted on multiple angles and appliances because of its magnetic base (Kelly, 2015). Other surveillance systems, as Elgato and Smanos, have a focus on increased camera resolution and more functionality in dark rooms and at night (Syrkett, 2016).

In addition to the Nest Cam, Nest also has a smoke alarm called Nest Protect. Roost has now launched a competing smoke alarm that notifies the owner through the phone when danger is detected. It can also distinguish between smoke, fire, natural gas and carbon monoxide (Lanaria, 2016a).

Lyse is partnering with NorDan to deliver smart doors and windows to their smart home solution Smartly (Smartly, 2016c). You can not only remotely lock or close the doors from your phone, and it also alerts you if the window is open. The window itself knows whether it's open, closed or in aeration-model.

Zenbo is a robot assistant for the smart home that Asus showcased in May of 2016 (Ungureanu, 2016a). The robot connects to smart home devices as both the smart hub and the user interface that usually is via an app. This means that you can see who’s ringing at the door and unlock the door via the robot. Zenbo is an overall smart home assistant. It offers assistance for all areas of a smart home.

### 4.2.2 Energy

Digital Market Outlook’s (2015a) report on Smart Homes shows that the Energy Management segments will reach a revenue of 1 961 million USD in 2016, and have an annual growth rate of 28,84% until 2020. Today, 0,27% of worldwide households use energy saving products and services. This is expected to grow to 1,32% in 2020 – an amount of 19,7 million households. Like with the security segment, the implementation of Energy Management products is most popular so far in the United States, Japan, Germany, China and the United Kingdom.

Systems, products and services in the energy segment in smart homes have the goal of being energy saving (Digital Market Outlook, 2015a). They manage and try to reduce the energy use within the home. Amazon launched the Amazon Echo speaker in late 2015 (Mamiit, 2016). Amazon Echo started as a device that you could ask for help, and would do tasks via voice commands. The speaker is always listening, and can catch commands from all corners of a room. The assistant carrying out the commands is Alexa. In the last year, Amazon has greatly expanded the product range that can connect with Echo. It can connect across producers and smart devices. Samsung, Philips, Wemo and Insteon and Wink all deliver smart devices and systems connectable with Echo (Amazon, 2016a), and the list of partners are continuing to grow. Echo and Alexa has become the basis for Amazon's smart home. Much of the focus of Amazon's smart home is on energy-solutions, controlling light, outlets, switches and thermostats. By giving Alexa a command, lights can be dimmed and turned on/off. The same can be done with temperatures, by setting an exact temperature or by adding/subtracting a number to the current temperature (Mamiit, 2016). In addition, appliances plugged into the smart outlets or switches can be turned on or off by the voice command. HomeKit, Apple's automation framework, rolled out in 2015 and consists of several different products from thermostats, to light controls, to smart outlets (Etherington, 2016). The Elgato Eve in a box with sensors that monitor temperature, humidity, air quality and air pressure both in- and outside. The sensors also checks if doors and windows are open or closed, and what's draining power so that it can be switched off. The ecobee3 is a smart thermostat who remotely monitors and adjusts the temperature in several rooms at the same time (Ecobee, 2016). Its goal is to save energy and maximize the well-being. The ecobee3 can also connect to Amazon's Echo, making it voice controlled.

The Asus Zenbo robot (Ungureanu, 2016a) introduced in the security section also connects to lighting systems, air conditioners and thermostats. The robot moves around in the house, responds to voice commands, and can be controlled by the touchpad.

One of the greater revolutions within the energy segment of a smart home is the new learning thermostat. Nest launched the Nest Learning Thermostat in the spring of 2016. This is the second edition of the thermostat – now a smarter product (Gibbs, 2016b). The unique thing about Nest is that it learns your heating patterns. Warm in the morning, colder in the afternoon, and then warm again at night? Nest learns and adjust to your preferences and needs (Nest, 2016). It will also turn off central heating if it's not needed to save money. The thermostat can calculate heating time needed given both the weather and the outline of the home. If nobody's home, Nest will detect it through sensors or by tracking the locations of the smartphones connected to it. It will then adjust the temperature accordingly. A downside to it is that it cannot control the temperature room-by-room like some other smart thermostats. Nest can today connect to Amazon's Echo, and will be connected to more smart appliances in the future.

Energy savings aren't only done inside of the house by regulating and turning appliances on or off at the right time. Multiple companies are developing solar systems and home battery storage for lowering energy costs. Tesla launched the Powerwall (TeslaMotors, 2016) – a home battery charged on solar panels or your own powerline. The Powerwall is set to deliver extra energy to the home, making it possible for the home to operate without the powerline and creating a more sustainable home. In the spring of 2016, Nissan launched their xStorage (S. Passary, 2016). xStorage competes directly with Tesla's Powerwall. Nissan has differentiated themselves by using more environmentally friendly batteries, building on the sustainable solutions. Companies does not only deliver these solutions by themselves. Solar, Tesla, and Nest has partnered up to deliver a package to manage energy and reduce dependence on powerlines (Lambert, 2016). Together they will deliver solar panels, the Tesla Powerwall, smart electric water heaters and the Nest Learning Thermostat (Weaver, 2016).

### 4.2.3 Health

An Aging World's report showed that within the next decade, there will be more elderly people than children (National Institute on Aging, et al., 2011); Pilkington, 2009). The age span of humans has increased over the last decade, and people over the age of 65 are estimated to rise to 19,3% worldwide by 2050 (Gavrilov and Heuveline, 2003). Our aging population expects a longer and independent life in their own home. Smart home healthcare and assisted living is therefore in high growth to meet their expectations. Digital Market Outlook (2015a) defines the segment Ambient Assisted Living as products and services that are aimed to support independent living for elderly. This includes emergency alarms, accident detection, activity monitoring and related products for living support. In their report, fitness and wearables aren't included. Digital Market Outlook has estimated a worldwide revenue

of 508,5 million USD in 2016 (Digital Market Outlook, 2015a), with an annual growth rate of 49,56% to the year 2020. Today, 0,05% of households uses ambient assisted living products and services, but this is expected to reach 0,27% in 2020. This accumulates to 4,1 million active households worldwide. The top user countries are expected to be the same as within the other segments, with the Unites States on top. Research and Markets' report on the global smart home healthcare market operates with a compound annual growth rate of 38% from 2016-2022 (Research & Market, 2016). This growth number includes mobile health products. Research and Markets expects that fall prevention and detection-products and services will experience the fastest growth (Business Wire, 2016).

If elderly are going to live at home as long as possible, complete systems have to be in place to ensure safe and healthy living conditions. Several researches and companies are working making these systems. Ghayvat et al. (2015) have proposed the Wellness Sensor Networks. It is a protocol for the home environment that monitors appliances used, and the movement of the inhabitant in the home. Through this it predicts the wellness of the inhabitant. Silverlink has been proposed as a smart home health monitoring system. According to Chuang et al. (2016), Silverlink offers "(1) affordable and non-invasive home-based mobile health technologies for monitoring health-related motion and daily activities; (2) advanced mobile health analytics algorithms for fall detection, health status progression monitoring, and patient health anomaly detection and alert; and (3) a comprehensive patient health activity portal for reporting user activity and health status and for engaging with family members." Both Wellness Sensor Networks and Silverlink are in development and will be launched in the near future.

Lyse is one of the Norwegian companies delivering smart homes suited for welfare – both for elderly and people with disabilities and/or similar issues. Smartly Welfare controls lighting, heating and appliances through smart switches and tablets. The doors and gates are connected to the phones, and sensor are in place in the case of fire and leaks (Smartly, 2016d). Smartly also offers automatic doors and windows, and control of sunblinds. An important feature is that sensors can control lighting, heat and some appliances based on events and movements (Smartly, 2016b). Smartly is even adapted to i.e. the hearing impaired (Smartly, 2016a). The phone and tv has video-options for phoning, the mobile vibrates when the doorbell is rung, if the alarm is going off the lights in the house starts blinking, and the bed vibrates to let you know if the fire alarm is on. Sensors are put in place to notify of all important activities. Lyse is one in a growing list of companies delivering a smart home for welfare.

Smart homes enabled with telecare systems are providing specific assistance to support older or handicapped people living independently who are suffering from prolonged illness (Suryadevara and Mukhopadhyay 2015). Smart home telecare can provide facilities to overcome the transportation for organizing multidisciplinary care outside the hospital (Ching-Lung, Lin-Song et al. 2009) (Nourizadeh, Deroussent et al. 2009). Most of patients favors tele-consultations as it saves money as well as time (Rahimpour, Lovell et al. 2008).

In addition to complete systems for a welfare smart home, there are enormous amounts of individual smart products directed towards health at home. The Asus ZenBo assistant not only connects to the security and energy sections of the home. It has the ability to give voice reminders of i.e. appointments and medicine (Ungureanu, 2016a). If an accident happens in the home, Zenbo will notify family members and let you see what's going on through a camera in the robot. Zenbo has the ability to move, see, speak, hear, connect, learn and express emotion (Asus, 2016). In addition to help at home, it's like a companion.

The Amazon Echo and Alexa got a new feature called KidsMD in April of 2016 (A. Passary, 2016b). The idea is that parents can ask Echo and Alexa about their kid's health, and get formal medical information from the Boston Children's Hospital. It gives information on symptoms and basic guidance for home treatment of some illnesses. KidsMD is a unique to Echo and Alexa products.

The Pure Cool: 2.0 is a smart air purifier delivered by Dyson (Tiongco, 2016). The air purifier filters indoor air, and removes up to 99,97% of allergens and pollutants. It automatically monitors and reacts, and can be controlled through a smartphone where you can adjust the settings yourself.

### 4.2.4 Home automation

It is predicted that by 2020 there will be about 50 billion objects connected to the internet (Machado & Shah, 2016). This not only includes mobiles, PC's and tablets – but all devices that somehow is connected to the internet. Already this year, it's predicted that there will be 6,4 billion smart products in use (van der Meulen, 2015). Smart products are being developed and produced in fast rates.

Assistant robots for the smart home is a huge trend (Crowe, 2016; South China Morning Post, 2016). Asus' Zenbo has been mentioned previously as a new and revolutionary assistant at home. Amazon's Echo also goes under this category. Robot assistants for the smart home are becoming increasingly popular and are beginning to be rolled out on the market. Samsung introduced their version of a personal assistant in April of 2016 (Sem, 2016). The robot, named Otto, can listen and answer to questions. Like ZenBo, it can control lighting, temperature and security, and has a display that shows facial expressions. Otto has a camera with facial recognition, but it also works as a security camera – live streaming to your phone, tablet or pc. Buddy is another similar smart home assistant and companion (Blue Frog Robotics, 2016). Multiple companies are working on personal home assistants in form of small robots, but few are ready. Sony's Xperia Agent (Pierson, 2016; Waniata, 2016), Jibo (Jibo, 2016), Robotbase's Personal Robot (Autonomous, 2016; Nichols, 2016), FURO-I Home Robot by Future Robot (Future Robot, 2016; Nichols, 2016), Cubic (Cubic, 2016; Nichols, 2016) and Branto (Branto, 2016) are personal home assistant robots in development that aim to work in a smart environment. Google also launched their competitor to Echo this year. Google Home works as a control center for the home and can so far do most of same basis features that Echo does (Eadicicco, 2016).

Whirlpool are working on a complete smart kitchen (Whirlpool, 2016). At CES 2016, they launched a demo for their interactive kitchen solution. The kitchen is intelligent, connected, learns and adapts to the needs of the inhabitants of the home. Whirlpool's complete kitchen is still a work in progress, but parts of what could be in such a smart kitchen is already available. Whirlpool has released the Smart Front Control Range oven that communicates with Nest and has an app that lets you control start, temperature, cooking time and the stop (Thompson, 2016). Samsung (Taylor, 2016), Whirlpool (Crist, 2016) and LG (Ungureanu, 2016b) are all making smart fridges. Samsung's fridge has a touchscreen and camera making it able to see what's in the fridge while grocery shopping. You can even restock through a Mastercard app. Whirlpool and LG's fridges are similar. Other smart kitchen appliances include i.e. smart pans (Calpito, 2016) and smart dishwashers that integrates with Nest and Amazon Dash (Gebhart, 2016). Amazon Dash is a smart device making shopping easier (AmazonFresh, 2016). With it you can scan products at home and add them to a shopping lists ready for ordering. Your appliances can also connect and automatically order new supplies when needed.

With the amount of smart products developed, not all are as necessary as others, and some could be seen as a joke. Amongst them is the Smartress (Lanaria, 2016b) mattress that has a "lover detection system", meaning that it will alarm you if your partner is cheating on you – or just someone else using the bed. With an app showing a speedometer, intensity and impact per minute and tracking pressure point, it's proven itself as a real product. Other quirky, but fun products are smart light bulbs, Philips Hue Color is for example synchronized with movies and tv-shows in intensity and colors, and even offers voice control (A. Passary, 2016a). Sony launched a LED Light

Bulb Speaker that connects to the smartphone via Bluetooth or an NFC remote. The Misfit Bolt is a light bulb that changes colour via a Bluetooth connection, and can adjust temperature and brightness. The Elegato Avea can make your whole living room to a forest, and the Sengled Pulse bulb can create a surround-sound system via their speakers (A. Passary, 2016a).

## 4.3 Costs

It is said that owning a house is the largest expense in a homeowner's life (Klein, 2016). Most of the averages person's budget is housing costs, estimated to be 33% of their annual expenses. Smart home products promise to save time, energy and money for homeowners.

The price of a smart home installation varies on the size of the house and how advanced technology you want. SMARTech has conducted an analysis of the value the equipment and appliances related to the KNX/EIB systems which is shown in Table 1 (SMARTech, 2016). The given prices covers the costs of the whole system (cabling, system devices, design, electric switch cabinets, system start-up, and outlets) without actuators (lamps, radiators, window blinds, etc.). The price differs only a few percent from a traditional installation. Micro Matic Norge AS (2016) estimates the difference to be 10-15% higher investment cost if you are already going to install a new electrical system. The low difference between the prices is most likely due to the fact that both installations has to include cabling, outlets, etc. (SMARTech, 2016). If the plan is to build a whole new residential, the extra cost of a smart home installation is a very small part - estimated to be less than 1% of the total cost of the house. In return for the extra investment the residentials value is raised, which you can benefit from at a later sale.

In table 1 you'll find the prices for the different systems from SMARTech's analysis (SMARTech, 2016). The prices given for each system were calculated for a sample house with an area of 200sq m, covering the control of 40 light circuits, 16 window blinds and 8 independent heating zones - as well as design, equipment assembly, laying of the installation, and system configuration. If a system cannot forecast heating control, then the price includes electronic programmable thermostats.

| Basic Systems | | ‘Middle-class’ systems | | Advanced systems | |
|---|---|---|---|---|---|
| traditional installation | $ 13 656 | Dupline | $ 20 964 | Lutron | $ 26426 |
| Cardio | $ 20 444 | IDRA | $ 20 038 | Lonworks | $ 21419 |
| Hometronic | $ 22 657 | IHC | $ 18 600 | Crestron | $ 25497 |
| Luxor | $ 18 214 | LCN | $ 21 138 | KNX/EIB | $ 21880 |
| X10 | $ 17 729 | Xcomfort | $ 19 565 | | |

*Table 1: Cost-comparison of smart home systems (SMARTech, 2016)*[1]

Even basic system configuration provides comfort that cannot be matched by traditional installations (SMARTech, 2016). Many can be blown away by all the options and equipment you can get in a smart home, and end up with a high input price (Micro Matic Norge AS, 2016). Focusing on practical solutions, you’ll get a smart home you will be satisfied with at a reasonable price. This also makes it easy to add features and equipment later. Thanks to energy savings, the cost of the system pays itself back within a few years.

## 4.4 Attitudes towards a smart home

Early users of smart home products were a small group of tech fanatics (Klein, 2016). However, the demographic of smart home users is massively expanding beyond just 30 to 40-year-olds in single family homes. A survey done by Icontrol Networks the spring of 2015 showed that there was a rise in the in the level of excitement about the smart home from the previous year. With 79% of millennials and 76% of parents leading the pack (Icontrol, 2015), and 50% of the overall population excited about the technology. A survey ordered by Intel Corporation and conducted by TNS reveals that 7 in 10 Americans are sure that smart homes will be as commonplace as smartphones within 10 years (Intel, 2016). As many as 50% of people say that they plan to buy at least one smart home product already within the next year (Icontrol, 2015). Intel Corporations survey shows that more than half of the survey respondents would blame manufactures if their device failed (Intel, 2016), leaving a narrow margin for error. System reboots, product glitches, system updates and connection failure were among top concerns.

[1] *Exchange 1 EUR = 1,2533 USD  (DNB, 2016)

### 4.4.1 Security

From Gezen's (2016) survey a notable result is that millennials are more open to the idea of selling their private data compared to other generations that were sampled. In total, 72% of consumers fear their personal information may get stolen by using smart home products. Consumers say they are more concerned about this than they are about the cost of the technology (Klein, 2016). In Intels survey Architecting the Future of the Smart Home 2025, 82% of American respondents agree that integrated security is a priority for living in a smart home (Intel, 2016), and that all smart devices should be secured through a single incorporated security package. However, 66% of the respondents have similarly expressed concern over potential security threats and cyber attracts (Gezen, 2016). Further, 75% of the respondents says that remembering a number of password to manage their smart homes makes them feel nervous. The survey suggest that more users prefer biometric security; 54% are comfortable with fingerprints, 46% are comfortable with voice recognition, and 42% are comfortable with retinal scans. Also, one in 10 men would even employ a robotic guard to secure their home in the future (Intel, 2016). Despite cybersecurity fears, 75% are still willing to risk their personal data in reward of the smart home technology, because they believe that it will offer them superior benefits such as reduced electricity bills, lower heating and cooling costs, and a greener home (Gezen, 2016).

### 4.4.2 Energy

Parks Associates *360 View: Energy Management, Smart home and Utility Programs* - consumer research study of 10 000 broadband households - revealed that 36% of consumers would participate in an energy program offering a free product (Kreber et al., 2016). In the Parks Associates (2016) research report - The Evolution of Home Energy Management - 62% of U.S broadband households strongly believe that saving energy and lowering utility bills are important, and 30% strongly believe that being "green" is important. However low consumer awareness and the concerns related to the cost of products and services could delay widespread adoption of home energy management. Icontrol's survey showed that 70% are excited about the potential cost savings from energy efficiency and monitoring (Icontrol, 2015). Consumers aged 55+ expressed the most excitement around the cost saving benefit. However in Parks Associates survey it was revealed that 44% of broadband households are concerned about incurring hidden cost with energy management programs (Parks Associates, 2016). The report also says that 83% of the respondents doesn't even know the price they are paying for electricity.

### 4.4.3 Health

In Demiris et al. (2004) pilot study confirm that senior citizen are positive towards technology and are willing to accept the installation of sensors and devices in their homes. Collings et. al.’s (1992) findings in their report “Elderly people in a new world: attitudes to advanced communications technologies” shows that there is a lack of evidence for a positive relationship between age and technophobia. The pilot study’s analysis revealed different categories where smart home technologies would benefit older adults living at home (Demiris et al., 2004). Categories such as emergency help, assistance with hearing and visual impairment, prevention and detection of falls, monitoring of physical parameters, etc. Their main concerns were privacy violation, lack of human responders, user friendly devices and the need for training tailored to older learners. Three categories were identified in relation to the installation of the technology: (a) wearables technology, (b) local installation of devices and sensors fixed within the residence and (c) a remote operation with networks operating in a bigger community. Participants did not object to any of object of these types of installations, and would accept any such device if it were to improve their life or prevent accidents.

Smart home technology has the potential to help seniors live happier, easier, and can be a great resource for family members to keep an eye on their aging parents (Icontrol, 2015). Both of which are scenarios consumers are starting to notice. In Icontrol Networks survey, 72 % of aged 25-34 and 74% of those identified as parents said that they would sleep better at night if their parents or grandparents has a smart home (Icontrol, 2015). That’s nearly half (49%) of all the respondents.

### 4.4.4 Home automation

U.S. consumers aged 25-34 expresses a high level of excitement around the benefits of greater productivity and ability to manage work-life balance (Icontrol, 2015), 40% compared to 23% of consumers overall. They are also excited about making it easier to enjoy music, movies and web surfing anywhere in the house, with 26% compared to 18% of consumers overall. Help with tasks as shopping lists and minor repairs had 24% of the younger consumers excited compared to 18% overall. The last benefit the aged 25-34 were most excited about were more interactive features that helps them connect with other people, with 21% compared to 13% of consumers overall.

A recent Intel Security survey, Internet of Things (IoT) and the Smart Home survey, shows that 54% of their global respondents are willing to share personal data from their smart home appliances in exchange for cash (Gezen, 2016), while 70% are satisfied with trading data with for coupons or some form of discount.

# 5. Discussion

In this chapter the findings from the analysis will be discussed with the theoretical background. We do this by looking at the users of smart home; who can use it, who uses smart homes today, and who will use it in the future. We also discuss the need of a smart home through looking at benefits and disadvantages. Finally, we discuss the future of smart homes.

## 5.1 Smart home users

Smart homes and smart devices to use in the home are found to be mostly used by early adopters of new technology. These are the start drivers proving the benefits of the smart home and its features. But technophiles aren’t the only users of smart home products. Icontrol’s report showed that 50% of the respondents planned to buy a minimum of one smart home product in 2016. Realistically, not all respondents in the surveys can be early adopters, implying that smart devices for the home has reached the regular home owner. 0,77% of households worldwide already has one or more devices in their resident to make it a smarter home. The wide range of products offered shows that we are interested. Companies do not make products without having faith and the proof of a market for it. They see the future of smart systems in every home, and are jumping on the bandwagon to position themselves.

### 5.1.1 Who can use a smart home?

The definition of a smart home is broad, and with only a few smart devices you can make your house smarter. Many products are widely available for commercial use, making it possible for everyone to have a smarter home. We see that smart homes are simple to use, and provides an added feeling of comfort and security. A system is set up via a hub, and from there on you connect the smart products you want. Lighting, temperature, security, and automation of much used appliances all have the possibility to make life easier. Even though many of the functions mostly used today does not take much time to fix, it’s the feeling of saving time and having someone doing it for you that adds comfort. Installing a smart system does not have to be expensive. If you only want a few features and devices, the cost is lower. Installing a complete system in a house can cost you a larger sum, but is estimated to be 10-15% more if you’re already changing the existing electrical system. A smart home is for everyone.

Smart homes originally had a strong focus on elderly as a target audience. As the number of older people living at home grow because of the lack of care home places for them, home automation is particularly useful. Through smart home solutions, their needs can be met. Monitoring all activities through mainly sensors and some cameras allows health personnel to keep track of the state of the resident. An Ambient Assisted Living (AAL) environment detects changes from the daily routines of the person(s). If the changes are significant, health personnel will be able to step in in timely fashion. The homes can be set up to a 24 hour alarm central, giving the added safety feeling for both the individuals and family. The resident can even use voice control to manage the home. If the individual has i.e. dementia, schedules can be programmed to help with a routines from day to day. With assistant robots that helps, learns and communicates, tasks normally done by nurses and home helps can be left to intelligent robots. All in all, older people can stay at home and still have a certain quality of life, while the health institutions can save money they need for others.

Smart homes are also improving the quality of life for disabled people. Depending on the disability, the home can be tailored to the resident’s needs. A house can automatically do what you normally cannot do or comprehend as a disabled. Making the home smart gives can give the feeling of both independence and belonging. Like Lyse advertises for their smart home setup; a paralyzed man from stomach and down can live alone because of practical solutions fitted to the person's needs. The doors can automatically be opened and closed, lights, heating, etc. can be controlled via the interface, an alarm central is close, and time in general is saved because of the easy use via one main control. A hearing impaired person can have sensors fitted to alarm him of all situations needed, and video makes it possible to communicate easier. The solutions suppliers comes with are smart enough for welfare in multiple areas.

The progress within wearable sensors for illnesses are adding to the benefits of a smart home. These sensors monitor the situation, and continuously updates doctors and other health personnel of the status of the individual. Everything from a small fever to a serious issue within the body can be monitored with sensors. When negative changes are identified, the patient can be called in to checks. This way, hospitals and doctors save beds, time and money.

### 5.1.2 Smart home users of the future

We believe that smart homes will be greatly affected by the increase of elderly and the decrease of newborns. Within this decade, it is expected that older people will surpass the number of children.

With more older than young people, the health system will experience an enormous pressure as there's not enough room for all in need. Already today, you see the competition of care home places. Reports shows that the staff do not have the capacity to meet the needs of the elderly. The lack of capacity decreases the quality of care, and over half of the respondents in a national survey in Norway says that the needs aren't met by the staff. Home automation can therefore be very useful for elderly to better the health system and their own life. Having an elderly at home as long as possible can decrease the costs of stately institutions, and with proper setup at home you can drastically improve the quality of the individual. Smart homes have been researched and tested for elderly for many years. Companies are already delivering welfare solutions of smart homes for this generation, and we believe that the progress of these solutions will continue further on. With the positive attitudes shown towards smart homes from elderly, implementation of the new technology should be easier. As previously discussed, smart homes are also ideal for people with disablements or illnesses wanting a better quality of life where they can manage themselves in a greater way. The health sector in general has great benefits of the technology and will take use of smart homes. With RFID and sensors fitted both in the body and the house, independence is enabled at the same time as the health personnel have control over the status quo.

Reports shows that 50% of the population are excited about the new technology. As many as 7 out of 10 Americans thinks that smart home products will be as common as smartphones already within 10 years. The discovered excitement and willingness to buy implies that smart homes will be used by everyone that can afford it, and not only within certain sectors. We believe that a smart home system will be the norm in the future – that new homes will come with basic packages pre-installed in a few decades. The expected growth for the next years supports this. Consumers see cost benefits of reducing electricity bills, and an easier life. They have the choice of a complete system or a partial system, and are even willing to risk parts of privacy for a more comfortable and easier life. Privacy has been an issue within the development of connected products, but an increasing willingness to risk parts of it shows that smart homes are attractive for all.

## 5.2 Is a smart home needed?

The smart home market is growing rapidly making products cheaper and more available for the individual user. The more providers there are, the higher the competition for producers. This means that the expected quality of the products is higher, and customers can choose to their preferences; quality, guaranty, life expectancy, price, etc. An issue for the user is to choose the standard that is most compatible with their needs. The producers issue is that their products with WSP needs a unique IP address, which is limited.

Interoperability between standards are still low, making it problematic for devices to communicate over a mass of wireless standards. When there is no compatibility among the different standards it means that your power meter from one company might not be able to control a device from another company. The hub could be unable to dim your lights, or the smoke alarm could refuse to turn off your own in case fire, without extra equipment that bridges the platforms. Another obstacle that can appear when there isn’t one standard is that monitoring alarm centers can have problems connecting their chosen camera with the customer of their monitoring system. The lack of common standards forces product developers to make more open and accessible products. Using standards allows for easier interoperation in M2M systems and facilities using mass-produced, standard-compliant equipment. This makes implementation less expensive, simpler and quicker. When products only fit to one standard, the producer excludes all users of a different standard. If everyone had the same standard or every product could connect to every standard, the users wouldn’t be restricted when choosing products. To minimize the gap between standards and product compatibility, the network rivalry, we feel, needs to end and the development of standards like WIFI and Bluetooth gets further developed.

As years go by, technologies becomes less foreign with an increasing amount of people using smart products. Research shows that 50% of overall population are excited the smart home technology. But still, technology is still an untouched area for many - especially the eldest generation. For them to get the benefit of all helping products offered, they need to learn to use and understand the products. This can be a challenge for some, but many are willing to learn if it can help them prevent accidents. Training can be tailored for those who is not used to technology. For the people not willing to learn, a solution could be devices that functions as self-controlled sensors that doesn’t have to be operated or controlled by the user. As the parent-generation of today reaches senior citizenship, the problem of resistance of technology could be minimized as most of these are exposed and actively participating in today’s technological world.

49% of respondents said that they would sleep better at night if their parents or grandparents had a smart home. Also research show that 82% of American respondents agree that integrated security is a priority in a smart home. We believe that one of the reasons for such a high agreement among Americans can be their high crime rate. One of the reasons people feel safer in a smart house is because of the extensive security systems available. These systems raises the security level of the home. 66% of the respondents expressed concern over potential security threats and cyber attracts. Smart, connected products has a need for robust security management to protect the data flowing to, from, and between products. This will require new authentication processes, protections against hackers for both product data and customer data, secure storage of product data, definition and control of access rights, and protections for the products themselves from unauthorized use.

72% of consumers fear their personal information may get stolen by using smart home products. Since there is high concern for hacking, consumers should demand more from companies in terms of protecting their private information, like security deals protecting data and devices from illegal intruders. We’ve seen how automated locking, cars, and even baby monitors have been easily hacked - indicating that these are not isolated events. A problem with security issues is that they grow exponentially worse as more devices are connected to the internet. An example where people’s safety is threatened by hacking is when a car is hacked and control is taken over by someone with bad intent. Since the Gezen’s survey suggest more users prefer biometric security, this can be one solution to making security systems stronger. Especially when 75% of the respondents are nervous about remembering a number of passwords. Senior citizens have also expressed a concern about being watched as a violation of their privacy, i.e. being watched by a control station. A solution to this is to have the cameras showing only shadows, so specific people are recognized by the right people but not anyone else. This still makes them able to help in emergencies, and seniors would still have more privacy. When security features are increased and implemented, it is essential to effectively communicate how secure the producers products are to convert nervous consumers into buyers.

Creating scenes and schedules can improve your lifestyle and help you save energy and money without a change in your daily routine. Software embedded in products enables users to control and personalize their interaction with the product in many ways. Connected products can be controlled through remote commands or algorithms that are built into the device or reside in the product cloud. For example, users can adjust their Philips Lighting hue lightbulbs via the smartphone - turning them on and off, programming them to blink red if an intruder is detected, or dimming them slowly at night. Controls like these can help manage your energy level by controlling it to use minimal energy in peak hours or automatic turning off lights when you’re not home. By getting more people to control their energy use the better it is for the planet, and for our own benefit of saving money. Giving people rewards you're not using extra energy in peak hours can be an incentive.

It seems that senior citizens don't have a problem being monitored as long as it were to improve their life or prevent accidents. Smart, connected products enabled the comprehensive monitoring of a product's condition, operation, and external environment through sensors and external data sources. Using data, a product can alert users or others to change in circumstances or performance. In cases where medical devices are involved, monitoring is a core element of value creation. For example, if you have a pacemaker implanted it monitors your heart; if it is going too slow or stopping, it will send a little electricity. Monitoring allows companies and customers to track a product's operating characteristics and history and to better understand how the product is actually used. With close monitoring companies get the benefits of knowing how the product is used and handled after sale, which can help them improve products. Monitoring can help with detecting device failures. This is very important since research shows that more than half of consumers say they will blame the producer if there is something wrong. If the companies can monitor and register every time the product glitches or a connection is lost, the company know they need to work on it. The more device failures are prevented the better. Monitoring also helps the product users by getting notifications or alert if something is wrong or changing. For example, if your fridge is running low on milk, your fridge can notify you so you'll remember to buy milk, or you can check fridge status when you're already in the store. An issue arises if there is a device failure when you plan on using the function. Let's say you're at work and plan to open the door for the plumber. If the app doesn't work, you need to use extra time to get home and open the manually and calling to get the function fixed. This can cost you both time and money - two things you normally will save with these kinds of products.

U.S. consumers aged 25-34 expresses a high level of excitement around the benefits of greater productivity and ability to manage work-life, 40% compared to 23% of consumers overall. A combination of control and monitoring will allow smart, connected products to achieve a previously unattainable level of autonomy. At the simplest level is autonomous product operation like that of the iRobot Roomba, a vacuum cleaner that uses sensors and software to scan and clean floors in rooms with different layouts, with you only turning it on. More-sophisticated products are able to learn about their environment, self-diagnose their own service needs, and adapt to user's' preferences. Autonomy not only can reduce the need for operators but can improve safety in dangerous environments and facilitate operation in remote locations. If you have an autonomous robot assistant it can easily help in emergency situations. Or if you are unable to call the emergency number due to vision loss or loss of tactile senses. In some cases, this can even save the life of the user. For example, if the user is home alone and has a heart attack. A big issue can a robot wrongly programmed that does not respond to commands.

62% of U.S broadband households strongly believe that saving energy and lowering utility bills are important, and 30% strongly believe that being “green” is important. 70 % says they are excited about the potential cost saving from energy efficiency. With smart products there are lots of ways you can reduce cost. You pay less for your energy bill then before, you can check your fridge for groceries before you buy to avoid double stocking and having to throw away food. An option for patients and the health sector to save time and money via smart home telecare - providing services to overcome the transportation for organizing multidisciplinary care outside of the hospital. If smart homes make elderly people live at home longer the government will save money by not needing to provide a nursing home or a retirement home. Still consumers are concerned about hidden cost that can arise unexpectedly, like maintenance costs. Solutions to this concern can be long warranties or a fixed yearly cost for service on system and products. Having a fully integrated smart house solution will rise the value of the house, apartment or cabin.

## 5.3 The future

Internet of Things is described as a backbone of smart homes. The future of object-to-object communication is somewhat open and unknown, but we can assume that new applications will arise as the enabling technology advances - especially within sensor technology. We believe that it will be important to focus on the development of RFID wirelessly connected. The tags are in need of a longer range and battery time, as well as improved networks. As individual companies, corporate ecosystems, cities, and regional governments adds more RFID technology, the systems will be linked. We see that IoT has a huge impact in every aspect. When it comes to healthcare and saving life we believe that the IoT can make an enormous difference by furthering development of implantable sensors. The overall sophistication of sensors and intelligence capabilities is certain to increase dramatically. Once a large critical mass of technology networks of the enabling technologies in IoT is achieved, existing on the outside of the system will become inconvenient, or even impossible. For IoT to reach its full potential, universal standards for technologies, systems and architecture has to be in place.

The smart home industry is growing as the technologies enabling smart homes and smart devices continue to advance. Parallel with technology, acceptance grows. The attitudes towards a smart home are already positive. People are showing concerns of their privacy and the security of data, but are overall very positive. The systems in smart homes today are highly developed, but there is still enormous areas to explore. Robots and Artificial Intelligence are future possibilities of smart homes, and we're already starting to see robots as smart home personal assistants. We expect that the smart home is as well-integrated in the future that it's the norm having a smart home system. In addition, smart homes have great possibilities within the areas of health sector.

For smart homes to reach its potential and being a norm, we believe that it can only happen if there are advancements made in privacy & security, failure rates and standardizations. People are worried of their own privacy, and need to be assured that the privacy is as best held as possible. This is done by improving the protocols, laws and system of security and data. By minimizing device failure rates, producers can build trust. Finally, more standardizations has to be in place. Standardizations secure protocols for developing technology and protocols, as well as insuring interoperability.

# 6. Conclusion

The aim of the thesis has been to examine the developments of smart homes and how it affects us as consumers. From the research, we have the following findings;

The smart home industry is growing. Smart home systems worldwide have in 2016 entered 0,77% of households, and is expected to grow to 2,97% by 2020 - about 44,1 million active smart households worldwide. Both new and existing companies are entering the smart home market, creating either complete systems or smart hubs with possibilities for additional smart devices to connect to the system. To position and gain advantages, companies are entering alliances.

Security is still dominating, followed by energy efficiency and home automation. New developments within these areas include outdoor security cameras able to differ between humans, animal and cars, learning systems, and personal assistant robots for the smart home. Voice activation is becoming increasingly available in the smart home system.

We have identified smart homes as homes for everyone. The early adopters was technophiles, and smart homes have now reached the common home owner. The attitudes towards the technology and possibilities are overall positive. 50% say that they are intending to buy a minimum of one smart home device during 2016. The future smart home users will be everyone able afford it, as smart homes comes at a wide range of prices depending on the installation. There are great future opportunities, especially within the health sector. We believe that a smart homes can benefit elderly by enabling them to live at home and more independently for a longer time. This is especially important as the amount of elderly are outgrowing children. Smart homes and healthcare is combined through continuous monitoring via sensors that converts data into tasks helping the individual. The sensors can be in the house itself, in products, and inside the human. Home automation can lead to an easier life.

We have identified three major issue areas that has to be properly addresses and found solutions for before the complete smart home to be fully adopted; privacy, security and standardizations. The right to privacy is deep within humans. Consumers are showing a willingness of risking some privacy for the benefits a smart home gives, but are still concerned of the privacy ramifications of smart systems. As many as 72% of the consumers fear that their personal information could get stolen via smart home devices. Security of the home and the data are equally important. To secure the data, and thus the privacy of the user's, laws and more extensive security systems have to be in place. A person has to be able to trust that data about them doesn’t end up in the hands of anyone other than it is meant to. Lastly, more standards for technology and protocols have to be in place. There are standards for many areas of technology, but the newer are lacking protocols within many areas - both within IoT and Smart Homes.

Overall, the areas of smart home has great opportunities and benefits for a use today and the future. The smart home industry faces issues that have to be addressed, but can potentially overcome large parts of them, making the smart home even more attractive. Positive attitudes towards a smarter and easier life pushed the technology adoption. The smart home will be the norm. A smarter home might just be the smarter choice.

# 7. References

Alliance, Z.-W. (2016). Alliance Overview. Retrieved 08.06, 2016, from http://z-wavealliance.org/z-wave-alliance-overview/

Alonso, I. G., Fernandez, M., Maestre, J., & Fuente, M. D. P. A. G. (2011). Service Robotics Fwithin the Digital Home. Dordrecht: Springer.

Amazon (2016a). Alexa Smart Home. Retrieved 07.06, 2016, from https://www.amazon.com/b?node=13575751011.

Amazon (2016b). Amazon Echo. Retrieved 08.06, 2016, from http://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-with-WiFi-Alexa/dp/B00X4WHP5E.

AmazonFresh (2016). Amazon Dash. Retrieved 08.06, 2016, from https://fresh.amazon.com/dash/.

Ammari, H. M. (2013). *Art of Wireless Sensor Networks : Volume 2: Advanced Topics and Applications*. Berlin/Heidelberg: Springer.

Armstrong, G. (2009). Addicted to healthcare - could alarming cost bankrupt us?. Retrieved 09.05.2016, from http://www.stuff.co.nz/national/health/2779009/Addicted-to-healthcare-could-alarming-cost-bankrupt-us.

Asus (2016). Zenbo - Your smart little companion. Retrieved 08.06, 2016, from https://zenbo.asus.com/.

Atzori, L., Iera, A., & Morabito, G. (2010). The internet of things: A survey. *Computer networks*, *54*(15), 2787-2805.

Autonomous (2016). Personal Robot. Retrieved 08.06, 2016, from https://www.autonomous.ai/personal-robot.

Bergen, M. (2016). "With $340 million in revenue, Nest is underperforming, and its future at Google is at risk." Retrieved 31.05.2016, from http://www.recode.net/2016/3/30/11587388/nest-2015-sales-budget.

Berners-Lee, T. and M. Fischetti (2000). *Weaving the Web : the past, present and future of the World Wide Web by its inventor.* London, Texere.

Blue Frog Robotics (2016). Buddy the first companion robot. Retrieved 08.06, 2016, from http://www.bluefrogrobotics.com/en/buddy/.

Branto (2016). Branto. Retrieved 08.06, 2016, from http://branto.co/#security.

Business Wire (2016, 07.06.2016). Global Smart Home Healthcare Market Forecast to 2022 - Key Players are Siemens AG, General Electric Company & Essence Group - Research and Markets. Retrieved 08.06, 2016, from http://www.businesswire.com/news/home/20160607005845/en/Global-Smart-Home-Healthcare-Market-Forecast-2022.

Business Dictionary. (2016). Sensor. Retrieved 09.05.16, from http://www.businessdictionary.com/definition/sensor.html

Calpito, D. (2016). Pantelligent Is A Smart Frying Pan That Talks To Your Smartphone So You Don't Burn What You’re Cooking. Retrieved 07.06, 2016, from http://www.techtimes.com/articles/135239/20160223/pantelligent-is-a-smart-frying-pan-that-talks-to-your-smartphone-so-you-dont-burn-what-youre-cooking.htm.

Carlo Gavazzi AS (2016). En Smart-House hverdag. Retrieved 27.05.2016, from http://www.smartbuilding.no/phone/en-smarthouse-hverdag.html.

CDC (2016). Chronic Disease Prevention and Health Promotion. Retrieved 30.05.2016, from http://www.cdc.gov/chronicdisease/overview/.

CES (2016). About Us. Retrieved 11.06.2016, from https://www.ces.tech/about-us.

Chan, M., Estève, D., Escriba, C., & Campo, E. (2008). A review of smart homes—Present state and future challenges. *Computer Methods and Programs in Biomedicine, 91*(1), 55-81. doi:10.1016/j.cmpb.2008.02.001

Chawla, V. H., Dong Sam. (2007). An Overview of Passive RFID. *IEEE Applications & Practice*(September 2007).

Ching-Lung, L., et al. (2009). Telecare system using RF communication technology in elderly center. Proceedings of the 13th International Conference on Computer Supported Cooperative Work in Design: 444-449.

Chuang, J., Maimoon, L., Yu, S., Zhu, H., Nybroe, C., Hsiao, O., . . . Chen, H. (2016). SilverLink: Smart Home Health Monitoring for Senior Care. In X. Zheng, D. D. Zeng, H. Chen, & J. S. Leischow (Eds.), *Smart Health: International Conference, ICSH 2015, Phoenix, AZ, USA, November 17-18, 2015. Revised Selected Papers* (pp. 3-14). Cham: Springer International Publishing.

Cognizant (2014). Designing for Manufacturing's "Internet of Things". June.

Collins, S. C., Bhatti, J. Z., Dexter, S. L., & Rabbitt, P. M. (1992). Elderly people in a new world: attitude to advanced communications tecnologies. In H. Boumqa & J. A. M. Graafmans (Eds.), Gerontechnology. Amsterdam: IOS Press.

coreRFID (2016). "Battery assisted passive tags." Retrieved 07.06.2016, from http://www.corerfid.com/rfid-technology/rfid-tracking/battery-assisted-passive-tags/.

Cousin, M., et al. (2015). Devices and diseases.

Craven, J. (2015). "What Is a Smart House." Retrieved 10.05.2016, from http://architecture.about.com/od/buildyourhous1/g/smarthouse.htm.

Crist, R. (2016). Whirlpool's new connected fridge offers smart features and smarter storage. Retrieved 08.06, 2016, from https://www.cnet.com/products/whirlpool-wrf995fifz-smart-french-door-refrigerator/.

Crowe, S. (2016). 6 Robotics Sights to See at CES 2016. Retrieved 10.06, 2016, from http://www.roboticstrends.com/article/6_robotics_sights_to_see_at_ces_2016.

Cubic (2016). Hi, I'm Cubic the AI butler for smart home. Retrieved 08.06, 2016, from http://cubic.ai/.

Curtis, S. (2015). CES 2015 preview: 4K TV, wearables and the connected home. Retrieved 11.06, 2016, from http://www.telegraph.co.uk/technology/ces/11321336/CES-2015-4K-TV-wearables-and-the-connected-home.html.

Demiris, G., Rantz, M. J., Aud, M. A., Marek, K. D., Tyrer, H. W., Skubic, M., & Hussam, A. A. (2004). Older adults' attitudes towards and perceptions of 'smart home'technologies: a pilot study. *Medical informatics and the Internet in medicine*, 29(2), 87-94.

Digital Market Outlook. (2015a). *Smart Home*. Retrieved from https://www.statista.com/outlook/279/100/smart-home/worldwide#

Digital Market Outlook. (2015b). *Smart Home: Ambient Assisted Living*. Retrieved from https://www.statista.com/outlook/283/100/ambient-assisted-living/worldwide

Digital Market Outlook. (2015d). *Smart Home: Energy Management*. Retrieved from Statista: https://www.statista.com/outlook/284/100/energy-management/worldwide#

Digital Market Outlook. (2015f). *Smart Home: Security*. Retrieved from Statista: https://www.statista.com/outlook/281/100/security/worldwide#

Demongeot, J., et al. (2002). Multi-Sensors Acquisition Data Fusion, Knowledge Mining and Alarm Trigering in Health Smart Homes for Elderly People. Comptes Rendus Biologies: 673-682.

DNB (2016). Valutakalkulator. Retrieved 08.06.2016, from https://www.dnb.no/bedrift/markets/valuta-renter/kalkulator/valutakalkulator.html.

Duin, H. S., M.; Schumacher, J.; Thoben, K.-D.; Zhao, X. . (2008). Cross-Impact Analysis of RFID Scenarios for Logistics *Lascg, R.; janker, C. G. (Hrsg): Logistik Management* (pp. 363-376). Wiesbaden: DUV Gabler Edition Wissenschaft.

Eadicicco (2016). Meet Google's Answer to the Amazon Echo. Retrieved 08.06, 2016, from http://time.com/4340140/google-io-amazon-echo/.

Ecobee (2016). Remote sensors. The smarter solution. Retrieved 07.06, 2016, from https://www.ecobee.com/ecobee3-wireless-remote-sensors/.

Etherington, D. (2016). Here Are The First Connected Home Devices For Apple's HomeKit. Retrieved 07.06, 2016, from http://techcrunch.com/2015/06/02/here-are-the-first-connected-home-devices-for-apples-homekit/.

ETSI (2016a). Internet of Things in the Smart Home. Retrieved 09.06.2016, from http://www.etsi.org/news-events/events/1047-2016-02-iotinthesmarthome.

ETSI. (2016b). Internet of Things.   Retrieved 09.05.2016, from http://www.etsi.org/technologies-clusters/technologies/internet-of-things

Ferguson, G. T. (2002). Have Your Objects Call My Objects. *Harvard Business Review* (June 2002).

Futurehome (2016). Futurehome. Retrieved 08.06, 2016, from https://futurehome.no/.

Future Robot (2016). Why True Home Robot?. Retrieved 08.06, 2016, from http://www.myfuro.com/furo-i/service-feature/.

Gautun, H., & Hermansen, Å. (2011). *Eldreomsorg under press*. Retrieved from https://www.nsf.no/Content/674278/NSF-190803-v2-Fafo-rapporten_om_eldreomsorgen_pdf.pdf

Gavrilov, L. A. and P. Heuveline (2003). "Aging of Population ". Retrieved 09.05.2016, from http://health-studies.org/Population_Aging.htm.

Gebhart, A. (2016). Whirlpool's dishwasher debuting at CES orders detergent from Amazon and integrates with Nest. Retrieved 08.06, 2016, from https://www.cnet.com/products/whirlpool-smart-dishwasher/.

Gershenfeld, N., et al. (2004). "The Internet of Things." Scientific American(October): 76-81.

Gezen, J. (2016). Who's Willing To Share Pwesonal Data For Money? A Lot Of People Will, A

New Intel Security Survey Says. Retrieved 08.06.2016, from http://www.techtimes.com/articles/149158/20160412/whos-willing-to-share-personal-data-for-money-a-lot-of-people-will-a-new-intel-security-survey-says.htm.

Ghayvat, H., Liu, J., Mukhopadhyay, S. C., & Gui, X. (2015). Wellness Sensor Networks: A Proposal and Implementation for Smart Home for Assisted Living. *Sensors Journal, IEEE, 15*(12), 7341-7348. doi:10.1109/JSEN.2015.2475626

Gibbs, S. (2015a). Samsung launches SmartThings internet of things hub. Retrieved 08.06, 2016, from https://www.theguardian.com/technology/2015/sep/03/samsung-launches-smartthings-internet-of-things-hub .

Gibbs, S. (2016b). Nest Learning Thermostat third-gen: the simple, effective heating gadget. Retrieved 07.06, 2016, from https://www.theguardian.com/technology/2016/jun/03/google-nest-learning-thermostat-third-generation-home-gadget-smart-heating.

GILC. (2002). *Privacy and Human Rights: An International Survey of Privacy Laws and Practice*. Retrieved from Global Internet Liberty Campaign: http://gilc.org/privacy/survey/

Greenberg, A. (2013). "New Car Attacks--With Me Behind The Wheel (Video)." Retrieved 11.05.2016, from http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#3f76b9d25bf2.

Greenberg, A. (2014). "This iPhone-Sized Device Can Hack a Car, Researchers Plan to Demonstrate." Retrieved 15.05.2016, from www.forbes.com/sites/andygreenberg/2014/02/05/this-iphone-sized-device-can-hack-a-car-researchers-plan-to-demonstrate/.

GreenPeak. (2015). GreenPeak Family@Home Solution transforms the Smart House into a Smart Home [Press release]. Retrieved from http://www.greenpeak.com/Company/PressReleases/PR201512-FamilyLifestyleSystem_EN.html

Halvorsen, K. (1993). *Å forske på samfunnet : en innføring i samfunnsvitenskapelig metode* (3. utg. ed.). Oslo: Bedriftsøkonomens forl.

Harmon, C. (2010). RFID standards: Opening a world of possibilities. *ISO Focus*(April 2010), 2.

Helal, A., et al. (2005). Gator Tech Smart House: A Programmable Pervasive Space. IEEE Computer Magazine: 67-74.

Higginbotham, S. (2015). Lowe's Has Big Plans for its New Home Smart Hub. Retrieved 08.06, 2016, from http://fortune.com/2015/11/16/lowes-iris-smart-hub/.

Honeywell (2016a). Protect What Matters. Retrieved 26.05.2016, from http://homesecurity.honeywell.com/home_security.html.

Honeywell (2016b). Think Green. Retrieved 26.05.2016, from http://homesecurity.honeywell.com/energy_management.html.

Honeywell (2016c). Your Connected Home. Retrieved 25.05.2016, from http://homesecurity.honeywell.com/home_automation.html.

Icontrol. (2015). *2015 State of the Smart Home Report*. Retrieved from http://www.icontrol.com/wp-content/uploads/2015/06/Smart_Home_Report_2015.pdf

IDC (2015). Wearables market remained strong in the first quarter despite the pending debut of the Apple watch, says IDC. Retrieved 30.05.2016, from http://www.idc.com/getdoc.jsp?containerId=prUS25658315.

IDTechEx (2015). RFID Forecasts, Players and Opportunities 2016-2026. October.

IMPINJ. Retrieved from http://www.impinj.com/resources/about-rfid/the-different-types-of-rfid-systems/

Infobionic (2016). The System. Retrieved 30.06.2016, from http://infobionic.com/the-system/.

Intel. (2015). *Could Smart Homes Be as Commonplace as Smartphones by 2025?* Retrieved from http://download.intel.com/newsroom/kits/iot/pdfs/IntelSmartHomeSurveyBackgrounder.pdf

Intel. (2016). *Intel Survey: Architecting the Future of the Smart Home 2025*. Retrieved from http://download.intel.com/newsroom/kits/iot/pdfs/IntelSmartHomeSurveyBackgrounder.pdf

Intille, S. S., et al. (2006). "Using a live-in laboratory for ubiquitous computing research." *Pervasive 2006. LNCS 3968: 349-365.*

ISACA (2014). ISACA 2014 IT Risk/Reward Barometer. Retrieved 14.05.2016, from http://www.isaca.org/pages/2014-risk-reward-barometer.aspx.

ISACA (2015). *Internet of Things: Risk and Value considerations*. Isaca.org: http://vbn.aau.dk/files/208325607/Internet_of_Things_whp_Eng_0115.pdf

Jibo (2016). Jibo. Retrieved 08.06, 2016, from https://www.jibo.com/.

Johannessen, A., Christoffersen, L., & Tufte, P. A. (2011). *Forskningsmetode for økonomisk-administrative fag* (3 ed.): Abstrakt forlag.

Kastrenakes, J. (2015). Amazon's Echo speaker is now also a smart home hub. Retrieved 08.06, 2016, from http://www.theverge.com/2015/4/9/8379411/amazon-echo-smart-home-control-wemo-hue.

Kavis, M. (2014). The Internet Of Things Will Radically Change Your Big Data Strategy. Retrieved 24.05.2016, from http://www.forbes.com/sites/mikekavis/2014/06/26/the-internet-of-things-will-radically-change-your-big-data-strategy/#2c29ea383abe.

Keating, L. (2016). Latch Is The Smart Lock For Luxury Apartment Buildings And Tech-Loving Offices. Retrieved 04.06, 2016, from http://www.techtimes.com/articles/132416/20160210/latch-smart-lock-luxury-apartment-buildings-tech-loving-offices.htm.

Kellner, T. (2013). Analyze This: The Industrial Internet By The Numbers Outcomes. Retrieved 24.05.2016, from http://www.gereports.com/post/74545267912/analyze-this-the-industrial-internet-by-th.

Kelly, H. (2015). Nest's new security camera lets you watch your pets. Retrieved 04.06, 2016, from http://money.cnn.com/2015/06/17/technology/nest-dropcam-google/.

Khawaja, M. (2011). Population ageing in New Zealand. Retrieved 09.05.2016, from http://www.stats.govt.nz/browse_for_stats/people_and_communities/older_people/pop-ageing-in-nz.aspx.

Klein, C. (2016). 2016 predictions for IoT and smart homes. Retrieved 08.06.2016, from http://thenextweb.com/insider/2015/12/23/2016-predictions-for-iot-and-smart-homes/#gref1.

Kreber, T., Jiang, Y., & Mitchel, D. (2016). 360 View: Energy Management, Smart Home, and Utility Programs. Retrieved from http://www.parksassociates.com/360view/360-hem-2016

Lambert, F. (2016). SolarCity is launching a new Solar+Tesla Powerwall+Nest Smart Thermostat package to manage energy and reduce grid dependence. Retrieved 07.06, 2016, from http://electrek.co/2016/02/25/solarcity-tesla-powerwall-nest-hawaii/.

Lanaria, V. (2016a). Roots Introduces New Smart Smoke Alarms That Could Give Nest Protect A Run For Its Money. Retrieved 04.06, 2016, from http://www.techtimes.com/articles/156079/20160505/roost-introduces-new-smart-smoke-alarms-that-could-give-nest-protect-a-run-for-its-money.htm.

Lanaria, V. (2016b). Smart Mattress Will Notify You If You're Partner Is Cheating - Or Rocking The Bed. Retrieved 07.06, 2016, from http://www.techtimes.com/articles/151627/20160420/smart-mattress-will-notify-you-if-youre-partner-is-cheating-or-rocking-the-bed.htm.

Lawton, G. (2004). Machine-to-machine technology gears up for growth (Vol. 37, pp. 12-15). USA.

Lowe's (2016). A Smarter Way to Live. Retrieved 08.06, 2016, from https://www.irisbylowes.com/about/.

Lyse (2016). Slik fungerer Smartly. Retrieved 26.05.2016, from https://www.smartly.no/om-smartly/slik-fungerer-smartly/.

Machado, H. and K. Shah (2016). Internet of Things (IoT) impacts on Supply Chain. Retrieved 19.05.2016, from http://apicsterragrande.org/images/articles/Machado__Internet_of_Things_impacts_on_Supply_Chain_Shah_Machado_Second_Place_Grad.pdf.

Mamiit, A. (2016). Amazon Echo: Here's A List Of Compatible Devices With Alexa" Retrieved 07.06, 2016, from http://www.techtimes.com/articles/142090/20160319/amazon-echo-heres-a-list-of-compatible-devices-with-alexa.htm.

Marr, B. (2015a). 3 Ways the Internet Of Things Will Change Every Business. Retrieved 19.04.2016, 2016, from http://www.forbes.com/sites/bernardmarr/2015/08/17/3-ways-the-internet-of-things-will-change-every-business/#6a465538d152.

Marr, B. (2015b). 17 'Internet Of Things' Facts Everyone Should Read. Retrieved 19.04.2016, 2016, from http://www.forbes.com/sites/bernardmarr/2015/10/27/17-mind-blowing-internet-of-things-facts-everyone-should-read/#4b4481ae1a7a.

Micro Matic Norge AS (2016). Bo Smartere.

Minor, J. (2016). 9 Top Trends at CES 2016. Retrieved 11.06.2016, from http://uk.pcmag.com/samsung-gear-vr/74376/news/9-top-trends-at-ces-2016.

Misic, V. B., & Misic, J. (2014). *Machine-to-machine Communications: Architectures, Technology, Standards, and Applications*: CRC Press.

Mynatt, E. D., et al. (2004). Aware technologies for aging in place: understanding user needs and attitudes. *IEEE Pervasive Computing 3(2)*: 36-41.

National Institute on Aging, National Institute of Health, & U.S. Department of Health and Human Services. (2011). Global Health and Aging. Retrieved from http://www.nia.nih.gov/sites/default/files/global_health_and_aging.pdf

Nest (2016). Nest Thermostat. Retrieved 07.06, 2016, from https://nest.com/thermostat/meet-nest-thermostat/.

Netatmo (2016). Netatmo Presence. Retrieved 04.06, 2016, from https://www.netatmo.com/en-US/product/presence.

Nichols, G. (2016). At your service: 8 personal assistant robots coming home soon. Retrieved 08.06, 2016, from http://www.zdnet.com/pictures/at-your-service-8-personal-assistant-robots-coming-home-soon/

Newton, T. (2012). Internet Connected Toasters: A history . Retrieved 21.03, 2016, from https://recombu.com/digital/article/internet-connected-toasters-a-history_M10281.html.

Nourizadeh, S., et al. (2009). Medical and Home Automation Sensor Networks for Senior Citizens Telehomecare. Proceedings of the IEEE International Conference on Communications Workshops: 1-5.

Novak, M. (2015). Nikola Tesla's Incredible Predictions For Our Connected World. Retrieved 10.03.16, 2016, from http://paleofuture.gizmodo.com/nikola-teslas-incredible-predictions-for-our-connected-1661107313.

Olafsen, H. K. (2007). *Wireless sensor network localisation strategies*

Orton-Jones, C. (2014). Internet of Things: Changing how we live. Retrieved 23.07.2015, from http://raconteur.net/technology/internet-of-things-changing-how-we-live.

Parks Associates. (2016). *The Evolution of Home Energy Management*. Retrieved from http://www.parksassociates.com/report/evolution-home-energy-management

Passary, A. (2016a). Best Smart Light Bulbs That You Can Buy Today: Philips Hue, Sony LED Light Bulb Speaker, Misfits Bolt And More. Retrieved 08.06, 2016, from http://www.techtimes.com/articles/151165/20160419/best-smart-light-bulbs-that-you-can-buy-today-philips-hue-sony-led-light-bulb-speaker-misfit-bolt-and-more.htm.

Passary, A. (2016b). Parents, Don't Panic: Amazon Echo, Other Alexa-Enabled Devices Can Answer Quesions About Your Kids' Health. Retrieved 07.06, 2016, from http://www.techtimes.com/articles/151118/20160419/parents-dont-panic-amazon-echo-other-alexa-enabled-devices-can-answer-questions-about-your-kids-health.htm.

Passary, S. (2016). Nissan Takes On Tesla Powerwall With New Home Battery xStorage: Is It Better?. Retrieved 07.06, 2016, from http://www.techtimes.com/articles/157516/20160512/nissan-takes-on-tesla-powerwall-with-new-home-battery-xstorage-is-it-better.htm.

Patel, S. N., Kientz, J. A., Jones, B., Price, E., Mynatt, E. D., & Abowd, G. D. (2007). An Overview of the Aware Home Research Initiative at the Georgia Institute of Technology. . *Proceedings of the International Future Design Conference on Global Innovations in Macro-and-Micro-Environments for the Future*, 169-181.

Pierson, R. M. (2016). Meet Sony's Cool New Robotic Personal Assistant. Retrieved 08.06, 2016, from http://readwrite.com/2016/02/26/sony-xperia-agent-concept/.

Pilkington, E. (2009). Population of older people set to surpass number of children, report finds. Retrieved 09.05.2016, 2016, from http://www.theguardian.com/world/2009/jul/20/census-population-ageing-global.

Press, G. (2014). A Very Short History Of The Internet Of Things. Retrieved 19.04.2016, 2016, from http://www.forbes.com/sites/gilpress/2014/06/18/a-very-short-history-of-the-internet-of-things/#ea93ba2df55e.

Rahimpour, M., et al. (2008). Patients Perceptions of a Home Telecare System. *International Journal of Medical Informatics*: 486-498.

RCN. (2010). *Care homes under pressure - an England report*. Retrieved from https://www.rcn.org.uk/about-us/policy-briefings/pol-0410

Research & Market. (2016). *Global Smart Home Healthcare Market Size, Share, Development, Growth and Demand Forecast to 2022*. Retrieved from http://www.researchandmarkets.com/research/nkj7qz/global_smart_home

RFID Journal (2016b). RFID Journal. Retrieved 09.05.2016, from http://www.rfidjournal.com/

Rossen, E. and I. M. Liseter (2015). Internetts historie. Retrieved 12.04.2016, 2016, from https://snl.no/Internetts_historie.

Rothfeld, L. (2015). Tech time machine: The smart home. Retrieved 01.06.2016, from http://mashable.com/2015/01/08/smart-home-tech-ces/#m_8xvT3vOkqy

Rouse, M. (2005). Smart home or building. Retrieved 01.06.2016, from http://internetofthingsagenda.techtarget.com/definition/smart-home-or-building

Rubens, P. (2014). How to Develop Applications for the Internet of Things. Retrieved 07.06.2016, from http://www.cio.com/article/2843814/developer/how-to-develop-applications-for-the-internet-of-things.html.

Rubin, B. F. (2015). Apple Watch nips at Fitbit's heel in wearables race. Retrieved 24.05.2016, from http://www.cnet.com/news/apple-watch-poised-to-overtake-fitbit-in-wearables-shipments/.

Schoenberger, C. R. (2002, 18.03.2002). The Internet of Things. Retrieved 01.05.2016, 2016, from http://www.forbes.com/global/2002/0318/092.html.

Sem, D. (2016). Samsung Introduces Personal Assistant Robot Otto: Should Alexa Be Worried? Retrieved 07.06.2016, from http://www.techtimes.com/articles/154729/20160430/samsung-introduces-personal-assistant-robot-otto-should-alexa-be-worried.htm.

Shankland, S. (2016). Your smart-home network will be a mess. Retrieved 09.06. 2016, from https://www.cnet.com/news/your-smart-home-network-will-be-a-mess-to-start-with/.

Smartly (2016a). Aktivitet of deltakelse. Retrieved 08.07, 2016, from https://www.smartly.no/smarthjem/velferd/velferd-senarioer/aktivitet-og-deltakelse/.

Smartly (2016b). Egenomsorg og mestring. Retrieved 08.06, 2016, from https://www.smartly.no/smarthjem/velferd/velferd-senarioer/egenomsorg-og-mestring/.

Smartly (2016c). Nå får du se smarte dører og vinduer. 04.06.2016, from https://www.smartly.no/om-smartly/smarte-venner/naa-faar-du-smarte-doerer-og-vinduer/.

Smartly (2016d). Smartly. Retrieved 08.06, 2016, from https://www.smartly.no/.

Smartly (2016e). Trygg og selvstendig. Retrieved 08.07. 2016, from https://www.smartly.no/smarthjem/velferd/velferd-senarioer/trygghet-og-selvstendighet.

Smiley, S. (2016). What Are BAP RFID Tags?. Retrieved 07.06.2016, from http://blog.atlasrfidstore.com/bap-rfid-tags.

Smart Home Energy. (2016). What is a "Smart Home”? Retrieved 31.05.2016, from http://smarthomeenergy.co.uk/what-smart-home

SMARTech (2016). How much does a smart home cost? . Retrieved 08.06.2016, from http://www.smarthome.eu/how-much-does-a-smart-home-system-cost.

South China Morning Post (2016). Retrieved 10.06, 2016, from http://www.scmp.com/lifestyle/article/1896925/six-consumer-tech-trends-coming-2016-virtual-reality-and-robots.

Store Norske Leksikon (2016). Metode. Retrieved 12.06, 2016, from https://snl.no/metode.

Suryadevara, N. K., & Mukhopadhyay, S. C. (2015). Smart Homes: Design, Implementation and Issues (Vol. v.14). Cham: Springer International Publishing.

Syrkett, A. (2016). "CES 2016: 5 Smart Home Tech Trends to Watch." Retrieved 04.06, 2016, from http://www.curbed.com/2016/1/11/10848046/home-tech-smart-home-ces-2016-trends.

Tan, Lu and Neng Wang. (2010). *Future Internet: The Internet of Things.* ICACTE. Retrived 22.02.16 http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5579543

Taylor, H. (2016). How your home will know what you need before you do. Retrieved 07.06, 2016, from http://www.cnbc.com/2016/01/06/ces-smart-homes-of-the-future.html.

TeslaMotors (2016). Powerwall -Tesla hjemmebatteri. Retrieved 07.06, 2016, from https://www.teslamotors.com/no_NO/powerwall.

Thomas, J. R., Silverman, S. J., & Nelson, J. K. (2005). *Research methods in physical activity* (5th ed. ed.). Champaign, Ill: Human Kinetics.

Thompson, A. C. (2016). Whirlpool's smart oven talks to Nest. Retrieved 08.06, 2016, from https://www.cnet.com/products/whirlpool-smart-front-control-range/.

Tiongco, S. (2016). Dyson Outs Pure Cool Link Smart Air Purifier: Here's What It Can Do. Retrieved 07.06, 2016, from http://www.techtimes.com/articles/145851/20160402/dyson-outs-pure-cool-link-smart-air-purifier-heres-what-it-can-do.htm.

U.S. Department of Energy (2016). Tips: Time-based electricity rates. Retrieved 12.06.2016, from http://energy.gov/energysaver/tips-time-based-electricity-rates.

Ungureanu, H. (2016a). Asus Unveils Walking, Talking Robot for The Smart Home: Meet Zenbo [Video]. Retrieved 03.06, 2016, from http://www.techtimes.com/articles/161925/20160530/asus-unveils-walking-talking-robot-for-the-smart-home-meet-zenbo-video.htm.

Ungureanu, H. (2016b). If You Have 4 Grand Lying Around, You Might As Well Play Music On This LG Fridge. Retrieved 07.06, 2016, from http://www.techtimes.com/articles/159896/20160520/if-you-have-4-grand-lying-around-you-might-as-well-play-music-on-this-lg-fridge.htm

van der Meulen, R. (2015). Gartner Says 6.4 Billion Connected "Things" Will Be in Use in 2016, Up 30 Percent from 2015. Retrieved 24.05.2016, from http://www.gartner.com/newsroom/id/3165317.

Waniata, R. (2016). "Sony's Xperia Agent is the cute little robot that could. But will he?". Retrieved 08.06, 2016, from http://www.digitaltrends.com/home/sony-xperia-agent-adorable-internet-of-things-robot/#:nukraWn-g65cZA.

Weaver, J. F. (2016). Energy Management making plays for the SmartHouse, and it might win it all. Retrieved 07.06, 2016, from http://electrek.co/2016/06/05/energy-management-making-plays-for-the-smarthouse-and-might-win-it-all/.

Webb, W. (2008). RFID in embedded designs: Your move. Retrieved 22.02.2016, from http://www.edn.com/design/communications-networking/4326834/RFID-in-embedded-designs-Your-move

Whirlpool (2016). A Future Inspired by Care. Retrieved 08.06, 2016, from http://ces.whirlpool.com/

Wikipedia (2016a). Big Data. Retrieved 31.05.2016, from https://en.wikipedia.org/wiki/Big_data.

Wikipedia (2016b). Home Automation. Retrieved 08.06.2016, from https://en.wikipedia.org/wiki/Home_automation

Wikipedia. (2016c). Institute of Electrical and Electronics Engineers. Retrieved 09.05.2016, from https://en.wikipedia.org/wiki/Institute_of_Electrical_and_Electronics_Engineers

Wikipedia. (2016d). Machine to machine. Retrieved 09.05.2016, from https://en.wikipedia.org/wiki/Machine_to_machine#cite_note-45

Wikipedia. (2016e). Observation. Retrieved 25.05.2016, from https://en.wikipedia.org/wiki/Observation

Wikipedia. (2016f). Wireless sensor network. Retreived 09.05.2016, from https://en.wikipedia.org/wiki/Wireless_sensor_network

Wikipedia. (2016g). X10 (industry standard). Retrieved 01.06.2016, from https://en.wikipedia.org/wiki/X10_(industry_standard)

Woodford, C. (2015, 27.05.15). Smart homes and the Internet of Things. Retrieved 01.06.2016, from http://www.explainthatstuff.com/smart-home-automation.html

Woollaston, V. (2016). Intel and Netflix steal the show at CES 2016: Stats reveal which brands made the best announcements at this year's conference. Retrieved 07.06, 2016, from http://www.dailymail.co.uk/sciencetech/article-3393698/Intel-Netflix-steal-CES-2016-Stats-reveal-brands-talked-tech-conference.html.

World Development Indicators (2012). The World by Income. Retrieved 09.05.2016, from https://openknowledge.worldbank.org/bitstream/handle/10986/6014/681720PUB0EPI004019020120Box367902B.txt?sequence=2.